Nikita S. Dvoryankin
Central Research Insntitute of Economics, Informatics and Control Systems,
2/7, str. 1, Malaya Bronnaya, Moscow, Russia, 123104
nik.dvrn@gmail.com, orcid.org/0000-0002-1580-7179

Analysis Methods of Secretive Labeling Voice Commands for Remote Voice Control to Confirm their Authenticity

Keywords: voice information security, steganography, SMS – banking service, mobile – banking, verification of customer, information security in the banking sector, remote voice control systems.

In connection with the gradual transfer of spheres of human activity in the information field, every day there is a growth of threats associated with their information security. The result of this process leads to a technological race between the development of information security and the development of threats to information security technologies. The article analyzes the benefits of using voice commands in the remote management systems in terms of their security from unauthorized access and further use of the prospects. It is proposed to use the methods of marking a digital voice command as additional protection in applications where it is necessary to establish their authenticity. Also promoted analysis methods secretive marking voice commands in the course of their transmission through a variety of voice communication channels. An example of the use of these methods in the banking sector, for extra protection, and customer verification.

Н.С. Дворянкин
Центральный научно-исследовательский институт экономики, информатики и систем управления
Россия, 123104, Москва, ул. Малая Бронная, 2/7, стр. 1
nik.dvrn@gmail.com, orcid.org/0000-0002-1580-7179

АНАЛИЗ МЕТОДОВ СКРЫТНОГО МАРКИРОВАНИЯ ГОЛОСОВЫХ КОМАНД ДИСТАНЦИОННОГО РЕЧЕВОГО УПРАВЛЕНИЯ ДЛЯ ПОДТВЕРЖДЕНИЯ ИХ ПОДЛИННОСТИ

Ключевые слова: защита речевой информации, стеганография, смс-банкинг, мобильный-банкинг, верификация клиента, информационная безопасность в банковской сфере, системы дистанционного речевого управления.

В связи с постепенным переводом сфер жизнедеятельности человека в информационное пространство, с каждым днём происходит рост угроз, связанный с их информационной безопасностью. Результат этого процесса приводит к технологической гонке между разработкой технологий информационной защиты и разработкой угроз информационной безопасности. В статье проанализированы преимущества использования голосовых команд в системах дистанционного управления с позиций их защищённости от НСД и перспектив дальнейшего использования. Предложено применять методы цифрового маркирования голосовых команд в качестве дополнительной защиты в приложениях, где необходимо установление их подлинности. Также произведён анализ методов скрытного маркирования голосовых команд в процессе их передачи через различные каналы речевой связи. Рассмотрен пример использования данных методов в банковской сфере для дополнительной защиты и верификации клиента.

Введение

В настоящее время наблюдается процесс постепенного отказа от «традиционных» способов взаимодействия между компаниями-«поставщиками информации» и их клиентами – «потребителями информации». Большинство крупных компаний уже внедрили различные виды информационных систем оказания услуг и поддержки клиентов в формате «умных чатов», «автоответчиков-роботов» и пр., преследуя такие цели, как автоматизация процесса оказания услуг и поддержки, сокращения издержек и поиска новых способов повышения прибыли и др. Данные цели понятны. Они напрямую связаны с разрешением противоречия, связанного с ростом числа клиентов и, неспособностью оказания им качественных услуг и техподдержки в полном объёме клиентам такими «традиционными» способами, как содержание офисов с большим штатом консультантов и(или) call-центров с большим штатом техподдержки.

Однако, несмотря на необратимый процесс тотальной автоматизации и информатизации процессов взаимодействия в различных сферах человеческой жизни, ещё существует множество нерешённых проблем информационной безопасности, большинство из которых связано с «банальным» человеческим фактором. Угрозы информационной безопасности могут исходить как от проектировщиков информационных систем, так и самих конечных пользователей – «потребителей информации».

В данный момент и, вполне вероятно, в ближайшем будущем, для решения таких важных проблем в критических областях в ходу останутся технологии информационного обмена, основанные на речевых коммуникациях между «поставщиками» и «потребителями» информации.

Преимущества использования голосовых команд в системах дистанционного управления

Известно, что речь – один из важнейших атрибутов жизни человека, предназначенный для взаимодействия с другими людьми и окружающим миром. Тогда становится понятным особое внимание исследователей к задачам защиты речевой информации. В настоящее время в связи с развитием числа и уровня услуг речевых коммуникаций, новых информационных угроз на основе методов и средств цифровой обработки речевого сигнала (РС), на первый план выходит задача установления подлинности передаваемых речевых сообщений (команд).

Сегодня среди новых информационных угроз для таких систем отмечаются: прямая имитация голоса диктора, уже реализованная как функция в современных версиях звуковых редакторах типа AdobeAudition; монтаж и комбинация речевых команд из ранее сделанных записей голоса диктора-оператора системы и др.

В качестве мер противодействия таким угрозам традиционно предлагается внедрение в речевую команду скрытых цифровых меток – маркеров. К сожалению, основная часть таких традиционных мер известна нарушителю и может быть им обнаружена и обойдена. Поэтому их рекомендуется использовать в качестве дополнительной защиты. А альтернативой может стать следующий метод.

Рассмотрим голосовую команду как некий информационный контейнер – К. Например, кодовую последовательность «*Тусезунг*», представленную в виде фразы, соответствующей исходной фразе «Проверка», текст которой зашифрован «шифром Цезаря» со сдвигом 3). Данный контейнер-фразу необходимо передать от пользователя А к информационной системе (ИС) – Б.

Пользователь А устанавливает соединение с информационной системой Б, используя любой из существующих каналов голосовой связи и передаёт сообщение информационной системе Б. Информационная система производит процесс оцифровки

данного контейнера (если он пришёл в аналоговом виде) или декодировки (если он пришёл, например, через GSM-канал), затем информационная система производит процесс распознавания содержимого данного речевого контейнера.

На этом шаге уже проявляются преимущества использования голосовых команд с точки зрения их защищённости от НСД.

Полученный речевой информационный контейнер со значением «*Тусезунг*» будет иметь колоссальную избыточность, в отличие от его текстовой формы, ведь данный контейнер пришёл к «ИС Б» в виде фонем – отдельных звуков для каждой буквы кодовой последовательности. При этом передаваемая команда пользователем А каждый раз будет иметь различные просодические характеристики, что в целом обеспечивает начальный уровень защищённости в отличии от тестовой команды. Ещё одним преимуществом применения голосовой команды вместо текстовой заключается в необходимости использования дополнительной вычислительной мощности для ее расшифровки или подделки в случае компрометации. Также голосовую команду можно дополнительно защитить, если, например, использовать сначала алгоритм распознавания с определёнными свойствами (который будет распознавать, например, каждую вторую фонему, слог и т.д. в команде), а потом применять установленные алгоритмы для распознанного (переведённого в текстовый вид) сообщения [1– 4].

С учётом того, что сегодня в отдалённых районах Российской Федерации всё ещё для коммуникаций используют сотовую связь 2-го поколения в основном с покрытием, предназначенным для голосовой связи, то использование голосовой связи, в отличие от текстовой (смс, Интернет) более экономично и целесообразно. Так как передача информации со стандартного листа А4 занимает 2–3 минуты при спокойном темпе речи, а при передачи данной информации в виде смс сообщений потребует отправки ~36 смс.

Использование методов маркирования голосовых команд для их дополнительной защиты

Как уже отмечалось, для дополнительной защиты системы дистанционного голосового управления в «шифрованную» голосовую команду существует возможность, при которой, используя методы скрытного маркирования (стеганографии), можно внедрить дополнительную информацию подтверждающую подлинность принятой команды.

Например, в информационную систему Б приходит команда от пользователя А, но предполагается, что данная команда скомпрометирована злоумышленником. В этом случае информационная система Б (по ранее назначенному алгоритму) производит процесс выделения скрытого «маркера». Маркер может представлять собой цифровой водяной знак (ЦВЗ), последовательность, графику или некий шифрованный токен. В случае выделения данного «маркера» и его целостности информационная система Б производит расшифровку данной команды и выполняет её.

Кратко рассмотрим перспективные методы аудиомаркирования подробно изложенные в работе [5].

Сигнальная группа методов. Из так называемой классической группы сигнальных методов, в которой встраивание маркера в сигнал происходит за счёт избыточности самого сигнала для использования, можно выделить только один метод – встраивание маркера посредством расширения спектра, который характеризуют высокий уровень скрытности и высокая устойчивость к преобразованиям.

В данном методе скрываемый «маркер» умножается на несущий сигнал и псевдослучайную шумовую последовательность – ключ, который характеризует широкий частотный спектр. В результате этого спектр данных расширяется на всю доступную поло-

су. В дальнейшем последовательность расширенных данных ослабляется и прибавляется к исходному сигналу [6].

Авторами метода получена скорость передачи данных около 4 бит/с. Стойкость к преобразованиям отмечается как высокая, поскольку встраивание информации производится путем «рассеивания» кодированных данных по всему частотному спектру. Уровень скрытности также высокий в связи с тем, что метод вводит в звук носителя аддитивный случайный шум малой мощности. Однако особенностью метода является то, что аудиосигналы, применяемые в качестве контейнеров, имеют дискретный формат и на принимающей стороне должны быть известны как ключ для дешифрования, тот же псевдослучайный шум, так и частота следования посылок, скорость передачи данных, частота (вид) несущей, точки начала и конца расширенных данных. Это ограничивает использование метода для различных участков применяемого канала речевой связи.

Группа методов, основанная на модификации просодических признаков речи. Согласно [7, 8] одним из эффективных подходов к встраиванию скрытых данных в речь (по сравнению с обычными сигнальными методами) является использование языковой просодии: совокупности таких фонетических признаков, как тон, громкость, темп, общая тембровая окраска речи. Значительная вариативность просодии, а также сложность формализации и анализа особенностей её индивидуальной и ситуационной изменчивости заключает в себе возможность её использования в аудиостегосистемах [9, 10].

С лингвистической точки зрения, речевой сигнал на передающей стороне поддаётся сегментации на участках, различающихся по характеру источника звука, а именно: пауза, голосовой, шумовой и др.

Применительно к скрывающим преобразованиям предполагается: если речевой сигнал сегментировать на естественные неоднородные участки, то на этих участках можно выделить некоторые акустические параметры, преобразование которых в определённых пределах от нормы не различаются ни на слух, ни с помощью инструментальных средств без сравнения с эталоном. К этим сегментам применимы амплитудные, фазовые, частотные и временны́е методы преобразования звука, в том числе модификации частоты основного тона (ЧОТ) и длительности самих сегментов речи. Основное требование к скрывающему преобразованию состоит в том, что речевой сигнал, который сегментирован и модифицирован на передающей стороне, должен однозначно сегментирован и измерен на принимающей стороне с точностью, позволяющей извлечь скрытые данные. Измеряемыми характеристиками скрываемого сообщения, как правило, являются ЧОТ и длительность сегментов речи, несущие в себе стегокод скрываемого сообщения [2].

Проведённые в [6, 7] исследования позволили выявить пределы психоакустической нормы модификации ЧОТ и длительности сегментов речи, при которых скрывающие преобразования не заметны на слух: они составляют около 7 – 10 и 3 – 5 % их абсолютных значений. Исследование обратимости и стойкости стегопреобразований проводилось с использованием вложения шумоподобных данных в пределах этих ограничений. При таких значениях информационная плотность стеговложения составляла 5–8 бит на сегмент, а пропускная способность стегоканала – 16 – 35 бит/с.

В работе [7] отмечается, что при подобных ограничениях пустые и заполненные контейнеры обладают одинаковой стойкостью к преобразованиям в канале связи. Это означает, что данная группа аудиостегометодов обладает значительной стойкостью к различным видам преобразований и помех в канале речевой связи. Учёт естественной сегментации речи и психоакустических особенностей слухового анализатора человека,

реализованные в данной группе методов, позволяют добиться высокой скрытности внедрения конфиденциальных данных. Согласно [5] указанные методы обладают высокой стойкостью к вокодерным преобразованиям, в связи с чем они могут быть предложены для использования в интересах скрытой связи в голосовом трафике стандарта GSM.

Методы, основанные на встраивании графических маркеров в спектральные развёртки голосовой команды и ее акустического фона. Данная группа методов сокрытия «маркеров» в голосовой командах, представляемых в виде графических образов на изображениях динамических спектрограмм акустического фона, сопровождающего РС так же, как и методы, основанные на модификации частоты основного тона и длительности сегментов речи, относится к нецифровой стеганографии в связи с тем, что внедрение данных производится в частотную и временную области аудиосигнала и его фона, а не в их цифровой код [11].

Здесь речеподобная волновая форма, модулирующая передаваемые данные в виде графического образа на спектральных развёртках речи и фона (в паузах), генерируется не заранее, а формируется непосредственно в процессе передачи, адаптируясь к типу передаваемых данных, пригодному для трансляции в системе GSM, учитывая особенности их передачи и восприятия, а также характеристики самого канала. Данные методы наиболее предпочтительны в использовании при маркировании голосовых команд систем дистанционного управления в связи алгоритмом, который прост в реализации применительно к мобильным приложениям и обеспечивет скрытное и стойкое к различным типам преобразованиям маркирование команды.

Пример использования маркирования голосовых команд в банковской сфере

В современной банковской сфере для увеличения качества обслуживания постоянно растущей клиентской базы и минимизации расходов на поддержание инфраструктуры (офис–call-центр) происходит процесс постепенного замещения традиционных видов взаимодействия с клиентами на взаимодействие с клиентами посредством использования таких перспективных интернет-технологий, как «банк–клиент» и(или) «мобильный банк–клиент».

Данные приложения заменяют собой необходимость посещения офиса банка для выполнения большинства операций, не связанных с большими рисками, и которым априори не требуется присутствие клиента и сотрудника (платежи за услуги, переводы и пр.). С учётом того, что разработчики данных приложений нацелены на широкую аудиторию с различным уровнем «мобильной» и «компьютерной» грамотности, интерфейс и процесс осуществления операций сделан максимально доступным для понимания большинству населения (например, приложение «Сбербанк Онлайн» имеет суммарное количество установок от 10 до 50 млн на двух основных мобильных платформах).

Для обеспечения безопасности работы с банк-клиентом и(или) мобильным банк-клиентом, службы информационной безопасности банков, помимо базовых методов защиты (шифрованное соединение и пр.), внедрили двухфакторную аутентификацию, преследуя цель, которая заключается в минимизации возможностей реализации противоправных действий со стороны «мошенников», а также лимитировали суммы операций в день и за раз (в каждом отдельном банке – свои лимиты).

Однако в последнее время, несмотря на данные механизмы защиты, из-за роста числа пользователей мобильного банка, основную угрозу безопасности представляет собой банальный человеческий фактор: передача ПДн, кодовых фраз, данных карты и смс-кодов подтверждения третьим лицам. Вторая массовая угроза безопасности – вредоносное ПО на компьютере и смартфоне клиента, которое позволяет получать доступ

к сообщениям клиента (чтение/запись) и(или) обладать функционалом «кей-логгера» и(или) «записывать голос пользователя».

Угрозу ИБ несут в себе и смартфоны, не имеющие сертификата соответствия (производимые на noname-фабриках и купленные через иностранные интернет-магазины), из-за внедрения в их ПО вредоносного кода на уровне ядра, а также восстановленные из noname запчастей смартфоны, в запчастях которых может содержаться программная или аппаратная закладка.

Для сокращения рисков, связанных с кражей данных карты и подтверждением операций, банки внедрили технологию известную как «3d–secure»/ «VerifybyVisa» или, иными словами, смс-подтверждение. Пользователь, получив карту в банке и желая использовать ее для покупок в Интернете (мобильный банк), регистрирует номер своего мобильного телефона в системе банка (рис. 1) и получает на свой мобильный телефон смс-сообщения с кодами подтверждения операций (рис. 2), при этом банк должен получать от оператора сотовой связи IMSI и TMSI сим-карты абонента для обеспечения безопасности.

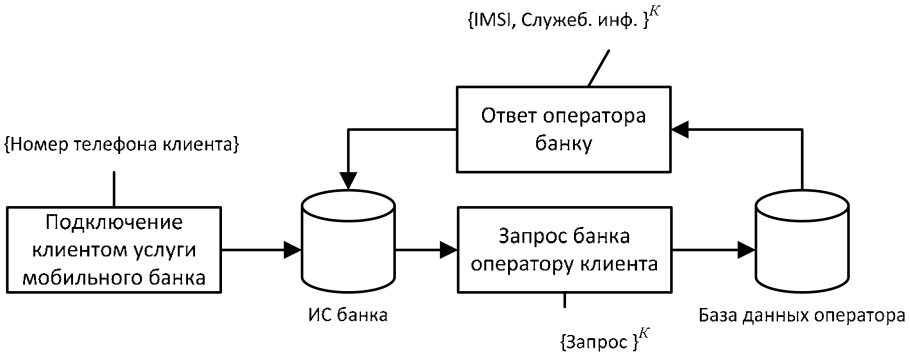

Рис. 1. Регистрация номера клиента в информационной системе банка

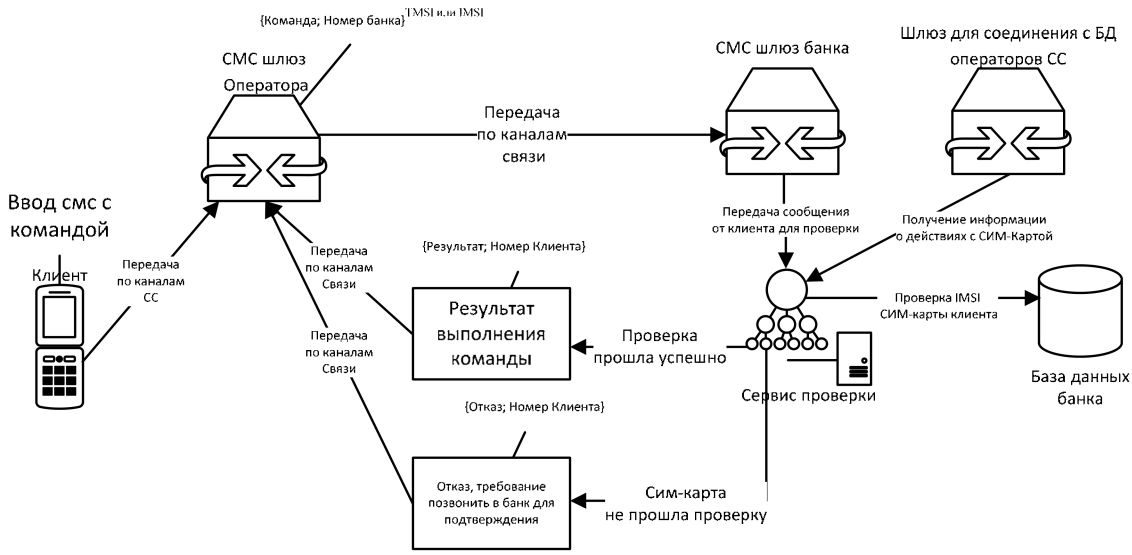

Рис. 2. Принцип работы системы обеспечения безопасности банка с подтверждением операций посредством смс-сообщений

Один из популярных способов мошенничества в недавнем прошлом (и в настоящем), осуществляется следующим образом: при краже личных данных «мошенник» звонит «жертве», представляясь сотрудником банка, просит назвать присланный код для «отмены операции».

Однако с течением времени данный способ постепенно уступает лавры популярности способу, основанному на замене сим-карты по поддельным документам или доверенностям. Данный способ популярен тем, что банки стали «добровольно/принудительно» подключать новым абонентам услугу смс-оповещения, а не во всех банках существует развитая структура коммуникации с операторами сотовой связи. При регистрации номера банк получает от оператора IMSI «индивидуальный номер» сим-карты абонента, и при смене сим-карты IMSI меняется. В результате злоумышленник оставляет клиента банка без связи и без средств на счёте банка.

С недавних пор банки приняли на вооружение системы безопасности (помимо встроенных в «банк–клиент» антивирусов и развития взаимодействия с операторами сотовой связи), анализирующие действия пользователей. В случае совершения «подозрительных» действий система автоматически блокирует последующие до звонка оператору банка для подтверждения выполнения операций. Оператору банка для подтверждения требуется передать по голосовой связи (через GSM или ТФОП) все свои ПДн, секретную фразу, данные карты отправителя и получателя. Недостаток данного метода один – при передаче данной информации она может быть скомпрометирована по акустическому каналу утечки, а данный разговор может быть записан вредоносным ПО, что даст злоумышленнику расширенные знания о жертве.

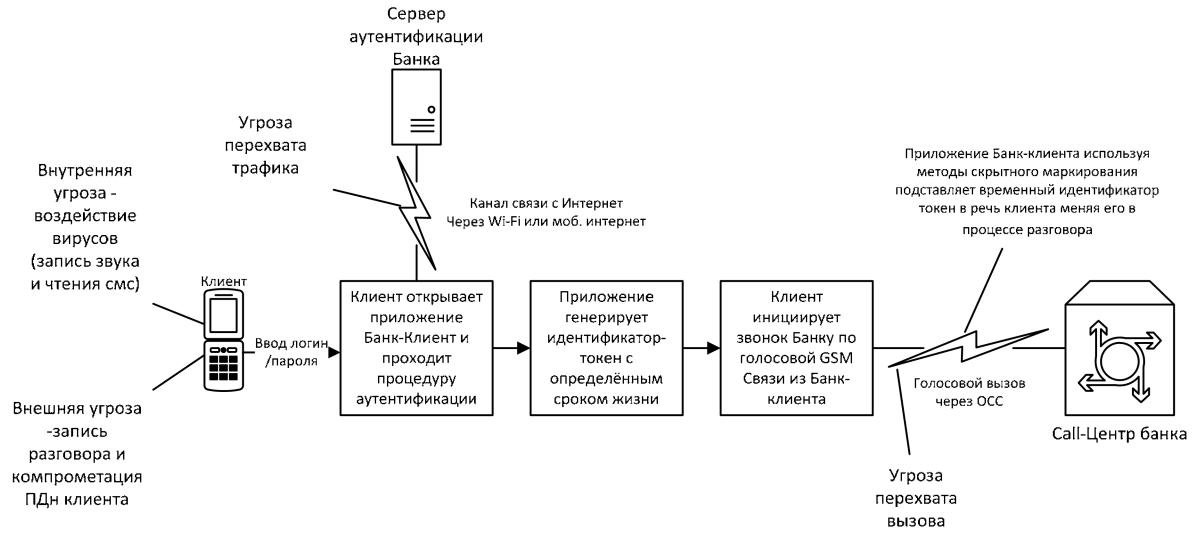

Рис. 3. Пример использования методов скрытного маркирования голосовых команд

Поэтому для обеспечения безопасности подтверждения личности и(или) подтверждения операций через оператора банка, предлагается применять методы скрытного маркирования [12–15], рассмотренные в данной статье. Пример использования, приведенный на рис. 3, представляет собой перспективный способ внедрения технологий скрытного маркирования голосовых команд, где в качестве голосовой команды выступает звонок клиента оператору банка (через мобильное приложение банк-клиента), в который в процессе разговора, используя методы скрытного маркирования, «подмеши-

вают» некий токен. Данный токен распознается в подсистеме «распознавания» банка (рис. 4). В случае успеха оператору Call-центра передается сообщение об успешной верификации токена. Иными словами, подтверждается, что с оператором Call-центра говорит клиент, а не мошенник.

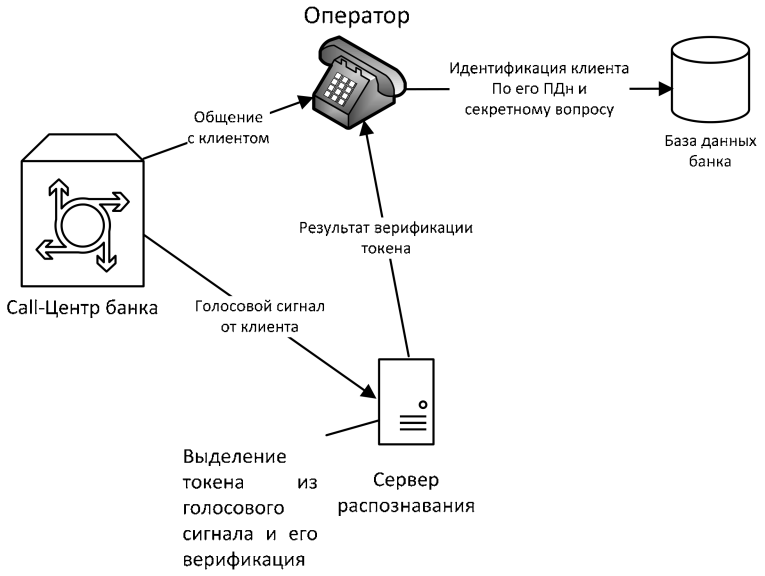

Рис. 4. Подтверждение подлинности голосового сигнала

Заключение

Рассмотрены преимущества использования голосовых команд в системах дистанционного управления

Проведённый анализ существующих и перспективных методов скрытного маркирования голосовых команд и последующих их передачи по каналам связи относительно применимости к встраиванию маркера в голосовые команды и последующей их передачи в системе дистанционного управления показал, что:

известные традиционные сигнальные методы построения аудиостегосистем, както: внедрение скрываемой информации в наименее значащие биты (НМЗ) аудиосигналов, модификация их фазы, эхо-отклик и другие, – не могут быть использованы для скрытной передачи КИ в голосовом трафике СПСС при наличии «вокодерных» и «цифровых преобразований» с частичной потерей информации об исходном сигнале. Более того, существует большое количество программ стегоанализа, настроенных на обнаружение именно этих хорошо известных стегометодов;

группа методов на основе применения просодических признаков речи, обладая повышенной скрытностью и устойчивостью к цифровым преобразованиям в каналах сотовой связи, не может обеспечить достаточно высокую скорость передачи скрываемой информации, превышающую 40 бит/с.

Сегодня наиболее привлекательными перспективными методами маркирования голосовых команды являются методы встраивания «маркера» в графическом виде, то есть в параметрах спектральных частотно-временных развёрток аудиосигналаносителя. Также интересным становится вопрос использования для сокрытия передаваемой информации акустического фона, сопровождающего голосовую команду с применением для внедрения маркера подобных спектрально-временных описаний.

Предложен пример внедрения технологии маркирования голосовых команд применительно к банковской сфере.

СПИСОК ЛИТЕРАТУРЫ:

1. Dutta P., Bhattacharyya D., Kim T. Data Hiding in Audio Signal: A Review // International Journal of Database Theory and Application Vol. 2, No. 2, June 2009 http://www.sersc.org/journals/IJDTA/vol2_no2/1.pdf (дата обращения 22.11.2016).
2. Paulus J., Muller M., Klapuri A. Audio-Based Music Structure Analysis // Tampere University of Technology & Saarland University and MPI Informatics& Queen Mary Univ. of London http://www.cs.tut.fi/sgn/arg/klap/2010_PaulusMuellerKlapuri_STAR-MusicStructure_ISMIR.pdf (дата обращения 22.11.2016).
3. Divya S.S., Ram Mohan Reddy M. Hiding text in audio using multiple LSB steganography and provide security using cryptography // International Journal Of Scientific & Technology Research Volume 1, Issue 6, July 2012 http://www.ijstr.org/final-print/july2012/Hiding-Text-In-Audio-Using-Multiple-LSB-Steganography-And-Provide-Security-Using-Cryptography.pdf (дата обращения 22.11.2016).
4. Sundermann D., Hoge H., Bonafonte A., Ney H., Black A., Narayanan Carnegie S. Text-Independent Voice Conversion Based On Unit Selection // Mellon University, University of Southern California, Siemens Corporate Technology https://www.cs.cmu.edu/~awb/papers/ICASSP2006/0100081.pdf (дата обращения 22.11.2016).
5. Дворянкин С.В., Дворянкин Н.С. Способ установления подлинности речевых сообщений, передаваемых по каналам сотовой связи // Спецтехника и связь. 2015. № 4. С. 32–39.
6. Салагай М.О. Просодические средства защиты смысловой информации (экспериментально-фонетическое исследование в области стеганографии) // Автореферат диссертации на соискание ученой степени кандидата филологических наук по специальности 10.02.21 Прикладная и математическая лингвистика. М., 2011. С. 25.
7. Пономарь М.О. Метод сокрытия данных в речевых сигналах в интересах защиты информации// Речевые технологии. 2009. С. 80–84.
8. Пономарь М.О. Требования к алгоритмам скрытного встраивания информации в просодические параметры речи // Речевые технологии. 2010. С. 77–81.
9. Панов А.А. Передача данных через речевые каналы системы GSM // Безопасность информационных технологий. БИТ. 2012. № 1. С. 22–28.
10. Алюшин В.М., Дворянкин С.В. Технологии образного анализа в задачах цифровой обработки речевой информации // Научная визуализация. 2013. Т. 5. № 3. С. 75–88.
11. Rehna V.J., Jeya Kumar M.K. A Strong Encryption Method of Sound Steganography by Encoding an Image to Audio // International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.
12. Алюшин А.М., Дворянкин Н.С. Технология защитного аудиомаркирования документированной информации с использованием мобильных устройств // Спецтехника и связь. 2015. № 6. С. 26–31.
13. Алюшин А.М., Дворянкин Н.С. Особенности распознавания изображений речевой подписи на мобильных устройствах // Безопасность информационных технологий. 2015. № 4. С. 38–45.
14. Костров Д. Бимодальная верификация по голосу/лицу с помощью мобильного приложения// Первая миля. 2016. № 6. С.56–59.
15. Бельфер Р.А. Сети и системы связи (технологии, безопасность). М.: МГТУ им. Н. Э. Баумана. 2012.

REFERENCES:

1. Dutta P., Bhattacharyya D., Kim T. Data Hiding in Audio Signal: A Review // International Journal of Database Theory and Application Vol. 2, No. 2, June 2009 http://www.sersc.org/journals/IJDTA/vol2_no2/1.pdf (accessed 22.11.2016).
2. Paulus J., Muller M., Klapuri A. Audio-Based Music Structure Analysis // Tampere University of Technology & Saarland University and MPI Informatics & Queen Mary Univ. of London http://www.cs.tut.fi/sgn/arg/klap/2010_PaulusMuellerKlapuri_STAR-MusicStructure_ISMIR.pdf (accessed 22.11.2016).
3. Divya S.S., Ram Mohan Reddy M. Hiding text in audio using multiple LSB steganography and provide security using cryptography // International Journal Of Scientific & Technology Research Volume 1, Issue 6, July 2012 http://www.ijstr.org/final-print/july2012/Hiding-Text-In-Audio-Using-Multiple-LSB-Steganography-And-Provide-Security-Using-Cryptography.pdf (accessed 22.11.2016).
4. D.Sundermann, H.Hoge, A. Bonafonte, H. Ney, A. Black, S. Narayanan Carnegie. Text-Independent Voice Conversion Based On Unit Selection // Mellon University, University of Southern California, Siemens Corporate Technology https://www.cs.cmu.edu/~awb/papers/ICASSP2006/0100081.pdf (accessed 22.11.2016).
5. Dvorjankin S.V., Dvorjankin N.S. Sposobustanovlenijapodlinnostirechevyhsoobshhenij, peredavaemyhpokanalamsotovojsvjazi // Spectehnikaisvjaz'. 2015. № 4. S. 32-39. (in Russian).
6. Salagaj M.O. Prosodicheskiesredstvazashhitysmyslovojinformacii (jeksperimental'no-foneticheskoeissledovanie v oblastisteganografii). // Avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata filologicheskih nauk po special'nosti 10.02.21 Prikladnajai matematicheskaja lingvistika. Moskva 2011. S. 25. (in Russian).
7. Ponomar' M.O. Metod sokrytija dannyh v rechevyh signalah v interesah zashhity informacii // Rechevyetehnologii. 2009. S. 80–84 (in Russian).

8. Ponomar' M.O. Trebovanija k algoritmam skrytnogo vstraivanija informacii v prosodicheskie parametry rechi // Rechevye tehnologii. 2010. S. 77–81 (in Russian).
9. Panov A.A. Peredacha dannyh cherez rechevye kanaly sistemy GSM // Bezopasnost' informacionnyhtehnologij. BIT. 2012. №1. S. 22–28 (in Russian).
10. Aljushin V.M., Dvorjankin S.V. Tehnologii obraznogo analiza v zadachah cifrovoj obrabotki rechevoj informacii // Nauchnaja vizualizacija. 2013. T. 5. № 3. S. 75–88 (in Russian).
11. Rehna V.J., Jeja Kumar M.K. A Strong Encryption Method of Sound Steganography by Encoding an Image to Audio // International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.
12. Aljushin A.M., Dvorjankin N.S. Tehnologija zashhitnogo audiomarkirovanija dokumentirovannoj informacii s ispol'zovaniem mobil'nyh ustrojstv // Spectehnikaisvjaz'. 2015. №6. S. 26–31 (in Russian).
13. Aljushin A.M., Dvorjankin N.S. Osobennosti raspoznavanija izobrazhenij rechevoj podpisi namobil'nyh ustrojstvah // Bezopasnost' informacionnyhtehnologij. 2015. № 4. S. 38–45 (in Russian).
14. Kostrov D. Bimodal'naja verifikacija po golosu/licu s pomoshh'ju mobil'nogo prilozhenija // Pervaja milja. 2016. №6. S. 56–59 (in Russian).
15. Bel'fer R.A. Setiisistemysvjazi (tehnologii, bezopasnost'). M.: MGTU im. N.Je. Baumana. 2012. (in Russian).