

10, октябрь 2015

УДК 004.056

Видеостеганография: средство для унификации тестирования программ

***Сорокин Р. Ю.**, студент,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»*

*Научный руководитель: Самарев Р.С., к.т.н., доцент,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Компьютерные системы и сети»
sorokinroman@student.bmstu.ru*

Введение

В Конституциях большинства стран мира гарантируется право на тайну коммуникаций, однако в настоящее время возросло количество фактов слежки за пользователями сети Интернет со стороны спецслужб. Введение цензурных барьеров и фильтрация трафика ограничивают возможность свободно обмениваться информацией в сети. Для решения двух вышеописанных проблем требуются программные средства, способные выполнять следующие функции:

- скрывать от провайдера трафик;
- зашифровывать трафик от отправителя до получателя [1].

Сегодня существует ряд программных средств, которые тем или иным образом способны обеспечить двустороннюю секретную передачу данных между пользователями в сети, как например Tor, I2P и некоторые другие. Недостаток подобного рода систем заключается в том, что:

- факт наличия трафика от этих программ может быть выявлен с помощью специальных анализаторов трафика у провайдера (DPI) [2];
- все программные системы имеют разные цели и архитектуру, таким образом, плохо совместимы;
- некоторые программы (например, I2P) пересылают много транзитного трафика, предназначенного другим пользователям, что может засорять канал передачи данных.

Для организации обмена секретными данными, когда участники знают друг друга, требуются системы другого класса, наиболее успешной из которых является SkypeHide [3]. SkypeHide использует Skype по принципу LACK, однако стеганограмма передается с помощью специальных 70-битных пакетов, отправляемых программой Skype при наличии тишины (условная архитектура существующей системы приведена на рисунке 1) [4]. Система имеет два серьезных недостатка:

- зависимость от программы Skype (если в будущем архитектура системы Skype будет изменена – потребуется изменять и программу SkypeHide);
- несовместимость с другими средствами видеотелефонии.

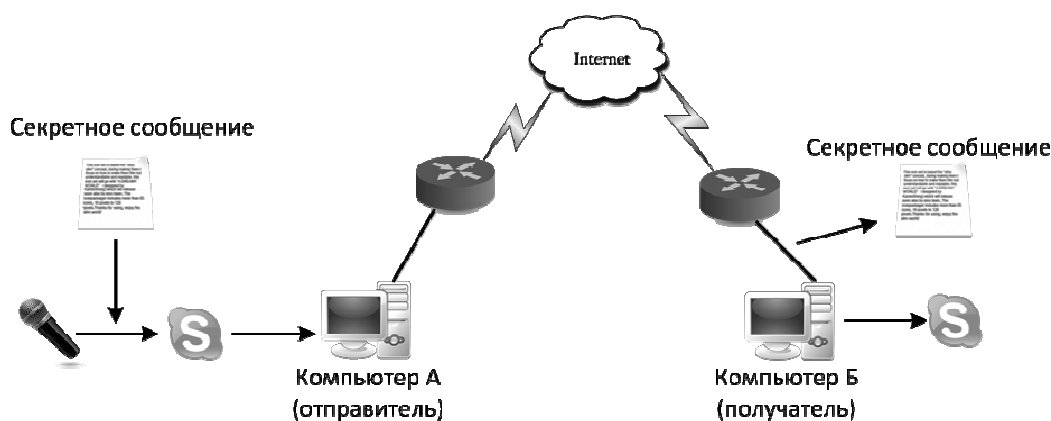


Рис. 1. Архитектура функционирования существующей системы SkypeHide

Разработка программы «Видеостеганографический Фреймворк»

По результатам анализа типовых задач при оценке алгоритмов видеостеганографии была сформулирована задача разработать набор программных средств «Видеостеганографический Фреймворк», предназначенный для тестирования видеостеганографических методов и методов анализа, который имел бы следующие особенности:

1. Простота использования. Программа должна быть интуитивно понятна разработчику методов стеганографии, иметь дружелюбный пользовательский интерфейс, обладать необходимой отказоустойчивостью.
2. Производительность. Программа должна справляться с обработкой видео в режиме реального времени, выводя на экран несколько окон с видеоданными.
3. Гибкость и кроссплатформенность. Разрабатываемое ПО должно иметь возможность дальнейшей модернизации и перекомпиляции под различные платформы.

4. Расширяемость за счет удобного добавления новых методов стеганографии, имитации искажений видео и анализа, в том числе статистического.

При создании набора программных средств тестирования видеостеганографических методов были использованы следующие средства программирования и разработки ПО:

1. Базовая платформа: операционная система с ядром Linux, и библиотека Qt для языка программирования C++. При необходимости программа может быть легко перенесена на другие операционные системы.

2. Библиотека компьютерного зрения openCV. ПО использует стандартные функции захвата видео с камеры, искажения и вывода на экран.

3. Для удобства подключения новых функций использован объектно-ориентированный подход к программированию, что позволяет добавлять новые классы обработки и анализа видеок кадров в виде классов потомков предоставленных интерфейсов.

Для реализации программного продукта была разработана следующая архитектура, кратко представленная на рисунке 4. Видео, захватываемое с вебкамеры пользователя, последовательно проходит несколько блоков. При этом на экран выводятся 6 окон, отображающих видеоданные в режиме реального времени:

- окно захваченного видео (1);
- окно с видеоданными, подвергшимися обработке блоком модификации (2);
- 2 окна видеоданных, полученных в результате работы анализаторов (3,4);
- окна вывода сравнительного и неинформированного анализатора (5,6).

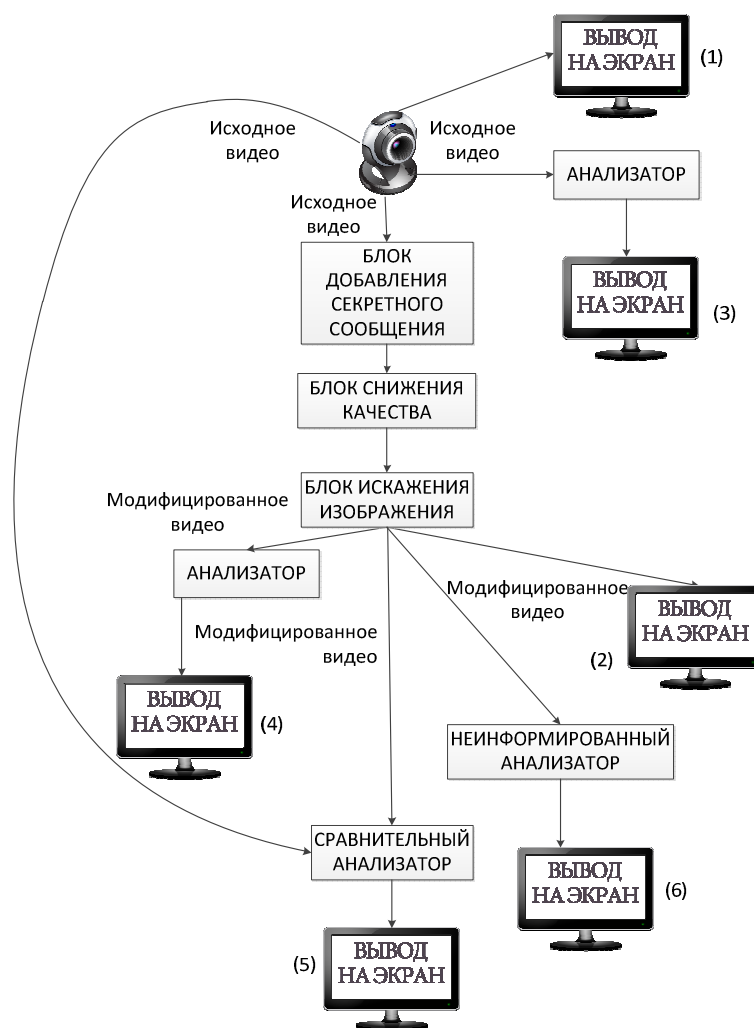


Рис. 2. Архитектура программы «Видеостеганографический Фреймворк»

Такая архитектура наиболее удобна в использовании – пользователь в реальном времени видит результат работы примененного алгоритма стеганографии, а также результаты анализаторов.

Пример использования программы «Видеостеганографический Фреймворк»

В качестве примера использования и тестирования архитектуры были разработаны специальные наглядные алгоритмы:

- в качестве метода стеганографии – добавление QR-кода к выбранному цветовому каналу RGB видеоизображения;
- в качестве метода искажения - медианное размытие кадров;
- в качестве метода сравнительного анализа – разностный сравнительный анализ исходного видео, захваченного с камеры и результирующего видео, полученного в результате применения метода добавления QR кода и медианного размытия;
- в качестве метода неинформированного анализа – неинформированный визуальный анализ по заданному цветовому каналу;

- в качестве оценочного метода анализа – методы вычисления гистограмм исходного и результирующего кадра по трем цветовым каналам RGB.

Тестирование проводилось на компьютере с Intel Core i5 2.70 GHz , 2Gb RAM, OS Ubuntu 12.04.

На рисунке 3 показаны исходное видео и видео со встроенным QR-кодом, подвергшееся медианному размытию. Подмеська проводилась в красный канал RGB путем увеличения значения интенсивности пикселя, попадающего в область QR-кода. Как видно из правого рисунка – QR код практически не заметен.

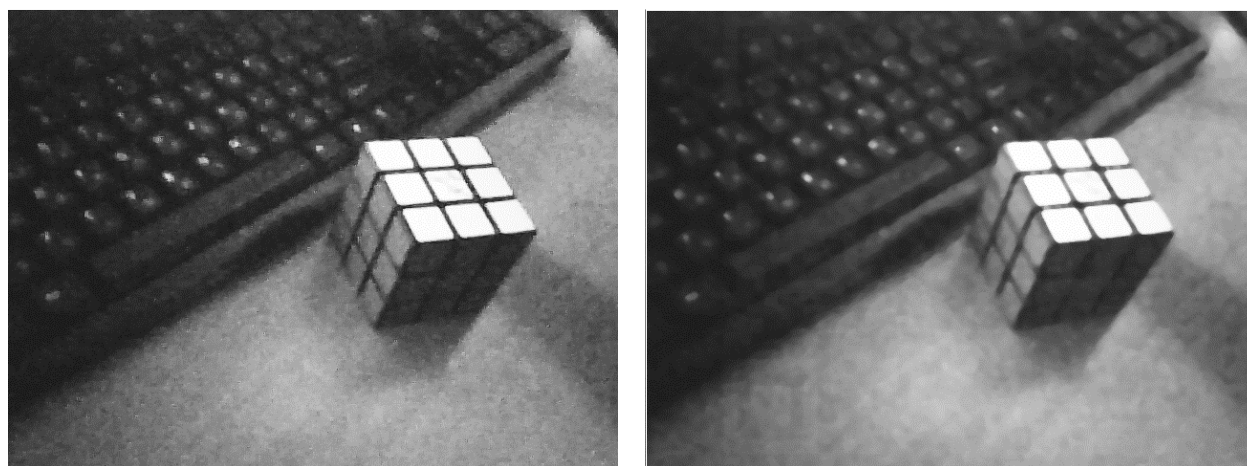


Рис. 3. Исходное видео (слева) и видео, содержащее QR-код в красном канале, подвергшееся медианному размытию (справа)

На рисунке 4 показан результат работы сравнительного и неинформированного анализаторов. QR-код слева получен путем вычитания из интенсивности каждого канала каждого пикселя результирующего искаженного видео интенсивности каждого канала каждого пикселя исходного видео. При определенной яркости фона и качестве печати возможно распознать QR-код с помощью стандартных распознавателей для Android, iOS и т.д. Секретное сообщение представляет собой фразу: *«enter your secret message here»*.

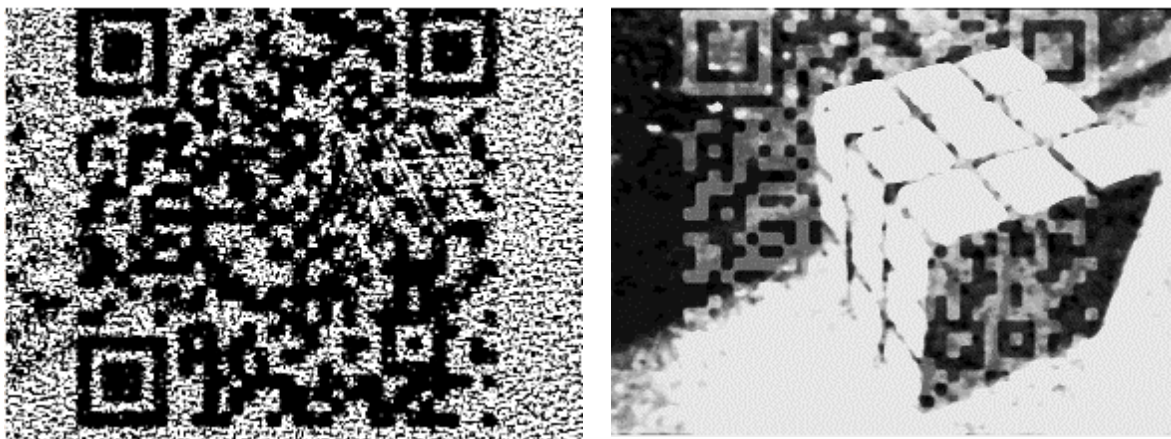


Рис. 4. Результат работы сравнительного анализатора (слева) и результат работы неинформированного визуального анализатора (справа)

Заключение

Рассмотренное средство унификации анализа видеостеганографических методов с реализованным простейшим алгоритмом анализа показало работоспособность разработанной архитектуры в целом.

В качестве дальнейшей работы в этой области автор статьи предполагает усовершенствовать функционал программы «Видеостеганографический Фреймворк», наполнить его наиболее актуальными на сегодняшний день методами анализа, в том числе добавить статистический анализ. После проведенных сравнительных тестов будет выбран наиболее подходящий алгоритм для использования в архитектуре новой виртуальной сети.

Проект доступен в сети Интернет по адресу:

github.com/rosoroki/Realtime-videosteganography-test-framework

Список литературы

1. Ding Feng, Yang Zhiqing, Chen Xuelong, Guo Jianfeng. Effective Methods to Avoid the Internet Censorship // Parallel Architectures, Algorithms and Programming (PAAP), 2011 Fourth International Symposium (Tianjin, 9-11 Dec. 2011): Institute of Electrical and Electronics Engineers proceedings. Tianjin, 2012. P. 67-71.
2. I2P Introduction. Available at: <http://www.i2p2.de/techintro.html> (accessed 22.09.2015).
3. Wojciech Mazurczyk, Maciej Karaś. Krzysztof SzczypiorskiSkyDe: a Skype-based Steganographic Method // INT J COMPUT COMMUN. Warsaw, 2013. P. 432-443.
4. Wojciech Mazurczyk, Józef Lubacz. LACK—a VoIP steganographic method // Telecommunication Systems. 2010. Volume 45 (2). P. 153-163.

5. Steganosaurus. Available at: <http://www.steganosaur.us> (accessed 22.09.2015).
6. Kaushal M. Solanki. Multimedia Data Hiding: From Fundamental Issues to Practical Techniques. Santa Barbara: University of California Santa Barbara, 2005. 250 p.
7. Jonathan Cummins. Steganography And Digital Watermarking. Birmingham: The University of Birmingham, 2004. 24 p.
8. Wen-Chuan Wu, Zi-Wei Lin, Wei-Teng Wong. Application of QR-Code Steganography Using Data Embedding Technique // Lecture Notes in Electrical Engineering. 2013. Volume 253. P. 597-605.
9. Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk, Borko Furht. New approaches to encryption and steganography for digital videos // Multimedia Systems. 2007. Volume 13, Issue 3. P. 191-204.