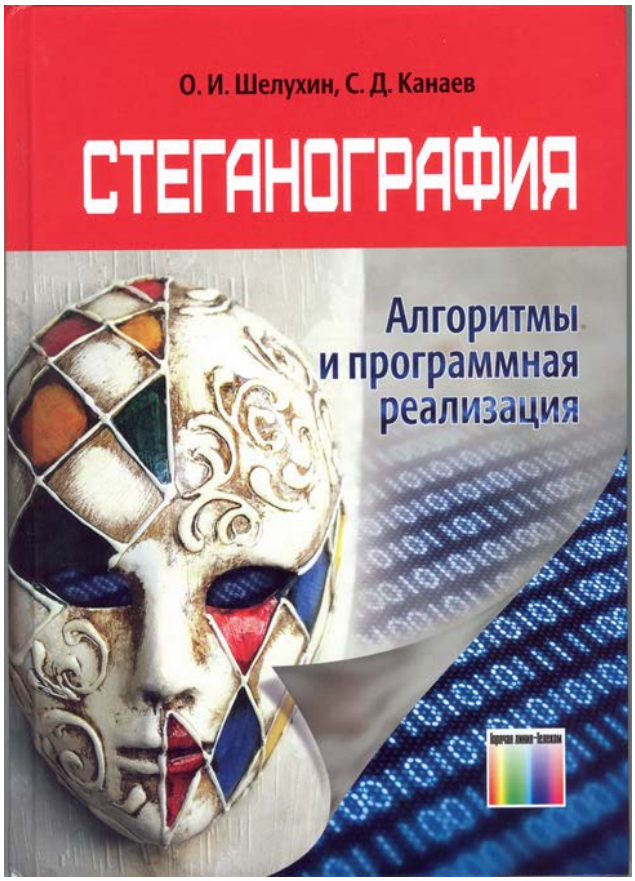
МНЕНИЕ ЭКСПЕРТА

РЕЦЕНЗИЯ НА КНИГУ «СТЕГАНОГРАФИЯ. АЛГОРИТМЫ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ»

(авторы: О.И. ШЕЛУХИН, С.Д. КАНАЕВ)



Книга позиционируется авторами как учебное пособие для студентов, обучающихся по направлению «Информационные технологии и системы связи», хотя «Стеганография» является частью «Информационной безопасности», т. е. соответствует скорее специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Авторы данного труда О.И. Шелухин и С.Д. Канаев не известны своими научными работами в области стеганографии как в России, так и тем более за рубежом. В огромном списке литературы, содержащемся в пособии, есть только две ссылки на работы авторов, причем одна из них – также учебное пособие, а вторая – в достаточно общем по тематике журнале «Спецтехника и связь». Поэтому надо признать, что авторы книги не являются специалистами в области стеганографии и тем более никогда не отмечались на различных международных форумах, хотя таких по этому направлению великое множество.

Как говорил в своих «Беседах об уме» Гельвеций, «он был не собственником, а лишь арендатором науки, которую преподавал, потому что в ней ему не принадлежало и клочка». Авторы пособия, очевидно, является специалистами в области программирования, о чем свидетельствуют и различные программы по построению случайно выбранных стегосистем. Поэтому можно заключить, что предлагаемый материал являются скорее пособием по построению компьютерных программ, в значительной степени заимствованных из Mathlab, но не пособием по практическому применению стеганографии.

Хотя японский писатель Кобо Абэ и дал определение, что «программирование является превращением реальности качественной в реальность количественную», но качественная реальность также требует своего пояснения. На протяжении почти всей книги чаще всего употребляется слово «современная стеганография» (далее – СГ), «современный стегоанализ» и т. п., однако по существу в ней не изложено ни одного современного, скрытного метода построения стегосистемы. Это относится и к списку литературы, где основные публикации, особенно зарубежные, датируются не позднее чем 2010 годом.

В предисловии к книге авторы в качестве ее преимущества приводят «не перенагруженность математическими выкладками». По этому поводу следует заметить, что, вообще говоря, математика в точных науках служит не для усложнения понимания материала, а для доказательства правильности утверждений и используется там, где без них нельзя обойтись. Иначе все это описание выглядит как беллетристика.

Прежде чем обратиться к рецензированию глав пособия, отметим, что используемый часто по тексту термин «контейнер» не нашел широкого употребления в зарубежной литературе (см., например, основополагающую монографию [1], где он вообще не используется). И действительно, «контейнер», в обычном обиходе это некая емкость,

всегда предназначенная для ее заполнения. Тогда как объекты, рассматриваемые в стеганографии, могут и не иметь отношения к процедуре вложения в них дополнительной информации. Поэтому более уместным представляется термин «покрывающий объект» (cover object [1]).

Наконец, существенным методическим недостатком книги является то, что в ней отсутствует четкое разделение «стеганографии в широком смысле» (information hiding – в зарубежной терминологии) на два класса: «стеганография в узком смысле» (или просто – «стеганография» – СГ) и «цифровые водяные знаки» (ЦВЗ). Эти два класса имеют часто похожие методы вложения и извлечения, но различные основные атаки на них; в первом случае основной атакой является обнаружение присутствия стеговложения в анализируемом объекте, а во втором – устойчивость к атакам по удалению ЦВЗ без значительного искажения основного покрывающего объекта. Заметим, что понимание этого факта значительно упрощает изложение курсов по стеганографии.

Приступим далее к рецензированию всех глав книги.

Глава 1. «Стеганография: основные положения»

В этой главе основные положения стеганографии сформулированы верно, однако не подчеркнуто наиболее важное обстоятельство – при вложении дополнительной (секретной) информации не должно быть заметного искажения содержания покрывающего объекта («контейнера» – в терминологии авторов). Иначе, задача решалась бы тривиально.

Таблица 1.1 (в книге – «Сопоставительный анализ методов КС»), хотя и не противоречит некоторым используемым методам стеганографии, но не охватывает всей совокупности таких методов; при этом классификация производится по довольно произвольным критериям авторов, тогда как более типично классифицировать методы по видам покрывающих объектов.

Определение 1 (в книге – «Стеганография – это…») нестрого. *Определение 2 (в книге – «Контейнером …называют…»),* – просто неверно. Секретность СГ определена расплывчато и лишь качественно. Общая модель стегосистемы похожа на «индексологию», т.е. не имеет содержательного наполнения и включает лишь пустые обозначения. *Таблица 1.3 (в книге – «Формализация объектов, предметов на уровне ЭМВ СС»)* выглядит как типичная индексология.

В *разделе 1.7 (в книге – «Цифровые водяные знаки»)* правильно отмечено назначение цифровых водяных знаков. Однако, далее идут откровенные неточности («изменение ЦВЗ не доступно даже их автору») и «ляпы» (модуляция информации выполняется лишь двумя способами – шумоподавлением и квантованием). В действительности таких методов десятки (если не больше) – (см. [1], [2], [4] и др.).

Раздел 1.8 (в книге – «Принципы внедрения и извлечения водяных знаков»), и раздел *1.9 (в книге – «Модели внедрения водяных знаков в виде телекоммуникационной системы»),* представляют собой наивные разговоры авторов, основанные на популярном материале и на их первичных размышлениях, где ничего не доказывается, а все лишь постулируется. Кроме того, этот материал должен быть размещен ниже, где описываются конкретные системы СГ и ЦВЗ.

В *разделе 1.11 (в книге – «Оценка качества стеганосистемы»)* не введена количественная характеристика обнаруживаемости СГ. Описание стегоанализа в *разделе 1.12 (в книге – «Стеганоанализ»),* примитивно и не содержит даже предварительного описания современных методов. (см. [1], [3], [4] и др.). Список литературы к главе 1 содержит в основном устаревшие источники.

Глава 2. «Сокрытие информации в текстовых документах»

Глава 2 посвящена описанию известных авторам методам СГ для текстовых документов, которые в международной терминологии называются «лингвистическими стегосистемами».

Здесь алгоритм вложения и извлечения информации описан верно, хотя сама методика, когда описание метода начинается с программного модуля, а не с общего описания алгоритмов вложения и извлечения информации, представляется методически неверной.

В приведенном описании отсутствует наиболее эффективный метод лингвистической СГ, основанный на небольшой редакции текста (см., например [4]), а также ссылки на него в списке литературы к главе 2 рецензируемой книги). *Методы сетевой СГ*, хотя и весьма полезны, но они не имеют никакого отношения к заголовку главы 2 – «Сокрытие информации в текстовых документах».

Также нельзя не отметить, что имеет место неточность при составлении оглавления, в котором глава 2 именуется как «Скрытие информации в текстовых документах».

Глава 3. «Скрытие информации в аудиосигналах»

Приведенные здесь методы не вызывают возражений, однако принятый авторами подход с «засорением» текста программами, применяемый ими на начальном этапе, весьма затрудняет понимание для тех читателей, которые хотят понять сущность методов, а не просто выполнить проце-

дуру «paste and copy». Метод «эхо-кодирования» описан примитивно и без количественных оценок.

Вообще не описаны методы с модуляцией по частоте, а также наиболее перспективный метод с использованием реверберации. Это и понятно – ведь литература к главе 3 почти вся устаревшая.

Глава 4. «Скрытие информации в неподвижных изображениях»

Глава 4 посвящена наиболее актуальному применению СГ – вложению информации в неподвижные изображения (см. поясняющее замечание в [1]).

Авторы значительное внимание уделили весьма примитивному методу с заменой наименьших значащих бит. К данной главе приложен список литературы, состоящий из 110 названий, однако абсолютное большинство из них относится к…. *прошлому веку*.

Неудивительно поэтому, что в перспективные методы СГ для неподвижных изображений не вошли такие алгоритмы как: матричное вложение, адаптивное квантование, квантование с двойным сжатием, СГ с использованием заданной модели («model-based S6»), СГ на основе маскировки шумами сканера и, наконец, наиболее перспективный в настоящее время метод – с оценкой «стоимости» вложений, известной как проект «HUGO».

Текст данной главы читается также с большим трудом из-за отсутствия формулировки основных принципов оценки обнаруживаемости рассматриваемых методов, а также перегруженности программами, которые вполне могли бы быть вынесены в приложение к книге.

Глава 5. «Внедрение цифровых водяных знаков на основе вейвлет-преобразований»

Авторы описывают здесь, как используются вейвлет-преобразования для построения систем ЦВЗ.

Таблица 5.1 (в книге – «Классификация существующих алгоритмов внедрения водяного знака в вейвлет-домене») выглядит впечатляюще. Однако из текста главы не ясно – от каких атак по удалению ЦВЗ защищают упомянутые в таблице методы и как можно их использовать для обеспечения copyright. Вообще, конечно, методы с использованием вейвлет-преобразований все еще остается «модными» до настоящего времени. Однако надо было бы доказать, почему именно их использование обеспечивает определенные преимущества перед другими.

В этой части рецензируемой книги также наблюдается неточность при составлении оглавления: глава 5 именуется в тексте «Внедрение цифровых водяных знаков на основе вейвлет-преобразований», а в оглавлении «Внедрение водяных знаков на основе вейвлет-преобразований».

Глава 6. «Встраивание ЦВЗ в сжатые видеопоследовательности»

В Главе 6 рассматривается по существу ЦВЗ для видеосигналов, хотя четкое различие между СГ и ЦВЗ здесь не просматривается. Вообще следует отметить, что материал данной главы изложен значительно доступнее, чем в предыдущих главах, однако, он страдает прежним дефектом – отсутствием описания атак по удалению ЦВЗ (или обнаружению СГ) и оценки их эффективности.

Глава 7. «Стеганографический анализ»

Глава 7 посвящена стеганографическому анализу. Особых замечаний по этому материалу нет, так как он добросовестно списан из известных источников. Однако представляется, что описание стегоанализа должно сопровождаться каждым из рассмотренных ранее методов построения СГ, а не представляться в конце книги, так сказать «на десерт», поскольку любая СГ имеет право называться СГ тогда и только тогда, когда она устойчива, если не ко всем, то хотя бы к некоторым методам стегоанализа. Заметим, что из рассмотрения «выпали» такие важные методы стегоанализа, как побочные атаки (см. [3]).

В рецензируемой книге абсолютно не рассмотрен подход к построению СГ на основе сценария канала с шумом, хотя только этот подход обеспечивает построение идеальной (то есть необнаруживаемой СГ) – см. описание в ссылке [4], а также в многочисленных публикациях автора этой рецензии в отечественных и зарубежных изданиях [5-15].

Выводы

1) Материал рецензируемой книги не структурирован таким образом, чтобы он мог бы позволить читателю найти перспективные современные направления построения систем СГ и ЦВЗ.

2) Терминология, относящаяся к определению основных понятий СГ, не вполне соответствует международной терминологии в этой области.

3) В книге упущен ряд перспективных методов построения систем СГ, ЦВЗ, а также новых методов стегоанализа.

4) Рассмотрен большой набор методов вложения и извлечения систем СГ и ЦВЗ, что может предоставлять определенный интерес, особенно у читателей, интересующихся историей стеганографии. Однако даже среди предоставленных методов нет рекомендаций по предпочтительному выбору некоторых из них.

5) Смешения описания алгоритмов построения стегосистем и программ вызывает методологиче-

ские трудности, если не позиционировать данную книгу как пособие для тренировки программистов.

6) Рецензируемая книга не представляет собой ни научную монографию (тут нет новых результатов авторов), ни учебник (материал изложен недостаточно систематично и доступно для понимания) или даже справочник (поскольку книга не структурирована должным образом). Однако она может содержать полезный материал по примерам построения различных систем СГ и ЦВЗ, особенно для тех читателей, которые не имеют доступа к Интернету или затрудняются с переводом книг и статей с английского языка.

В.И. Коржик,
доктор технических наук,
почетный профессор СПбГУТ,
заслуженный работник высшей школы РФ,
член IEEE on IT

Список используемых источников

1. Fridrich Y. Steganography in Digital Media: Principles, Algorithms and Applicaticks. Cambridge Press, 2010. 462 p.
2. Cox I. et al. Digital watermarking. МК, 2002.
3. Korzhik V. et al. Steganalysis Based on Statistical Properties of the Encrypted Messages // Computer Network Security. 7-th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security: Lecture Notes in Computer Science. 2017. Vol. 10446. PP. 288-298.
4. Коржик В.И. и др. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стенография. СПб.: СПбГУТ, 2016. 225 с.
5. Коржик В.И. и др. Цифровая стеганография и цифровые водяные знаки. Часть 2. Цифровые водяные знаки. СПб.: СПбГУТ, 2017. 198 с.
6. Korzhik V. On the Use of Bhattacharyya Distance as a Measure of the Detectability of Steganographic Systems // Transaction on Data Hiding and Multimedia Security III: Lecture Notes in Computer Science. 2008. Vol. 4920. PP. 23-32.
7. Korzhik V. Undetectable Spread-Time Stegosystem Based on Noisy Channels // International Journal of Computer Science and Applications, Special Issue on Multimedia Application. 2011. Vol. VIII. Iss. 1.
8. Korzhik V., Morales-Luna G., Nebaeva K. Capacity of a Stegosystem for the Noisy Attack Channel // International Journal of Information Hiding. 2012. Vol. 3 No. 2. PP. 205-211.
9. Korzhik V., Morales-Luna G. Information hiding through Noisy Channels // Information Hiding: Lecture Notes in Computer Science. 2001. Vol. 2137. PP. 42-50.
10. Korzhik V., Morales-Luna G., Lee M.H. On the Existence of Perfect Stegosystems // IWDW: Lecture Notes in Computer Science. Vol. 3710. PP. 30-37.
11. Korzhik V., Morales-Luna G., Lee M.H. Stegosystems Based on Noisy Channels // Proc. IX Spanish Meeting on Cryptology and Information Security. 2006. PP. 379-387.
12. Korzhik V., Morales-Luna G. Undetectable Spread-Time Stegosystem Based on Noisy Channels // Proc. of International Multiconference on Computer Science and Information Technology. 2010. PP. 723-728.
13. Коржик В.И., Небаева К.А., Алексеевс М. Использование модели канала с шумом для построения стегосистемы // Телекоммуникации. 2013. Спецвыпуск. С. 33–36.