

УДК 681.3

А.Э. Бекиров, К.Ю. Трифоненко, Н.В. Кутя

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

ПУТИ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В данной статье рассмотрены пути повышения информационной безопасности информационных ресурсов в системах видеоконференцсвязи автоматизированных систем управления специального назначения Министерства обороны Украины. Определены группы показателей качества стеганографических методов. На основе сформулированных требований проведен анализ существующих стеганографических алгоритмов встраивания информации в контейнер изображения.

Ключевые слова: стеганография, показатели качества, стойкость, алгоритм встраивания.

Введение

Широкое распространение и развитие телекоммуникационных сетей находит применение в самых различных областях деятельности человека. Также, остро стоит вопрос о внедрении современных телекоммуникационных систем в автоматизированных системах управления специального назначения в интересах Министерства обороны (АСУ СН МО). Одним из возможных вариантов реализации оперативного обмена информацией в АСУ МО является видеоконференция. Применение такого вида связи имеет преимущества, обусловленные сокращением времени обмена информацией между абонентами, обеспечением максимально приближенных к реальным условий обмена информацией, обеспечением возможности передачи дополнительной информации в каналах передачи видеоданных и сокращением времени, необходимым для управления и принятия решения.

Несмотря на то, что в интересах Министерства обороны применяется закрытая видеоконференцсвязь, существует необходимость повышения безопасности информационных ресурсов АСУ МО. Такая необходимость обусловлена как появлением у

противника большого количества информационно-технических средств для проведения атак, так и использованием зарубежных технологий для организации обработки и передачи данных. Одним из возможных способов повышения стойкости, является применение методов цифровой стеганографии. Такие методы позволяют одновременно с видеоданными незаметно передавать закрытую информацию.

Таким образом, предлагается направление для повышения информационной безопасности, а именно применение стеганографического метода встраивания информации в изображение-контейнер. Такой метод применяется дополнительно к криптографическому методу защиты и не требует дополнительных затрат.

Основная часть

Для сравнения и оценки существующих стеганосистем необходимо наличие адекватной системы показателей оценки качества их функционирования. Такое оценивание должно давать полную картину успешности их использования для скрытия данных [1].

Показатели качества стеганографических алгоритмов можно разделить на следующие группы характеристик (рис. 1):



Рис. 1. Показатели качества стеганоалгоритмов

I. Группа показателей, характеризующих стега-ноалгоритм с позиции скрытности, т.е. стойкости стега-ноалгоритма к выявлению факта наличия в изо-бражении скрытого сообщения и его извлечения. Рас-смотрение скрытности возможно по составляющим:

1. Вероятность $P_{уст}$ установления злоумышлен-ником факта наличия секретного сообщения в изо-бражении.

При наличии исходного изображения контей-нера, стойкость стега-ноалгоритма может быть оце-нена с помощью количественных разностных и кор-реляционных показателей [2]:

1. Максимальная разность MD:

$$MD = \max_{x,y} |C_{x,y} - S_{x,y}|, \quad (1)$$

где $C_{x,y}$ - пиксели изображения контейнера, с коор-динатами x,y , $S_{x,y}$ - пиксели стеганограммы с коор-динатами x,y .

2. Средняя абсолютная разность AD:

$$AD = \frac{1}{XY} \sum_{x,y} |C_{x,y} - S_{x,y}|. \quad (2)$$

3. Качество изображения IF. Чем $IF \rightarrow 0$, тем ближе полученное изображение приближается к оригиналу.

$$IF = 1 - \frac{\sum_{x,y} (C_{x,y} - S_{x,y})^2}{\sum_{x,y} (C_{x,y})^2}. \quad (3)$$

4. Отношение сигнал-шум SNR.

$$SNR = \frac{\sum_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}. \quad (4)$$

5. Нормированная взаимная корреляция NCC. При высокой подобности изображений $NCC \rightarrow 1$.

$$NCC = \frac{\sum_{x,y} (C_{x,y} \cdot S_{x,y})}{\sum_{x,y} (C_{x,y})^2}. \quad (5)$$

Качественно вероятность установления зло-умышленником факта наличия секретного сообще-ния в изображении $P_{уст}$ может быть определена при помощи экспертных оценок.

6. Вероятность $P_{бл}$ правильного определения блока изображения со встроенной информацией.

7. Вероятность $P_{из}$ правильного изъятия встроенного сообщения из стеганограммы.

II. Группа показателей характеризующих сте-га-ноалгоритм с позиции объема встраиваемых дан-ных.

1. Нормированный коэффициент стега-нопреоб-разования τ , т.е. минимально требуемый объем изображения или его части, в который, в соответст-вии с заданным стега-нопреобразованием, возможно встроить сообщение объемом $w_{встр}$.

$$\tau = \frac{w_{встр}}{W_{исх}}, \quad (6)$$

где $W_{встр}$ - объем встраиваемой информации, изме-ряется в битах; $W_{исх}$ - объем части изображения, в которую необходимо встроить сообщение, объемом $w_{встр}$.

2. Стега-нографический битрейт p_b , т.е. вели-чина, характеризующая, какое количество пикселей в среднем необходимо для встраивания одного бита информации. Измеряется в битах на пиксель, бит/пиксель.

$$p_b = \frac{w_{встр}}{Z_{строк} Z_{столб}}, \quad (7)$$

где p_b - стега-нографический битрейт, бит/пиксель; $Z_{строк} Z_{столб}$ - минимально требуемый размер изо-бражения, достаточный для встраивания стега-но-графическим алгоритмом информации, объемом $w_{встр}$.

III. Группа показателей характеризующих сте-га-ноалгоритм с позиции временных затрат на обра-ботку.

1. Время встраивания $\tau_{(w_{встр})пр}$, т.е. временные затраты, необходимые для встраивания информации объемом $w_{встр}$.

2. Время изъятия $\tau_{(w_{встр})обр}$, т.е. время изъятия из стеганограммы информации, объемом $w_{встр}$.

IV. Группа показателей характеризующих сте-га-ноалгоритм с позиции стойкости к атакам.

Основным показателем является вероятность $P_{мод}$ модификации встроенных сообщений. Данная вероятность принимает значения $0 \leq P_{мод} \leq 1$. Чем $P_{мод} \rightarrow 0$, тем выше стойкость стега-нопреобразо-вания к атакам. Вероятность $P_{мод}$ может оценивать стойкость алгоритмов к различным видам атак.

V. Группа показателей характеризующих сте-га-ноалгоритм с позиции ухудшения его компресси-онных представлений.

Из-за использования в современных телеком-муникационных системах компрессионного пред-ставления изображений, появляется необходимость учитывать влияние встроенной информации на по-казатели сжатия стеганограммы.

Поэтому предлагается ввести следующие пока-затели оценки влияния стега-нографических преоб-

разований на показателі компрессионного представлення зображення-контейнера:

1. Коэффициент снижения степени сжатия Δk

$$\Delta k = \frac{W_{сж}}{W'_{сж}}, \quad (8)$$

где $W_{сж}$ - объем сжатого изображения-контейнера без встраивания;

$W'_{сж}$ - объем сжатого стеганографически преобразованного изображения.

2. Степень изменения пикового отношения сигнал-шум Δh

$$\Delta h = |h - h'|, \quad (9)$$

где h - пиковое отношение сигнал-шум контейнера-изображения, дБ;

h' - пиковое отношение сигнал-шум изображения со встроенной информацией, дБ.

3. Степень увеличения суммарного времени обработки Δt

$$\Delta t = \frac{t'_{обр} - t_{обр}}{t_{обр}} \cdot 100\%, \quad (10)$$

где

$$t'_{обр} = t_{обр} + \tau_{(W_{встр})пр} + \tau_{(W_{встр})обр};$$

$t_{обр}$ - время компрессионной обработки изображения-контейнера;

$\tau_{(W_{встр})пр}$ - время встраивания информации в контейнер-изображение;

$\tau_{(W_{встр})обр}$ - время изъятия информации из стеганограммы.

VI. Группа показателей характеризующих стеганоалгоритм с позиции устойчивости к ошибкам.

Показатели устойчивости встроенного сообщения к ошибкам в канале связи и потерям пакетов при его передаче в инфокоммуникационных каналах:

1. Вероятность $P_{ошб}$ появления ошибки встроенного сообщения;

2. Вероятность $P_{потр}$ потери встроенного сообщения.

Проанализировав принципы построения и организации закрытых систем видеоконференцсвязи, можно сформулировать требования к характеристикам разрабатываемого метода встраивания:

1. Возможность извлечения сообщения «вслепую», т.е. без наличия исходного контейнера и какой либо информации о встроенном сообщении.

2. Стойкость стеганосистемы к искажению контейнера и сообщения при передаче по каналами с потерей данных и пакетов.

3. Стойкость стеганосистемы к пассивным и активным атакам. Вероятность модификации $P_{мод} \rightarrow 0$, что обеспечит доставку встроенного со-

общения получателю в условиях активных и пассивных атак.

4. Возможность встраивания сообщения в реальном времени. При этом время встраивания $\tau_{(W_{встр})пр}$ и время изъятия $\tau_{(W_{встр})обр}$ стремятся к нулю.

5. Возможность встраивания данных большого объема. При реализации алгоритма объем встраиваемых данных $w_{встр} \rightarrow 0$.

6. Операции по встраиванию секретного сообщения не должны увеличивать размер контейнера.

7. Разрабатываемый алгоритм должен быть устойчив к сжатию. При этом

$$\Delta k \rightarrow 0 \text{ и } \Delta t \rightarrow 0.$$

В АСУ МО, информация, которую необходимо встроить в видеопоток, имеет произвольную природу. Таким образом, алгоритмы, используемые в видеоконференцсвязи, должны проводить извлечение встроенного сообщения без наличия на принимающей стороне какой либо информации о контейнере и исходном сообщении.

Метод замены наименее значащего бита. Физика метода заключается в замене младшего значащего бита, битом секретного сообщения [1]. Среди модификаций данного метода, существуют реализации случайного распределения битов секретного сообщения в контейнере и их псевдослучайной перестановки.

Метод блочного кодирования представляет собой реализацию алгоритма замены, при которой в одном из блоков изображения происходит скрытие одного секретного бита.

Метод замены палитры. В данном методе для встраивания секретного сообщения используется палитра цветов контейнера-изображения. При реализации алгоритма существует $N!$ различных способов перестановки N -цветной палитры, что достаточно для встраивания небольшого сообщения [2].

Метод модификации яркости (метод Куттера-Джордана-Боссена). Встраивание сообщения происходит в канал синего цвета RGB изображения [4].

Метод Дармстедтера-Делейгла-Квисквотера-Макка. Алгоритм представляет собой один из вариантов модификации яркости, при котором контейнер разбивается на блоки 8×8 пикселей, соразмерных с блоками при JPEG компрессии [5].

Метод относительной замены величин дискретного косинусного преобразования (метод Коха и Жао). В методе реализована модификация коэффициентов ДКП блоков, при котором создается зависимость, позволяющая встраивать «0» или «1» секретного сообщения.

Метод Бенгама-Мемона-Эо-Юнг. Метод представляет собой оптимизированную версию метода

замены величин ДКП и использует для встраивания три коэффициента ДКП из среднечастотной области изображения.

Для сравнения перечисленных стеганоалгоритмов, в табл. 1 приведены количественные разностные и корреляционные показатели.

Метод встраивания в наименее значимый бит и его модификации не вносят дополнительные данные в изображение, а лишь заменяют избыточные данные.

Достоинствами данных методов является его простота и достаточно большие объемы данных, которые возможно встроить в относительно небольшие файлы. Алгоритм встраивания реализуется без предварительной обработки изображения и это положительно отражается на времени встраивания $\tau_{(W_{встр})_{пр}}$. Основной недостаток методов - высокая чувствительность к малейшим искажениям контейнера.

Данный метод имеет низкую стеганографическую стойкость, и он не устойчив к атакам сжатием.

Метод замены палитры имеет достаточно высокие показатели.

Данный метод также не вносит дополнительной информации в контейнер, а использует избыточность палитры цветов.

Одним из преимуществ данного метода является наличие различных способов улучшения реализации, не вызывая при этом искажения изображения.

Среди недостатков данного алгоритма - ограниченное количество встраиваемой информации, а также отсутствие стойкости к атакам с изменением палитры изображения и атакам сжатия.

Метод модификации яркости (метод Куттера-Джордана-Боссена) учитывает избыточность цветовых компонент RGB, а именно синего цвета. Несмотря на устойчивость к различным атакам (НЧ фильтрация, компрессия JPEG, обрезание краев), данный алгоритм вносит значительные искажения в контейнер [4], что в свою очередь отобразится на его визуальной заметности и статистических характеристиках.

Таблица 1

Количественные показатели искажений

| Область встраивания | Алгоритм встраивания данных в изображение-контейнер | Показатели искажения изображения | | | | |
|--------------------------|--|----------------------------------|---------------------------------|--------------------------|---------------------------|---------------------------------------|
| | | Максимальная разность, MD | Средняя абсолютная разность, AD | Качество изображения, IF | Отношение сигнал-шум, SNR | Нормированная взаимная корреляция. NC |
| Пространственная область | Метод замены наименее значащего бита (метод НЗБ, LSB) | 1 | 0.494 | 0.99998 | 4975 | 0.999439 |
| | Метод псевдослучайного интервала | 1 | $7.690 \cdot 10^{-3}$ | ~1 | $3.193 \cdot 10^6$ | 0.999992 |
| | Метод псевдослучайной перестановки | 1 | $5.920 \cdot 10^{-3}$ | ~1 | $4.148 \cdot 10^6$ | 0.999998 |
| | Метод блочного кодирования | 1 | $6.165 \cdot 10^{-3}$ | ~1 | $3.983 \cdot 10^6$ | 0.999988 |
| | Метод замены палитры | 3 | $9.827 \cdot 10^{-3}$ | 0.999999 | $1.142 \cdot 10^6$ | 0.999942 |
| | Метод квантования изображения | 3 | $7.141 \cdot 10^{-3}$ | ~1 | $2.596 \cdot 10^6$ | 1.000001 |
| | Метод модификации яркости (метод Куттера-Джордана-Боссена) | 38 | 4.588 | 0.994799 | 192.271 | 0.988343 |
| Спектральная область | Метод относительной замены величин ДКП (метод Коха и Жао) | 45 | 11.392 | 0.992737 | 137.690 | 0.986178 |
| | Метода Бенгама-Мемона-Эо-Юнг | 51 | 3.042 | 0.998721 | 781.605 | 0.994154 |

Упомянутые спектральные стеганографические преобразования используются в алгоритмах сжатия изображений, поэтому большинство спектральных методов являются стойкими к компрессионным атакам [3]. Объем встраиваемых данных ограничен разрешением изображения и количеством блоков коэффициентов преобразования, выбранных для встраивания. Среди недостатков спектральных методов можно выделить избирательность контейнера. Наличие в контейнере гладких и текстурированных областей отображается на частотных коэффициентах преобразований. Гладкие области изображения содержат большое количество НЧ коэффициентов, а структурные области – ВЧ коэффициенты. Ограниченность использования ВЧ коэффициентов обусловлена их обнулением при квантовании. Использование НЧ коэффициентов сильно искажает исходный контейнер и отображается в приведенных разностных и корреляционных показателях. В некоторых источниках приводятся методы встраивания в СЧ коэффициенты преобразований. Дело в том, что определение таких коэффициентов возможно для конкретного блока преобразований, но не для всех блоков или других изображений. Такое определение является условным и при определенных условиях (квантование) СЧ коэффициенты будут обладать свойствами ВЧ и НЧ компонент. Также спектральные стеганографические алгоритмы, в силу их сложности, требуют достаточного времени на реализацию.

Таким образом, не существует алгоритма, который был бы стойким ко всем перечисленным видам атак. Некоторые стеганоалгоритмы вносят значительные искажения в контейнер – изображение, что влечет за собой снижение стойкости. Также, существенным недостатком большинства существующих методов, является потеря встроенных данных при обработке алгоритмами компрессии, такими как JPEG.

Выводы

В данной статье приведены группы показателей качества стеганографических систем, позволяющие давать адекватную оценку успешности использования систем для встраивания данных. Также сформулированы требования для алгоритмов встраивания данных в видеопоток в АСУ МО. Выполнен обзор и анализ существующих стеганографических методов встраивания сообщений в изображение вслепую. Существующие алгоритмы не в полной мере удовлетворяют требованиям скрытности и требованиям по времени встраивания и извлечения. Эффективность данных методов зависит от конкретных условий использования.

Список литературы

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.
2. Коначович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Коначович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
3. Тарасов Д.О. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д.О. Тарасов, А.С. Мельник, М.М. Голобородько // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка". – № 673.– Львів, 2010. – С. 365-374.
4. Kutter M. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. Of the SPIE Storage and Retrieval for Image and Video Databases V. – 1997. – Vol. 3022. – P. 518-526.
5. Darmstaedter V. Low Cost Spatial Watermarking / V. Darmstaedter, J.-F. Delaigle, J.J. Quisquater, B. Macq // Computers and Graphics. – 1998. – Vol. 5. – P. 417-423.

Поступила в редколлегию 15.04.2014

Рецензент: д-р техн. наук проф.. В.В. Баранник, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ШЛЯХИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

А.Е. Бекіров, К.Ю. Трифоненко, М.В. Куця

У даній статті розглянуті шляхи підвищення інформаційної безпеки інформаційних ресурсів в системах відеоконференцзв'язку автоматизованих систем управління спеціального призначення Міністерства Оборони. Визначені групи показників якості стеганографічних методів. На основі сформульованих вимог проведено аналіз існуючих стеганографічних алгоритмів вбудовування інформації в контейнер-зображення.

Ключові слова: стеганографія, показники якості, стійкість, алгоритм вбудовування.

THE WAYS OF INCREASE OF INFORMATION RESOURCES SAFETY IN THE SYSTEMS OF SPECIAL PURPOSE

A.E. Bekirov, C.Y. Trifonenko, N.V. Kutya

This article discusses ways to improve the information security of information resources in video conferencing systems of automated control systems for special purposes the Ministry of Defence. The groups of indicators of quality of steganographic techniques were determined. On the basis of formulated requirements, existing steganographic algorithm embedding information in an image container was analyzed.

Keywords: steganography, quality indicators, resistance, algorithm of embedding.