ПРИМЕНЕНИЕ МЕТОДА «CHIP-OFF» В КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

С.В. Дуга[1], А.Г. Себякин [1], А.И.Труфанов[2], О.Г.Берестнева[3], А.А.Тихомиров[4],
[1](г. Иркутск, Следственное управление Следственного комитета Российской Федерации по Иркутской области)
e-mail: siber@list.ru, quattro.sa@yandex.ru
[2](г. Иркутск, Иркутский Национальный исследовательский технический университет)
e-mail: troufan@gmail.com
[3](г. Томск, Томский политехнический университет)
e-mail: ogb6@yandex.ru
[4](г. Инчеон, РК, Университет Инха)

USING THE «CHIP-OFF» METHOD IN COMPUTER FORENSICS

S.V. Duga[1], A.G. Sebyakin[1], A.I.Trufanov[2], O.G.Berestneva[3], A.A.Tikhomirov[4]
[1](Irkutsk, Investigative Committee of the Russian Federation, Irkutsk Region)
[2](Irkutsk, Irkutsk National Research Technical University)
[3](Tomsk, Tomsk Polytechnic University)
[4] (Incheon, RK, Inha University)

Abstract. This article discusses contemporary techniques of information extraction from mobile phones as sources of important forensic information. Particular attention is paid to the method based on direct access to memory chips (chip-off). Pertinent hardware and software available on units of the Investigative Committee of the Russian Federation and used for chip-off application are presented, as well as the corresponding experiences.

Keywords: *digital forensics, mobile data, data extraction, analyzing data, mobile forensics, chip-off*

В статье рассматриваются существующие методы извлечения информации из мобильных телефонов, как источника важных криминалистически значимых сведений. Особое внимание уделено способу извлечения информационного содержимого мобильных телефонов путем прямого доступа к микросхеме памяти (chip-off). Приведены имеющиеся в подразделениях Следственного комитета Российской Федерации программно-аппаратные средства, используемые при применении способа chip-off, а также опыт их применения.

Введение. Согласно данным аналитического агентства «We Are Social» [1], по состоянию на январь 2018 года, уникальных мобильных пользователей в России насчитывалось 114,2 миллионов (при этом рост составил 3% с января 2017 года). Отметим, что криминалистическую значимость информации, полученную из исследований мобильных устройств, сложно переоценить. Значимость экспертизы данных устройств отмечается как в зарубежных исследованиях [2], [3], [4], [5],так и в отечественных [6], [7], [8], [9].

В частности, в [10] отмечается, что электронные следы - различные виды компьютерной информации, содержащейся на электронных носителях, - все чаще используются в качестве доказательств по уголовным делам о преступлениях различных видов. Наиболее важное место среди них занимают мобильные устройства как по частоте встречаемости, так и по количеству и информативности сведений, имеющих значение для уголовного дела.

Это подтверждается и исследованием практики применения универсального программно-аппаратного комплекса «UFED» (используется для осмотра информационного содержимого мобильных устройств) в территориальных следственных подразделениях Следственного комитета Российской Федерации, показавшее, что в 87 % случаев была получена криминалистически значимая информация, которая способствовала раскрытию и расследованию преступлений [11].

В криминалистическом исследовании мобильных телефонов принято выделять пять методов извлечения информации, в зависимости от сложности применения каждого из них [12].

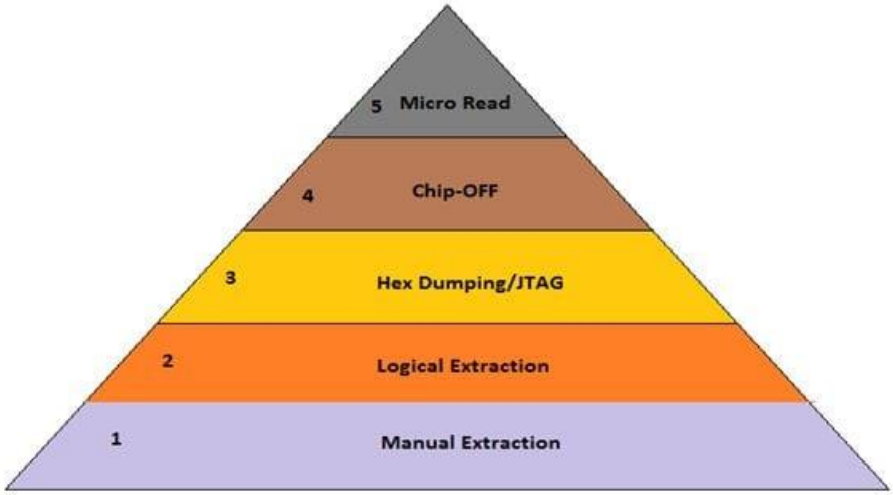

Рис. 1. Методы получения данных с мобильных телефонов.

Ниже приведем описание методов (уровней) извлечения информации, в соответствии с [13] (рис.1):

- ручное извлечение данных (manual extraction). Данный метод подразумевает обеспечение доступа к компьютерной информации, имеющейся в памяти мобильного устройства, посредством его клавиатуры или сенсорного экрана. Обнаруженная в ходе исследования информация документируется путем фотосъемки экрана телефона или планшета. Данные метод является наиболее простым и подходит для любого устройства. Важно отметить, что на данном уровне невозможно получить все данные, а также произвести восстановление удаленных файлов и записей;

- извлечение данных на логическом уровне (logical extraction). Данный метод подразумевает подключение мобильного устройства к рабочей станции эксперта посредством USB-кабеля, ИК-порта или «Bluetooth». После этого производится побитовое копирование файлов и каталогов, находящихся на логических дисках мобильного устройства. При этом используется интерфейс прикладного программирования, разработанный производителем и предназначенный для синхронизации телефона или планшета с персональным компьютером. Тем не менее, данный уровень извлечения данных также обеспечивает ограниченный доступ к компьютерной информации, и не позволяет восстановить удаленные данные. Исключением могут служить удаленные записи из баз данных SQLite, использование которых характерно для операционных систем iOS и Android. Стертые записи в указанных базах данных не перезаписываются сразу, а помечаются как «удаленные» до тех пор, пока место, занимаемое ими, не понадобится для записи новых данных. Также, на этом уровне возможно извлечение баз миниатюр, содержащих миниатюры графических и видео файлов, содержащихся в устройстве, в том числе, и удаленных файлов данных типов;

- извлечение данных на физическом уровне (hex dumping/JTAG). Этот метод подразумевает получение побитовой копии всей внутренней памяти мобильного устройства, что позволяет, в том числе, восстановить удаленные записи и файлы. Несмотря на привлекательность данного метода, осуществить извлечение данных на этом уровне представляется возможным далеко не всегда: производители зачастую ограничивают возможность чтения внутренней памяти мобильного устройства в целях обеспечения максимальной безопасности. Чтобы обойти данные ограничения, разработчики программного обеспечения для криминалистического исследования мобильных устройств разрабатывают собственные загрузчики, которые позволяют не только получить доступ к внутренней памяти, но и, иногда, обойти пароли, установленные пользователями;

- извлечение данных из интегральной схемы памяти (chip-off). Данный метод подразумевает извлечение данных непосредственно из интегральной схемы памяти мобильного

устройства. Интегральная схема извлекается из телефона или планшета и помещается в соответствующее устройство для чтения или аналогичное мобильное устройство. Использовать данный метод достаточно сложно, так как интегральные схемы памяти, применяемые в производстве мобильных устройств, весьма разнообразны. Преимуществом же извлечения данных на этом уровне является возможность получить компьютерную информацию даже из памяти неисправных мобильных устройств;

- извлечение данных на микроуровне (micro read). Данный процесс подразумевает изучение интегральной схемы памяти посредством электронного микроскопа и последующее преобразование полученных данных сначала в последовательность нулей и единиц, затем – ASCII-символы. Данный метод не нашел широкого применения ввиду его высокой стоимости и значительной сложности.

Метод. В данной работе представлялось разумным сосредоточиться на рассмотрении четвертого уровня (chip-off), как весьма эффективного, то есть на извлечении информационного содержимого мобильных телефонов путем прямого доступа к микросхеме памяти.

Сложившаяся в экспертных подразделениях СК России, и, как думается, не только в России, практика, свидетельствует о том, что исследование полностью или частично неисправных мобильных телефонов не такая уж и редкая задача.

Именно поэтому во вновь создаваемые экспертные подразделения СК России поставлялись специализированные программаторы и адаптеры, предназначенные для работы с неисправными мобильными телефонами.

Под частично неисправными мобильными телефонами мы понимаем устройство, часть узлов которого повреждена (что не позволяет извлечь информационное содержимое без применения специализированных программаторов), однако исправна системная плата и ее компоненты.

Под полностью неисправными мобильными телефонами мы понимаем устройство, у которого несправна системная плата, однако, для извлечения информационного содержимого, должна быть исправна микросхема памяти.

Метод извлечения информационного содержимого мобильных телефонов путем прямого доступа к микросхеме памяти является крайней мерой, когда иными способами извлечь информацию не представляется возможным. Это обусловлено сложностью процедуры извлечения и очистки микросхемы памяти. В любой момент существует опасность перегреть или механически повредить память, что повлечет утрату данных.

При всех своих недостатках данная технология позволяет извлекать информационное содержимое из неисправных мобильных телефонов, при этом другими методами извлечь информационное содержимое не представляется возможным, что подтверждено опытом использования специализированных программаторов и переходников в экспертно-криминалистическом отделе СУ СК России по Иркутской области.

Основные результаты. В ходе исследования, было успешно извлечено информационное содержимое неисправного мобильного телефона «ZTE BLADE A5 PRO» (рис. 2).

Рис. 2. Мобильный телефон «ZTE BLADE A5 PRO».

Для извлечения информационного содержимого мобильного телефона, была предварительно отделена микросхема памяти, которая затем подключалась к специализированному программатору «MEDUSA Pro» [14] через адаптер «MOORC E-Mate Pro eMMC» (рис. 3).

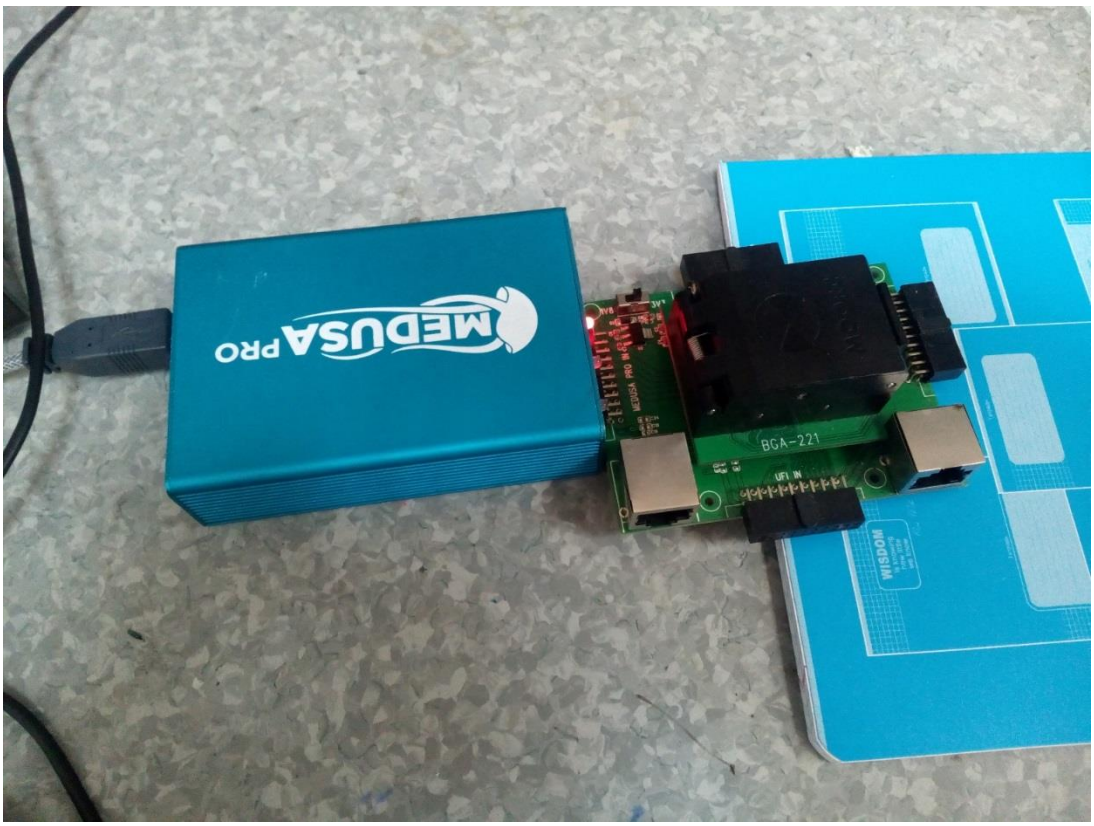

Рис. 3. Программатор «MEDUSA Pro» и адаптер «MOORC E-Mate Pro eMMC».

Далее, посредством программного обеспечения «Medusa Pro Software», создавался файл-образ информационного содержимого микросхемы памяти. После чего полученный файл-образ был проанализирован при помощи программного обеспечения «Мобильный криминалист» [15].

В ходе работы по извлечению информации, адаптер «MOORC E-Mate Pro eMMC» показал свою эффективность, а также удобство в обращении, так как для извлечения информационного содержимого микросхемы памяти с использованием данного адаптера не требуется восстановление шариковых выводов, а также пайка (рис. 4).

Рис. 4. Адаптер «MOORC E-Mate Pro eMMC».

Для использования специализированных адаптеров, имевшихся в экспертно-криминалистическом отделе СУ СК России по Иркутской области, требовалось восстановление шариковых выводов микросхемы памяти, а также ее пайка к адаптеру (рис. 5). При этом

микросхема памяти подвергается дополнительному термическому воздействию, что может повлечь выход ее из строя и, как следствие, потерю информации. Кроме того, контактные площадки адаптера от многократной перепайки могут повредиться, что приведет к выходу из строя всего адаптера.

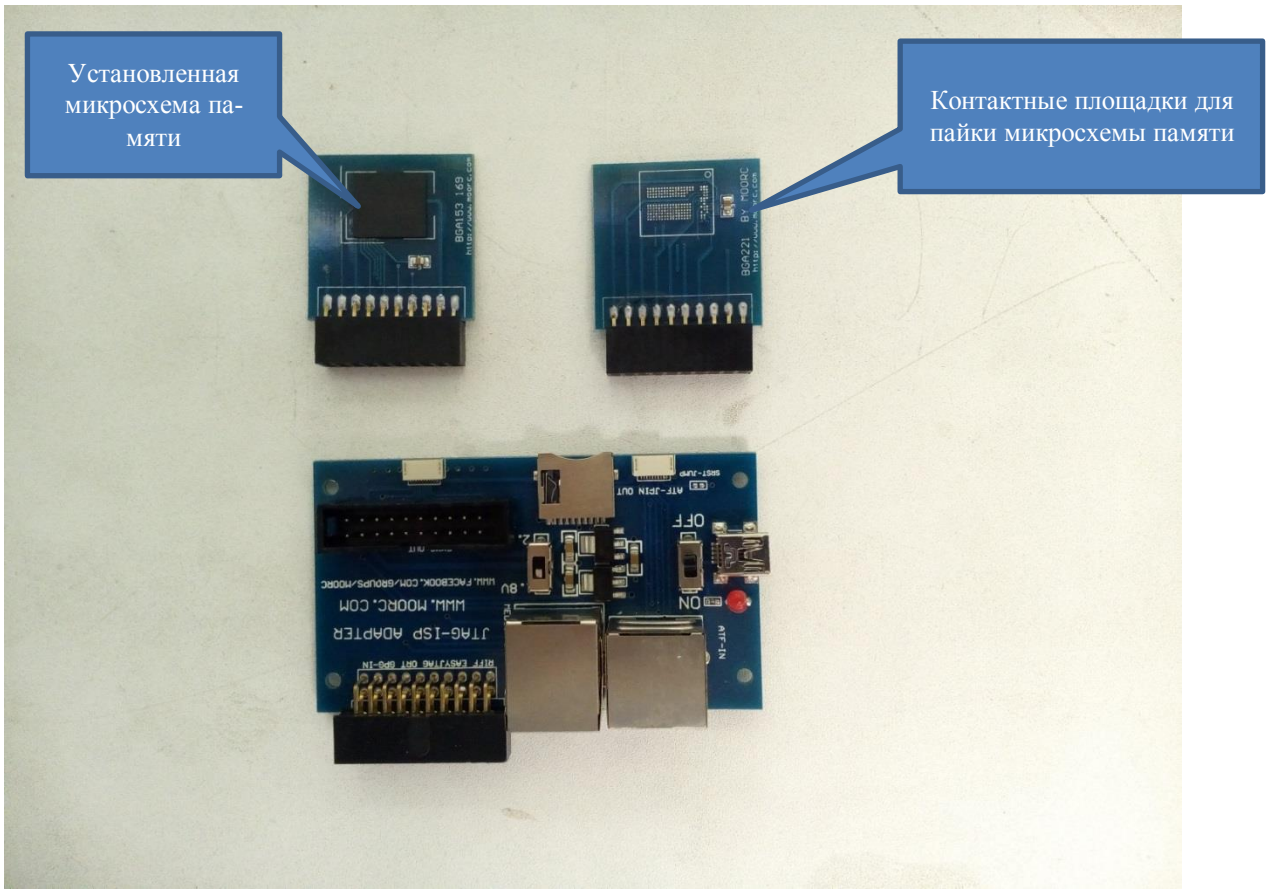

Рис. 5. Адаптер «JTAG-ISP ADAPTER».

Исходя из вышеуказанных технологических рисков в ЭКО СУ СК России по Иркутской области был приобретен специализированный адаптер «MOORC E-Mate Pro eMMC».

Кроме того известны случаи, когда при полностью исправном мобильном телефоне невозможно получить доступ к базам данных программного обеспечения для восстановления удаленных сведений.

Так, в ходе исследования мобильного телефона «Huawei Honor 5X (KIW-L21)», была поставлена задача по восстановлению ранее удаленных в мессенджере «WhatsApp» сообщений. При этом выяснилось, что получить полный доступ к файловой системе устройства, без потери пользовательских данных, не представляется возможным.

Поэтому была предпринята попытка извлечения информационного содержимого мобильного телефона другим методом - путем прямого доступа к микросхеме памяти.

Аналогично предыдущему случаю, из мобильного телефона была извлечена микросхема памяти, которая подключалась к специализированному программатору «MEDUSA Pro» через адаптер «MOORC E-Mate Pro eMMC», после чего посредством программного обеспечения «Medusa Pro Software» был создан файл-образ информационного содержимого микросхемы памяти.

Далее полученный файл-образ был проанализирован при помощи программного обеспечения «UFED Physical Analyzer» [16].

Для наглядности, на рис. 6 и 7, приведены результаты извлечения информационного содержимого мобильного телефона «Huawei Honor 5X (KIW-L21)» путем логического извле-

чения (рис. 6) и путем прямого доступа к микросхеме памяти (рис. 7). В первых скобках указано количество извлеченных записей. Во вторых скобках (при наличии) указано количество восстановленных после удаления записей.

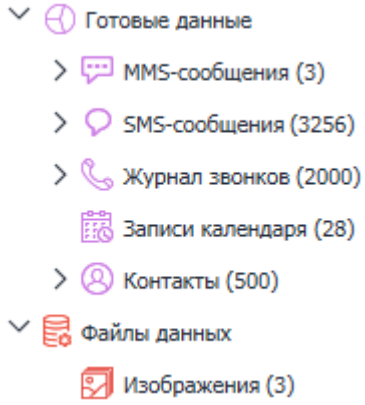

Рис. 6. Результаты извлечения информационного содержимого мобильного телефона «Huawei Honor 5X (KIW-L21)» путем логического извлечения.

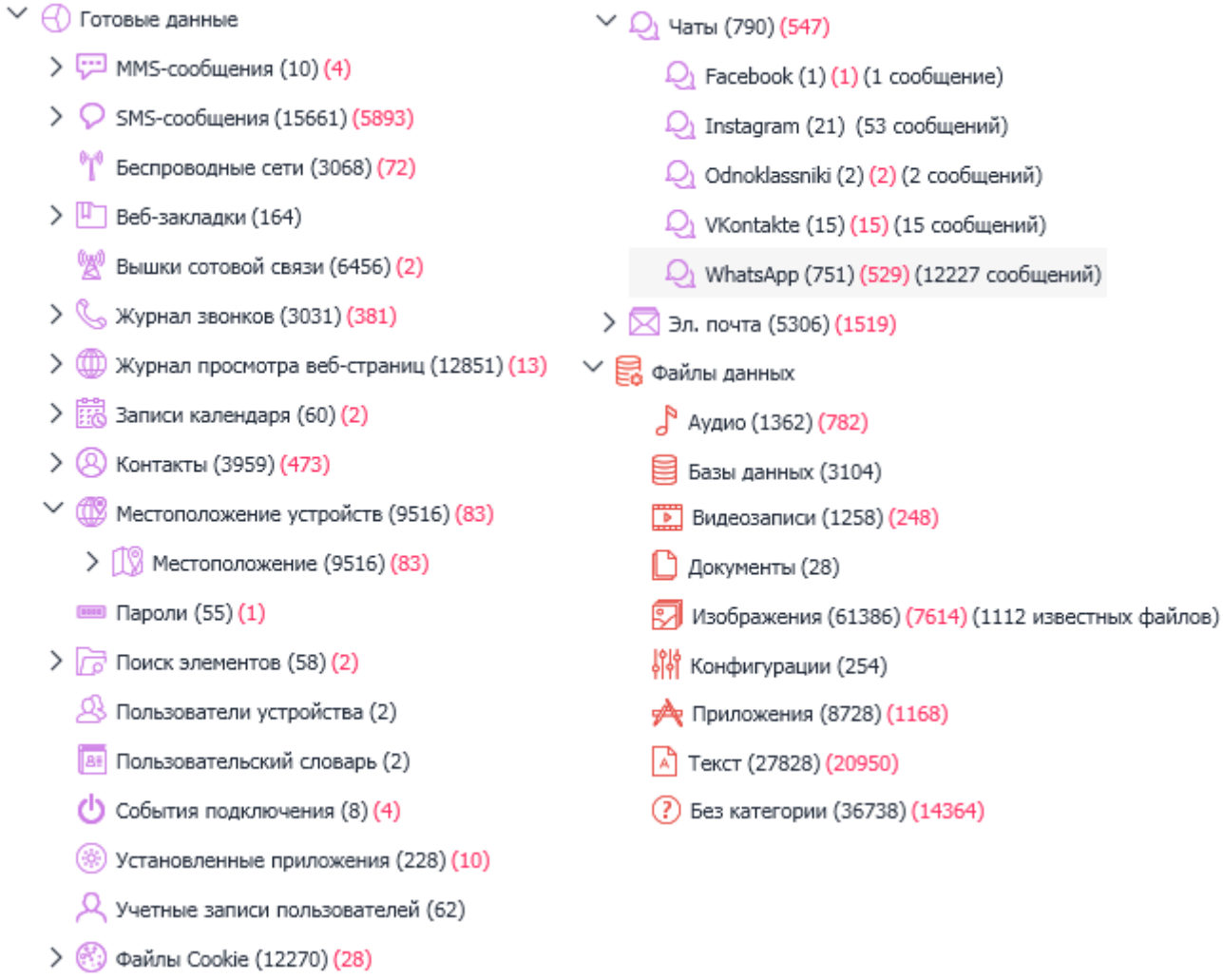

Рис. 7. Результаты извлечения информационного содержимого мобильного телефона «Huawei Honor 5X (KIW-L21)» путем прямого доступа к микросхеме памяти.

Выводы. Способ извлечения данных из интегральной схемы памяти (chip-off), показал высокую эффективность, когда иным способом извлечь информацию не представляется возможным. Однако, данный способ имеет ряд серьезных недостатком, в частности, опас-

ность повреждение микросхемы памяти в момент выпайки. Таким образом, применять «chip-off» следует в последнюю очередь, когда возможности иных способов были исчерпаны и не дали желаемый результат, или же их применение невозможно в принципе.

ЛИТЕРАТУРА

1. «We Are Social - Digital Report 2018,» [В Интернете]. Available: https://digitalreport.wearesocial.com/. [Дата обращения: 05 06 2019].
2. Ahmed R. и Dharaskar R. V., «Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective,» 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, pp. 312-23, 2008.
3. Dogan S. и Akbal E., «Analysis of mobile phones in digital forensics,» 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). – IEEE, pp. 1241-1244, 2017.
4. Binnar M. P. B., «An Forensic Case Study: Importance and Used of Multiple Tools in Recovery of Vital Evidences from Mobile Devices,» Asian Journal For Convergence In Technology (Founded by ISB &M School of Technology), 2018.
5. Raji M., Wimmer H. и Haddad R. J., «Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools,» SoutheastCon 2018. – IEEE, pp. 1-6, 2018.
6. Старичков М. В., «Устройства мобильной связи как источники криминалистической информации,» в Криминалистические чтения на Байкале-2015, 2015.
7. Бутенко О. С., «Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия,» Lex russica, т. 4 (113), 2016.
8. Платонов В. А., «Использование информационных технологий для получения доказательств по уголовному делу,» Вопросы науки и образования, № 10 (11), 2017.
9. Бутенко О. С. и Расчетов В. А., «Возможности изучения мобильных телефонов в рамках предварительного следствия,» Современные инновации: актуальные направления научных исследований, pp. 30-32, 2017.
10. В.Б. Вехов, «Использование компьютерных технологий в криминалистической деятельности и уголовном процессе,» ВЕСТНИК АКАДЕМИИ СЛЕДСТВЕННОГО КОМИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ, № 1, pp. 70-73, 2014.
11. Багмет А.М. и Скобелин С.Ю., «Особенности применения криминалистической техники для извлечения и анализа данных мобильных устройств,» в Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях: материалы международ. науч.-практич. конф. Тюмень: ТГАМЭУП, 2013.
12. Brothers S., «iPhone Tool Classification,» Retrieved on March. – 2007, т. 12, 2012.
13. «https://www.oxygensoftware.ru/ru/events/articles/640-osvovy-kriminalsticheskogo-issledovaniya-ustroistv,» [В Интернете]. Available: https://www.oxygensoftware.ru/ru/events/articles/640-osvovy-kriminalsticheskogo-issledovaniya-ustroistv. [Дата обращения: 05 06 2019].
14. «Medusa PRO Box - read/write boot, flash and repair LG, Samsung, HTC and other mobile phone brands,» [В Интернете]. Available: https://medusabox.com. [Дата обращения: 05 06 2019].

15.«Мобильный Криминалист - Российское ПО для криминалистической экспертизы устройств,» 05 06 2019. [В Интернете]. Available: https://www.oxygensoftware.ru/ru/.
16.«UFED Ultimate - Cellebrite,» [В Интернете]. Available: https://www.cellebrite.com/en/products/ufed-ultimate/. [Дата обращения: 05 06 2019].

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ ВСТРАИВАНИЯ ИНФОРМАЦИИ В ОБЛАСТЬ ДВП ЦИФРОВЫХ ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ МЕТОДА QIM К ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ И СТЕГОАНАЛИЗУ

О.О. Евсютин, А.С. Мельман, А.А. Филиппов, И.Д. Чернов
(г. Москва, Национальный исследовательский университет «Высшая школа экономики»)
(г. Томск, Томский государственный университет систем управления и радиоэлектроники)
e-mail: evsutin.oo@gmail.com, annakokurina94@yandex.ru, filippov.new.9898@mail.ru, chernoffilya1997@mail.ru

THE STUDY OF ROBUSTNESS OF INFORMATION EMBEDDING INTO DIGITAL IMAGES DWT DOMAIN USING QIM METHOD TO DESTRUCTIVE EFFECTS AND STEGANALYSIS

O. Evsutin, A. Melman, A. Filippov I. Chernov
(Moscow, National Research University «Higher School of Economics»)
(Tomsk, Tomsk State University of Control Systems and Radioelectronics)

Abstract. Steganography is one of effective solutions to ensure information confidentiality. For this purpose, secret information is embedded into a cover object, for example, a digital image. However, embedded data can be detected using steganalysis techniques. As a result, an attacker can apply destructive effects to the stego-image and destroy the embedded data to prevent their hidden transmission. Therefore, this paper presents a study of robustness of information embedding into digital images DWT domain using QIM method to destructive effects (JPEG compression, brightness change, etc.) and statistical stegoanalysis at the same time. The results will help to increase the efficiency of information embedding into DWT domain of digital images.

Key words: steganography, digital image, discrete wavelet transform, destructive effect, steganalysis.

Введение. В современном мире задача защиты конфиденциальности цифровых данных представляет особую важность. Одним из вариантов решения данной задачи является применение методов цифровой стеганографии – науки о скрытой передаче и хранении информации таким образом, чтобы сам факт её наличия был тайной для злоумышленника. При этом конфиденциальная информация встраивается в некоторые цифровые объекты, которыми могут быть мультимедиаданные (изображения, аудио- и видеофайлы), исполняемые файлы программ, сенсорные данные и многое другое. В частности, наибольшей популярностью при использовании в качестве контейнеров для дополнительной информации пользуются цифровые изображения, поскольку обмен различными картинками, фотографиями и другими графическими объектами в настоящее время широко распространён и является обычным делом. Однако популярность сокрытия данных в цифровых изображениях одновременно приводит и к развитию методов стегоанализа – науки об обнаружении стеганографических вложений. Даже в том случае, если у злоумышленника всего лишь возникнут подозрения о наличии в том или ином изображении встроенной информации, он может применить какое-либо деструктивное воздействие к стегоизображению, например, сжать или обрезать его, чтобы разрушить потенциальное вложение. А если наличие вложения будет обнаружено с помощью стегоанализа, то вероятность его подмены или разрушения злоумышленником существенно увеличивается. Поэтому актуальной задачей является исследование устойчивости стеганографического встраивания одновременно к стегоанализу и к деструктивным воздей-