1. Takahashi, M. / M. Takahashi, M. Izuki, R. Kanno, Y. Kawamoto // J Appl. Phys. 83, 3920 (1998).
2. Dantelle, G. / G. Dantelle, M. Mortier, G. Patriarche, D. Vivien // J Solid State Chem. 179, 1995 (2006).
3. Qiao, X. / X. Qiao, X. Fan, M. Wang, 3. Zhang // Opt. Mater. 27, 597 (2004).

УДК 681

СТЕГАНОГРАФИЯ В ПОМЕХОУСТОЙЧИВЫХ КОДАХ

Слипенчук П.В.
Московский государственный университет им. Н.Э.Баумана
Москва, Российская Федерация

Стеганография – это искусство и наука передавать сообщения различными способами так, чтобы не было обнаружено наличие самого сообщения. Стеганография может быть применима для реализации трёх целей: скрытой передачи данных (СПД), цифровых отпечатков (ЦО) и стеганографических водяных знаков (СВЗ)[12].

В данной работе мы будем использовать следующие основные определения из области стеганографии (см [1]):

Сообщение*(или стегосообщение) – передаваемая (или хранимая) скрытая информация.*

Контейнер *– любая информация, используемая для сокрытия сообщения.*

Пустой контейнер *– контейнер, не содержащий сообщения.*

Заполненный контейнер *(стегоконтейнер) – контейнер, содержащий сообщение.*

Ключ *(стегоключ) – секретный параметр, необходимый для сокрытия сообщения в контейнере.*

Стеганографический канал *(стегоканал) – канал передачи стегоконтейнера.*

Под ***стеганографической системой*** (стегосистемой) мы будем подразумевать программную, аппаратную или программно-аппаратную систему, пригодную для организации скрытого канала передачи информации. Аналогично криптографическому принципу Кирхгофа, будем считать, что третья сторона точно знает алгоритм работы стеганографической системы. Неизвестным для третьей стороны остаётся только секретный ключ(стегоключ), с помощью которого можно узнать о факте существования и о содержании сообщения.

Таким образом, при проектировании стеганографической системы надо руководствоваться следующими принципами:

а) без знания стегоключа, третьей стороне должно быть затруднительно даже установить факт существования сообщения;

б) при обнаружении противником наличия скрытого сообщения он не должен иметь возможности извлечь сообщение до тех пор, пока не будет владеть ключом.

Задача стегоанализа сводится к следующим подзадачам: обнаружение факта наличия сообщения и извлечение сообщения из заполненного контейнера.

Общая модель стеганографии в помехоустойчивых кодах. В общем случае есть блок, состоящий из букв какого-либо алфавита (например из {0,1}). Размеры блока **n** на **m**. С помощью помехоустойчивого кода **A** мы преобразуем блок размера **n** на **m** в блок, размера **n+n1** на **m+m1**.(см. рис. 1) В частном случае **m=m+m1=1**.

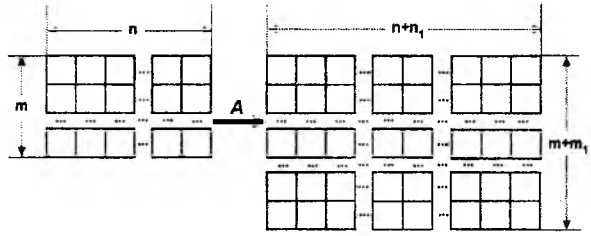

Рисунок 1

Блок, подаваемый на вход алгоритма, будем называть ***информационной матрицей***[10], а выход алгоритма **A** будем называть ***кодовой матрицей***[10]. Код исправляющий ошибки может быть создан для исправления одиночных и/или пакетных ошибок. Кодовая матрица подаётся в канал с шумом, принимается второй стороной и декодируется в исходную информационную матрицу.

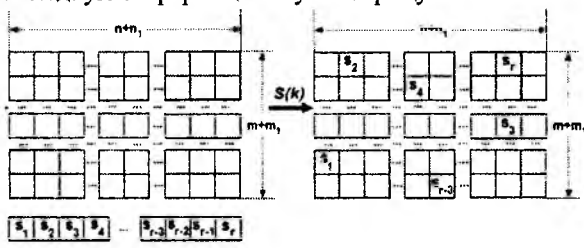

Рисунок 2

Предположим, что нам известно распределение ошибок в канале. Анализируя данное конкретное распределение, можно построить алгоритм **S**, зависящий в общем случае

от стегоключа **k**, который принимает на вход *кодовую матрицу* (*пустой контейнер*) и *сообщение*, а на выходе даёт *стегоконтейнер* в виде исходной кодовой матрицы с "вкрапленными" на определённых позициях битами сообщения. (см рис 2.)

Затем *стегоконтейнер* передаётся по каналу с шумом. Очевидно, что распределение возможных ошибок изменится по отношению к распределению ошибок при передачи по каналу *пустого контейнера*. При данной системе стеганографии необходимо соблюдать два условия:

1. после "вкрапления" стегосообщения и прохождения стегоконтейнера через канал с шумом, необходимо, чтобы вероятность ошибки декодирования была по прежнему крайне низкой;
2. распределение ошибок для стегоконтейнера должно быть максимально приближенным к распределению ошибок в пустом контейнере.

Первое условие необходимо для правильного восстановления исходной информационной матрицы. Второе – для уменьшения "подозрительности" контейнера на наличие скрытого сообщения. Очевидно, что чем меньше байт затирает **S(k)**, тем два распределения ближе друг к другу, но тем меньше объём скрываемой информации.

Модель "трёх каналов". В общей модели (см II) был рассмотрен один канал с шумом. По нему проходил и пустой контейнер и стегоконтейнер. Очевидно, что распределения ошибок для стегоконтейнера и для пустого контейнера при сообщении ненулевой длины должны быть разными. Если это допустить, то стеганография будет нестойкой.

Рассмотрим модель «трёх каналов»[11].

Пусть даны два канала с шумом: C_1 и C_2, при этом ошибок в C_2 в среднем меньше, чем в C_1, если через данный канал (C_2) не передавать сообщения. Допустим, что стегоконтейнер будет проходить через канал с шумом C_2, а пустой контейнер через канал с шумом C_1. Пусть **S** – стегосистема, вкрапляющая сообщение определённой длины в пустой контейнер. Пусть R_1 – распределение ошибок пустого контейнера, проходящего через канал C_1, а R_2 – распределение ошибок стегоконтейнера, проходящего через канал C_2.

Стегосистему **S** назовём ***идеальной стегосистемой*** (в кодах, исправляющих ошибки) для канала C_2 по отношению к каналу C_1, если распределения R_1 и R_2 совпадут.

Рассмотрим теперь следующую схему передачи сообщения (см рис.3): Алиса передаёт Бобу серию стегоконтейнеров. В общем случае Алиса берёт информационную матрицу **α**, подаёт на вход кодеру **A**. Затем, с помощью стегоалгоритма **S** и ключа **k**, создаёт стегоконтейнер, положив в него некое сообщение **s**. Этот стегоконтейнер проходит через два канала с шумом: C_2 и C_3 (в частном случае канал C_3 – канал без шума). Боб принимает стегоконтейнер, с помощью ключа **k**, извлекает стегосообщение **s**. Алёна передаёт Борису пустые контейнеры. Они и не думают с помощью стеганографических алгоритмов передавать скрытые сообщения. Иванов – третья сторона. Его задачи: 1)обнаружить, передаётся ли в контейнере скрытое сообщение; 2) если передаётся, то извлечь скрытое сообщение.

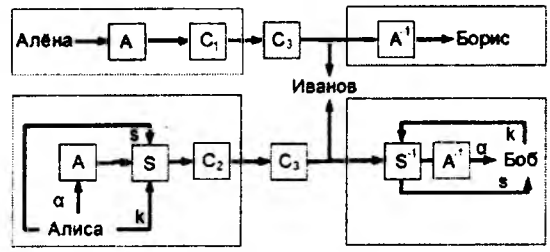

Рисунок 3

В качестве примера каналов можно привести процесс записи информации на компакт диск (Compact Disc, CD). Запись на него разным оборудованием с разной скоростью – это каналы C_1 и C_2. Передача диска или хранение на складе – это C_3. В первом случае C_3 – канал без шума, во втором, при долгом и/или неправильном сроке хранения – канал с шумом.

Предположим, что: 1) передаётся серия стего- контейнеров. (т.е. их количество существенно больше, чем один); 2)Иванов не знает не только ключа **k**, но и алгоритма **S**; 3) Иванов знает распределение ошибок каналов C_1 и C_3. 4)Иванов может прослушивать сообщения после прохождения в канале C_3.

Поскольку Иванов может прослушивать сообщения канала C_3, то при большом количестве передаваемых сообщений Иванов может вычислить распределение ошибок контейнеров от Алисы к Бобу и от Алёны к Борису. Распределения ошибок контейнеров от Алёны к Борису должны совпасть с теоретическими, т. к. они передают пустые контейнеры через каналы C_1 и C_3, распределение ошибок которых знает Иванов. Если у Алисы *неидеальная* система для канала C_2 по отношению к каналу C_1, то распределения ошибок контейнеров от Алисы к Бобу не совпадут. Чем "более существенно" отличаются распределения между C_2 и C_1, тем больше вероятность корректного распознавания стегоконтейнера из множества контейнеров. Таким образом, Иванов может решить первую проблему стегоанализа. Однако для извлечения сообщения необходимо знать алгоритм **S**.

Заметим также, что каналы C_1 и C_2 могут быть более сложными, чем симметрический канал с шумом. Например, рассматриваемые каналы могут быть каналами с пакетами ошибок. В данном случае, Иванову мало знать распределение ошибок, он должен так же

учитывать распределение вероятностей длин пакетных ошибок.

В работе Кристиана Кошена [2] даётся определение *совершенно секретной* системы. В одной из наших работ есть доказательство того, что *идеальная* система в модели трёх каналов является частным случаем совершенно секретной системы. Таким образом если мы построим идеальную стегосистему, то данная стегосистема будет являться совершенно секретной.

Стеганография в кодах, исправляющих ошибки, на оптических дисках CD, DVD, BD, HVD. В качестве примера для реализации стеганографии в кодах, исправляющих ошибки, нами были подробно изучены стандарты оптических дисков CD, DVD, BD, HVD [3,4,5,6,7]. Помехоустойчивые коды во всех четырёх популярных форматах оптических дисков основаны на кодах Рида-Соломона. Нами была найдена избыточность исправляющих кодов (Error Correction Codes, ECC) и разработаны алгоритмы стеганографии для каждого типа диска.

Оптический диск	Объём диска для пользовательских данных (не считая ECC)	Объём данных для ECC	Избыточность (в %)
CD	700 Мб	112 Мб	16,1%
DVD	4 Гб	155 Мб	3,85%
BD	25 Гб	3,22 Гб	12,9%
HVD	600 Гб	57,7 Гб	9,64%

Причины выбора оптических дисков для практических исследований обусловлено рядом причин.

Во-первых: Ввиду того, что производители оптических дисков и оптических приводов вынуждены разработать общие протоколы записи/чтения, стандарты по оптическим дискам в которых дано описание используемых помехоустойчивых кодов [3,4,5,6,7], в основном, общедоступны; что нельзя сказать, например, о USB-накопителях информации, SSD и HDD.

Во-вторых: реализация стеганографии для оптических накопителях имеет практическую пользу как в коммерческой сфере (лицензионная защита) так и в военной (скрытая передача данных), в отличие, например, от беспроводных сетей передачи данных, в которых также используются помехоустойчивые коды.

В-третьих: оптические диски и оптические приводы относительно доступны; существует огромное количество программных продуктов для работы с оптическими приводами. Данными качествами, к сожалению, не обладает другой перспективный контейнер для стеганографии – спутниковая связь, в которой реализовано помехоустойчивое кодирование на основе кодов Рида-Малера[8].

Правда, не смотря на хорошую документацию, на доступность оптических накопителей, на бесчисленное множество open sourse проектов, посвящённые процессу записи на оптические диски, существует ряд технологических трудностей. Например в стандарте MMC6, нет SCSI команды для чтения блоков помехоустойчивых кодов для DVD, BD и HVD[9]. Поэтому вести практические исследования без создания специального оборудования (или без знания недкларированных возможностей оптического привода) возможно только для CD дисков.

Реализация стеганографии. Беря заведомо более качественный оптический диск, записывая на него информацию более медленно, мы можем провести статистический расчёт ошибок на данном диске и найти вероятности P_i' для него. Количество ошибок каждой длины происходит на качественном диске меньше чем на среднестатистическом. Зная разницу $(P_i' - P_i)$ можно свести её к нулю, добавляя к ***подлинным*** ошибкам ***искусственные,*** которые и содержат скрытые данные. Таким образом мы получим канал C_2. В силу одинакового распределения ошибок мы получим *идеальную систему*, а значит и *совершенно секретную*, так как идеальная система является частным случаем совершенно секретной.

Заключение

В процессе построения совершенно секретной системы мы считаем математическую модель адекватной. Если по каким-либо причинам противник сможет разработать более адекватную модель и в рамках данной математической модели каналы C_1 и C_2 будут иметь различные распределения, то противник осуществит взлом стегосистемы. Таким образом рассмотренная выше стеганографическая система всегда является совершенно секретной только в рамках построенной математической модели возникновения ошибок.

Математический аппарат и принцип «трёх каналов» может быть успешно применен не только для реализации стеганографии на CD, но и для других носителей информации и каналов передачи данных, использующие помехоустойчивые коды. Это может быть: USB-накопитель, SSD, HDD, Wi-Fi и иные беспроводные сети, спутниковая связь и т. д.

1. Pfitzmann B. Information Hiding Terminology. Results of an informal plenary meeting and additional proposals // Springer Lecture Notes in Computer Science. – 1996. – v.1174. – P.347-350.
2. Christian Cachin. An Information-Theoretic Mo del for Steganography // MIT Laboratory for Computer Science - 2002. Edition. – October,2010. – P.31
3. International Standard ECMA-338. 80 mm (1,46 Gbytes per side) and 120 mm (4,70 Gbytes per

side) DVD Re-recordable Disk (DVD-RW). – December 2002.
4. Standard Blu-ray Disk Format: 1.B Physical Format Specifications for BD-R. 5th Edition. – October,2010.
5. Standard Blu-ray Disk Format: 1.A Physical Format Specifications for BD-RE. 3Rd Edition. – October,2010.
6. International Standard ECMA-378. Information Interchange on Read-Only Memory Holographic Versatile Disc (HVD-ROM) - Capacity 100 Gbytes per disk. 1st Edition. – May,2007.
7. International Standard ECMA-377. Information Interchange on Holographic Versatile Disc (HVD) Recordable Cartridges – Capacity: 200 Gbytes per Cartridge. 1st Edition. – May,2007.
8. European Telecommunications Standards Institute. Digital Video Broadcasting(DVB) Framing structure, channel coding and modulation
9. The INCITS T10 Technical Committee. Information Technology – Multi-Media Commands - 6 (MMC-6), Revision 2, 9 July 2008
10. Слипенчук П.В. Стеганография в кодах, исправляющих ошибки // М.: Вестник МГТУ, Специальный Выпуск №5, 2013.
11. Слипенчук П.В. Простое построение совершенных стегосистем на основе различных ошибок в помехоустойчивых кодах в модели трёх каналов. // М.: Вестник МГТУ, Специальный Выпуск (в печати)
12. Слипенчук П.В. Перспективы и практическое применение стеганографии в помехоустойчивых кодах. // М.: ВНИИ ПВТИ, журнал БИТ, № 3, 2013

УДК 629.783

ВЛИЯНИЕ ВОЗДЕЙСТВИЯ ВНЕШНИХ ФАКТОРОВ НА МИКРОСПУТНИК ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Старосотников Н.О., Фёдорцев Р.В.
Белорусский национальный технический университет,
Минск, Республика Беларусь

Мировой и в частности российский рынки в области разработки космической техники по дистанционному зондированию Земли (ДЗЗ) продолжают развиваться быстрыми темпами: приблизительно на 10 – 20 % в год [1]. На данный момент прослеживаются следующие тенденции ДЗЗ:

• увеличение относительного количества малоразмерных КА (малых, мини и микроспутников (МК));

• непрерывное возрастание уровня детализации объектов на космических снимках (пространственное разрешение до 0,5-1 м);

• начало интенсивного освоения микро/нано-технологий и создания больших космических систем из микро- и нано-спутников;

• неуклонное расширение состава исследовательских КА ДЗЗ и космических экспериментальных программ, направленных на научное изучение Земли и отработку новых методов и приборов ДЗЗ;

• активные организационные усилия ведущих космических держав по началу формирования космических систем глобального наблюдения Земли в рамках международного сотрудничества.

МК ДЗЗ относительно просты в разработке, обладают низкой себестоимостью производства, что ведёт к снижению риска больших потерь из-за неудачных запусков ракетоносителей, кроме того МК дают возможность создать многоспутниковую систему, предоставляющую информацию в реальном масштабе времени и др.

В процессе эксплуатации МК подвергается воздействию различных внешних факторов, которые оказывают значительное влияние на его работу:

• при выведении на орбиту: вибрации, ударные и линейные перегрузки, нагрев, акустический шум;

• во время орбитального полёта: космический вакуум, высокие и низкие температуры, электромагнитные излучения, корпускулярные потоки, микрометеориты, невесомость и др. [2].

Механическое воздействие проявляется в возникновении силы, способной привести к разрушению конструкции. К механическим факторам относятся [2]:

• акустические шумы;

• линейные и центробежные перегрузки (тяга двигателей, инерционные нагрузки, аэродинамические силы, такелажные и транспортные операции);

• удары (срабатывание пиротехнических элементов при отделении отработавших ступеней ракетоносителя);

• вибрации (пульсации тяги и колебаний компонентов топлива в трубопроводах).

Климатические факторы характеризуются температурой, относительной влажностью, наличием агрессивной среды и давлением. Источниками тепловой энергии являются тепловое излу-