УДК 003.262.45 Вестник УрФО № 2(48) / 2023, с. 62–66

Христофоров В.В., Беглецов В.А., Баранкова И.И. DOI: 10.14529/secur230206

РАЗРАБОТКА МЕТОДА СТЕГАНОГРАФИИ ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ В АУДИОФАЙЛАХ

В данной научной статье рассматривается метод стеганографии, где для передачи секретной информации исходное сообщение скрыто в контейнере, который представляет собой аудиофайл. Предложенный метод использует повторную конкатенацию звуковых волн заполненного и исходного контейнера с полярным изменением фазы исходного контейнера для расшифровки секретной информации на стороне получателя. Этот метод обеспечивает высокий уровень надежности и безопасности передачи информации, а также позволяет достичь высокой степени скрытности передачи данных. Разработанный метод может быть использован в различных сферах, где требуется надежная и безопасная передача конфиденциальной информации.

Ключевые слова: *стеганография, аудиофайлы, секретное сообщение, звуковые волны, скрытие данных, безопасность, надежность.*

Khristoforov V.V., Begletsov V.A., Barankova I.I.

DEVELOPMENT OF A STEGANOGRAPHY METHOD TO HIDE INFORMATION IN ADUIO FILES

This scientific article discusses the method of steganography, where the original message is hidden in a container, which is an audio file, to transmit secret information. The proposed method uses repeated concatenation of the sound waves of the filled and original container with a polar change in its phase to decrypt secret information on the recipient's side. This method provides a high level of reliability and security of information transmission, and also allows you to achieve a high degree of secrecy of data transmission. The developed method can be used in various fields where reliable and secure transmission of confidential information is required.

Keywords: *steganography, audio files, secret message, sound waves, data concealment, security, reliability.*

Введение

Стеганография — это метод передачи сообщений, который, собственно, скрывает само наличие связи, она занимает свою нишу в обеспечении безопасности: стеганография не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты [1].

Несмотря на бурное развитие стеганографических методов, в свободном доступе имеется недостаточно ПО для стеганографии в аудио файлах.

Проблема

Существует необходимость в защите конфиденциальной информации, передаваемой по различным каналам связи. Традиционными самым распространённым методом являетсякриптография, но алгоритмы симметричного и асимметричного шифрования, могут быть недостаточно эффективными или могут стать объектом атак со стороны злоумышленников. Альтернативным способом защиты информации может стать сокрытие самого факта передачи конфиденциальной информации – стеганография. В данной статье рассматривается метод стеганографии, где в качестве контейнера используется аудиофайл, который позволяет эффективно и надежно передавать конфиденциальную информацию без обнаружения [1].

Аналоги

Был проведен обзор существующих методов с их основным функционалом и выявлены работы посвященные схожим методам стеганографии: широкополосное кодирование, фазовое кодирование и LSB.

В методе широкополосного кодирования в сигнал добавляется модулированный сообщением шум с амплитудой чуть выше предела маскирования.Для извлечения скрытого бита из последовательности коэффициентов используется функция корреляции принятых коэффициентов и исходной случайной последовательности. Следует отметить, что из-за ненадежности извлечения данный метод требует использования кодов коррекции ошибок. Это приводит к уменьшению как быстродействия, так и пропускной способности метода. Еще одним недостатком может служить вносимые в сигнал слышимые искажения.

В методе фазового кодирования используется тот факт, что человеческое ухо воспринимает не значения фазы, а только их разность.Сигнал разбивается на участки, значения фазы на первом участке используются для кодирования скрываемого сообщения, значения фаз остальных участков таким образом, чтобы разность фаз между участками осталась неизменной.Вышеприведенные методы имеют ряд недостатков: они сложны для реализации и понимания, вносят явные искажения в аудио файл и имеют очень низкую пропускную способность. Поэтому при разработке программного обеспечения для стеганографии в настоящее время они используются достаточно редко.

LSBявляется методом, использующим избыточность звуковых файлов. Как известно, младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и обеспечивает возможность скрытия. К достоинствам можно отнести: возможность скрытой передачи большого объема информации, возможность защиты авторского права, скрытого изображения, товарной марки, регистрационных номеров и т.п. Среди недостатков можно выделить, что изменением информации искажаются статистические характеристики цифровых потоков. Ввиду этого для снижения компрометирующих признаков требуется коррекция статистических характеристик [2].

Описание метода

Метод, описанный в статье, имеет свои особенности и перекрывает недостатки предшественников. Данный метод может быть полезным в определенных задачах стеганографии.

В качестве контейнера для скрытого сообщения был выбран аудиофайл формата WAV. В качестве исходного сообщения использовался аудиофайл, но для данного метода, существует возможность использования и других форматов исходного сообщения.

Суть разрабатываемого метода заключается в том, что исходное сообщение помещается в контейнер, который представляет собой аудиофайл, путем наложения звуковых волн. Далее заполненный и пустой контейнеры передаются по различным каналам связи и на стороне получателя происходит расшифровка исходного сообщения, за счет по-

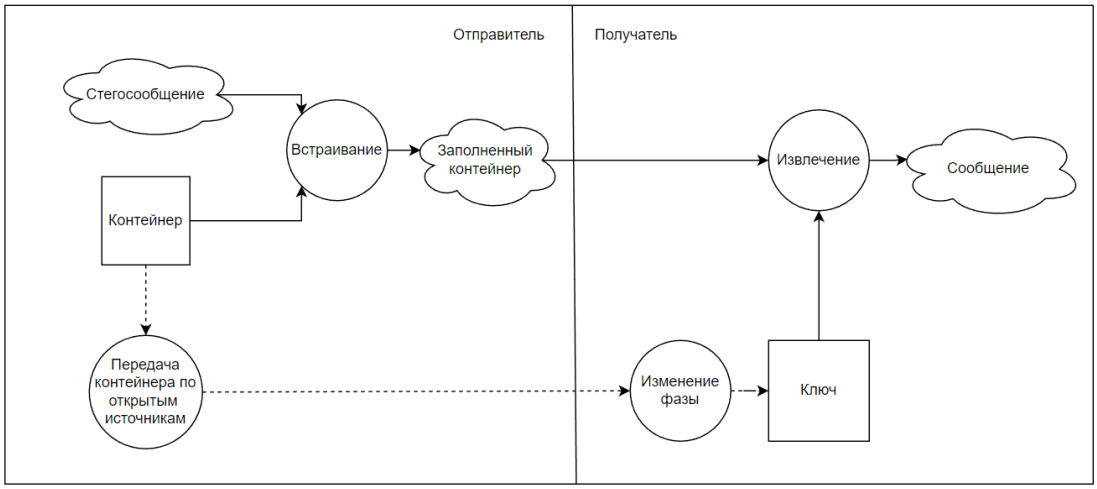

Рис. 1. Алгоритм работы метода

вторной конкатенации звуковых волн заполненного и исходного контейнера с полярным изменением его фазы. В общем виде алгоритм представлен на рис. 1.

Отличительной особенностью данного метода, является использованиеисходного контейнера в качестве ключа, что в свою очередь, делает невозможным извлечение стегосообщения без исходного контейнера.

Алгоритм работы метода

Первым этапом работы алгоритма будет объединение сообщения (рис. 2), которое пользователь хочет передать, и контейнера (рис. 3). При чем контейнером может служить любой аудио фрагмент, например аудиозапись, расположенная в открытом доступе на стриминговых сервисах.

В результате, сохраняется новый аудио-

Рис. 2. Сообщение

Рис. 3. Контейнер

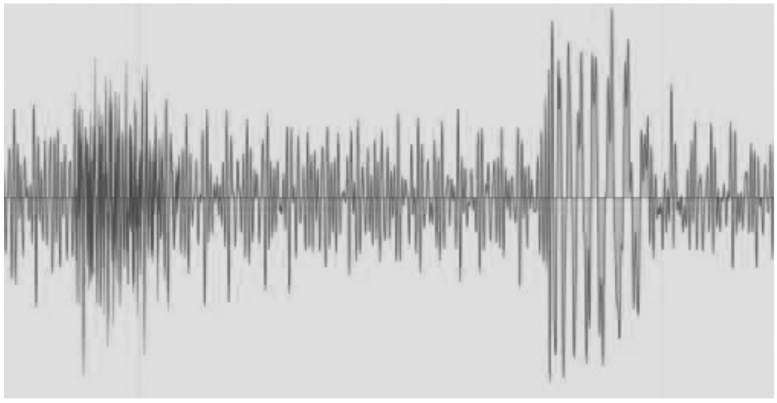

Рис. 4. Заполненный контейнер

файл с заполненным контейнером (рис. 4). В реальных условия контейнер маскирует сообщение, т.к. его громкость превышает громкость сообщения.

После данной операции полный и пустой контейнеры передаются по различным каналам связи конечному получателю.

На стороне получателя у пустого контейнера изменяется фаза сигнала и объединяется с заполненным контейнером. В результате выполнения данной операции, сохраняется аудиофайл, содержащий исходное сообщение. Данное преобразование, работает за счет принципа интерференции звуковых волн.

Объем контейнера для данного метода будет схож с объемом контейнера метода LSB и будет зависеть от частоты дискретизации и глубины аудиофайла (в настоящее время частота дискретизации WAV-формат начинается от 8 кГц до 192 Кгц), а также от психоакустического свойства звука – маскировка звука. Для того чтобы передаваемое сообщение можно было услышать в присутствии контейнера, уровень громкости сообщения должен превышать спектральный уровень контейнера на величину, равную суммарному уровню всех составляющих, лежащих в критической полосе.

Из-за особенностей формата WAV-файла размер заполненного контейнера не отличается от размера пустого контейнера. Недостатком данного метода является изменение контрольной суммы, по которой можно сделать вывод, что в файл вносились изменения. Но это будет возможно только при наличии у злоумышленника пустого и заполненного контейнера.

Результаты и выводы:

В результате работы был разработан и реализован метод стеганографии, где в качестве контейнера используется аудиофайл. Основными преимуществами метода являются незаметность передачи информации и возможность использования в различных областях, например, в системах защиты информации или при передаче конфиденциальных данных.

Литература

1. Федорова А.Р., Шпак В.А., Лукьянов Г.И. Разработка программного модуля для выявленияконфиденциальной информации в звуковых файлах// Актуальные проблемы современной науки, техники и образования.– Магнитогорск, 2021. – № 1. – С. 48–50.

2. Vsavm [Электронный ресурс]: Методы компьютерной стеганографии, URL: https://www.vsavm.by/knigi/kniga3/1740.html (дата обращения 15.03.2023).

3. Гераськин А.С., Смирнов Е.Д.Обнаружение скрытого стеганографического вложения и признаков монтажа в области данных аудиофайла// Вестник Воронежского государственного университета.– Воронеж, 2020. – № 2. – С. 69–78.

4. Маврина М.В.Программное средство сокрытия данных в звуковых файлах // Вопросы кибербезопасности. Москва, 2013 – № 3. С. 36–39.

5. Алексеев А.П., Аленин А.А.Скрытая передача данных в звуковых файлах форматаWAV // Инфокоммуникационные технологии.Самара, 2010 – № 3. С. 101–106.

6. Аленин А.А.Разработка и исследование методов скрытой передачи информации в аудиофай-

лах // Автореферат диссертации на соискание ученой степени кандидата технических наук / Поволжская государственная академия телекоммуникаций и информатики.Самара, 2011.

References

1. FedorovaA.R., ShpakV.A., Luk'yanovG.I. Razrabotkaprogrammnogomodulyadlyavyyavleniyakonfidentsial'noyinformatsiivzvukovykhfaylakh // Aktual'nyyeproblemysovremennoynauki, tekhnikiiobrazovaniya. – Magnitogorsk, 2021. – № 1. – S. 48–50.

2. Vsavm [Elektronnyyresurs]: Metodykomp'yuternoysteganografii, URL: https://www.vsavm.by/knigi/kniga3/1740.html (data obrashcheniya 15.03.2023).

3. Geras'kin A.S., Smirnov Ye.D. Obnaruzheniyeskrytogosteganograficheskogovlozheniyaipriznakovmontazha v oblastidannykhaudiofayla // VestnikVoronezhskogogosudarstvennogouniversiteta. – Voronezh, 2020. – № 2. – S. 69–78.

4.MavrinaM.V.Programmnoyesredstvosokrytiyadannykhvzvukovykhfaylakh//Voprosykiberbezopasnosti. Moskva, 2013 – № 3. S. 36–39.

5. Alekseyev A.P., Alenin A.A. Skrytayaperedachadannykh v zvukovykhfaylakhformata WAV // Infokomunikatsionnyyetekhnologii. Samara, 2010 – № 3. S. 101–106.

6. Alenin A.A. Razrabotkaiissledovaniyemetodovskrytoyperedachiinformatsii v audiofaylakh // Avtoreferatdissertatsiinasoiskaniyeuchenoystepenikandidatatekhnicheskikhnauk / Povolzhskayagosudarstvennayaakademiyatelekommunikatsiyiinformatiki. Samara, 2011.

ХРИСТОФОРОВ Валерий Валерьевич, студент кафедры «Информатики и информационной безопасности» ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Челябинская обл., г. Магнитогорск, пр. Ленина, 38. E-mail: valery.hristoforoff@yandex.ru

БЕГЛЕЦОВ Вадим Андреевич, студент кафедры «Информатики и информационной безопасности» ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Челябинская обл., г. Магнитогорск, пр. Ленина, 38. E-mail: begletsov.v777@gmail.com

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующая кафедрой «Информатики и информационной безопасности» ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, Челябинская обл., г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

KHRISTOFOROV Valery Valeryevich, a student of the Department of Informatics and Information Security of FSBEI VPO Magnitogorsk State Technical University named after G.I. Nosov. G.I. Nosov. 455000, Chelyabinsk region, Magnitogorsk, Lenin Ave. 38. E-mail: valery.hristoforoff@yandex.ru

BEGLETSOV Vadim Andeevich, a student of the Department of Informatics and Information Security of FSBEI VPO Magnitogorsk State Technical University named after G.I. Nosov. G.I. Nosov. 455000, Chelyabinsk region, Magnitogorsk, Lenin Ave. 38. E-mail: begelsov.v777@gmail.com

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security, FGBOU HE Magnitogorsk State Technical University named after M.V. G.I. Nosov. 455000, Chelyabinsk Region, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru