Московский Физико-Технический Институт(Государственный Университет)
Кафедра Радиотехники
http://re.mipt.ru/infsec

Эссе по курсу «Защита информации»

Различные технологии защиты для цифрового видео

Выполнила: студентка 116 гр.
Доронина М.В.

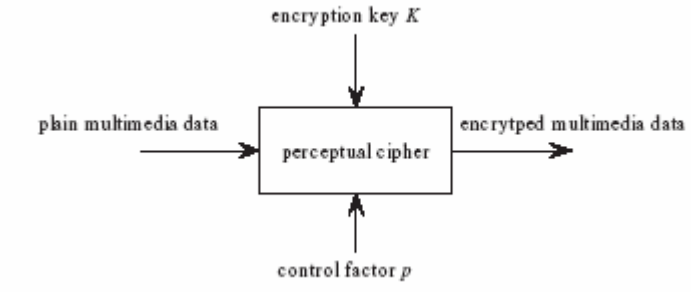
Долгопрудный
2005

Введение.

Широкое использование цифровых изображений и видео в различных областях в наши дни заставило обратить внимание на предмет их защиты и секретности. Несмотря на многочисленные преимущества цифрового видео в отношении и производителей и потребителей, главным недостатком остается опасность пиратства, основная цель которого – получение незащищенного экземпляра пленки для распространения в неограниченном количестве. Кроме того, требуется особая и надежная защита в хранении и передаче цифровых видео/изображений в таких отраслях как система платного телевидения, видео по запросу, конфиденциальные видео конференции, системах медицинской визуализации и тому подобных. Хорошо развитая современная криптография должна стать идеальным решением этой задачи. Как известно, с 1970-х годов было разработано множество достаточно безупречных систем шифрования, которые успешно широко применялись, например системы DES, IDEA, RSA. Но большинство традиционных систем шифрования не могут напрямую использоваться для кодирования цифрового видео в системах реального времени, поскольку их скорость шифрования не достаточно высока, особенно когда алгоритмы реализуются ПО. К тому же, существование различных алгоритиов сжатия в цифровых видео системах делает довольно сложным включение этапа шифрования во всю систему в целом. Таким образом, для защиты содержания цифровых видео/изображений требуются особые системы шифрования.
За последние годы было предложено множество различных алгоритмов шифрования в качестве возможного решения проблемы защиты цифровых изображений и видео. Большинство из них являются объединенной схемой «сжатие-шифрование», которые специально разработаны для обеспечения надежной защиты MPEG видео, которое в свою очередь привлекает наибольшее внимание в силу заметного преобладания на рынке потребителей электроники.

Система шифрования «Perceptual Encryption»

Эта система находит применение в таких сферах как платное телевидение, видео по запросу и проч. Ее особенностью является то, что восприятие акустических/визуальных данных лишь частично ослабляется кодированием. Это дает возможность потенциальным пользователям слушать/просматривать «низкокачественные» версии мультимедийных продуктов перед покупкой. Желательно, чтобы степень ослабления непрерывно управлялась множителем p, который отражает процентное соответствие степени кодирования.



Рассмотрим эффективный алгоритм шифрования видео изображений PVEA (Perceptual Video Encryption Algorithm). Он устраняет многие недостатки своих предшественников:

-совместимость стандартов
-не имеет потерь качества визуализации
-сохраняет прежний размер после кодирования
-шифрует MPEG видео напрямую без создания промежуточных временных файлов
-не зависит от скорости передачи
-высокая скорость шифрования
-простота применения
-многомерная воспринимаемость
-защита от атаки по известному/выбранному открытому тексту

Остановимся подробно на атаке по известному открытому тексту. Вообще говоря, существует четыре разных способа обеспечить защиту от этой атаки:

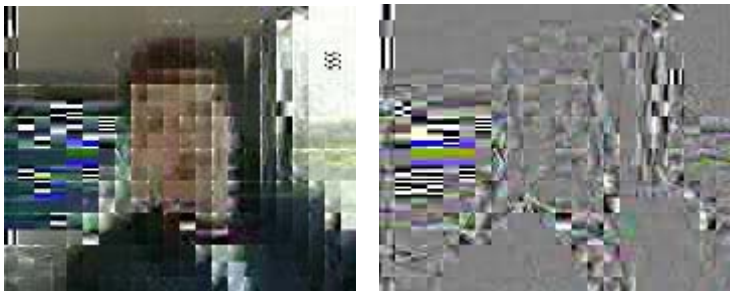
1. *Используя систему управления ключами и поточный шифр:* Когда в приложении доступна система управления ключами, может быть реализована процедура шифрования PVEA на основе поточного шифра. Для того, чтобы эффективно противостоять атаке по открытому тексту, секретный ключ поточного шифра должен непрерывно изменяться системой управления ключами. В большинстве случаев, достаточно изменять ключ для каждой картинки изображения.
2. *Используя поточный шифр с UID:* Когда система управления ключами не доступна в приложении, может использоваться уникальный идентификатор(UID), чтобы обеспечить защиту от атаки по известному открытому тексту, поскольку он гарантирует уникальность для разных видео. UID для MPEG видео может храниться в области пользовательских данных. Простейшим форматом UID является ID производителя плюс метка времени видео. Также можно определить UID с помощью хэш-функции или надежного генератора псевдо-случайных чисел(PRNG). В этом случае UID двух разных видео могут совпадать, но вероятность очень мала, если UID достаточно длинный(128 бит вполне хватает, чтобы обеспечить вероятность конфликта идентификаторов равной 2^{-128}). UID используется для инициализации поточного шифра вместе с секретным ключом, что обеспечивает шифрование различных видео различными потоками ключей. Таким образом, когда злоумышленнику удается заполучить поток для n известных/выбранных видео, он не может с их помощью взломать остальные. Естественно, применяемый поточный шифр должен быть надежным в том смысле, что секретный ключ не может быть получен из перехваченного сегмента потока ключей.
3. *Используя поточный шифр с обратной связью «открытый текст-шифротекст»:* После зашифровки каждого элемента исходных данных посылается открытый текст или шифротекст, чтобы поточный шифр кодировал следующий элемент. Таким образом, поток ключей, генерируемый поточным шифром, становится зависимым от всего исходного видео файла в целом, что делает бессмысленной рассматриваемую атаку. Заметим, что требуется начальный вектор для шифрования первого элемента.
4. *Используя блочный шифр:* С помощью блочного шифра довольно просто обеспечить защиту от атаки по известному открытому тексту. Поскольку длина различных дескрипторов элементов данных разная, для осуществления шифрования блочный шифр должен запускаться в режиме обратной связи(CFB) с

варьируемой длиной. Заметим, что в блочных шифрах существует n-битовая ошибка распространения в режиме CFB, где n – размер блока.

Было проведено множество экспериментов для выявления реального качества функционирования алгоритма шифрования PVEA. Результаты одного из них приведены на рисунке, в эксперименте выбирались различные значения 2-х факторов p_{sr} и p_{sd} . Как видно из рисунка, ослабления качества видео восприятия полностью зависит от этих двух факторов.

Fig. 1 The encryption results of the 1st frame in "Carphone": a) (psr, psd) = (0, 0) – the plain frame; b) (psr, psd) = (0, 0.2); c) (psr, psd) = (0, 1);
d) (psr, psd) = (0.2, 0); e) (psr, psd) = (0.2, 0.2); f) (psr, psd) = (0.5, 0.5); g) (psr, psd) = (1, 0); h) (psr, psd) = (1, 0.2); i) (psr, psd) = (1, 1).

Эксперименты также показали, что алгоритм PVEA надежен против атак основанных на маскировании ошибок(ECA). Для двух зашифрованных кадров, изображенных на рис.1, восстановленые изображения после применения ECA показаны на рис. 2. Очевидно, что качество изображения восстановленных кадров с помощью такой атаки даже гораздо хуже качества зашифрованных изображений, что означает – ECA не позволяет атакующей стороне получить полной видео информации. Фактически защита PVEA от ECA основана на том факте, что злоумышленник не может отличить зашифрованные данные от незашифрованных не получив ключ.



a) b)

Fig.2 The recovered results after applying ECA for the 1st frame in “Carphone”: a) breaking Fig. 1c; b) breaking Fig. 1i.

Итак, мы рассмотрели достаточно надежный алгоритм, который устраняет ряд недостатков ранее разработанных алгоритмов и обеспечивает защиту от различного вида атак.

Система хаотичного шифрования видео изображений(CVES)

Рассмотрим еще одну систему шифрования для видео.
Схема шифрования CVES не зависима от алгоритмов видеосжатия и, следовательно, не накладывает ограничений на формат кодируемого видео, обеспечивает высокий уровень защиты для цифрового видео в реальном времени с высокой скоростью шифрования, и может быть довольно просто реализована как аппаратной, так и программной частью.

Несколько слов о возникновении «хаотичной» криптографии. Первая научная статья появилась в 1989 году, в которой автор предложил новый поточный шифр, основанный на одномерной хаотичной схеме. В следующем году впервые была предложена система синхронизации и представлена надежная система сообщений через нее. С того момента началось развитие хаотичной криптографии в различных областях, главным образом в физике, электроннной инженерии, computer science и прикладной математике. Было разработано множество цифровых хаотичных шифров(Chaotic Ciphers - CC) и методы аналогового хаотичного безопасного сообщения; работы криптоаналитиков также были посвящены оценке надежности предложенных шифров.
Наиболее важными являются следующие проблемы: 1) *Скорость шифрования.* По сравнению с обычными шифрами, большинство CC имеют гораздо более низкую скорость шифрования. Это объясняется использованием множества итераций для шифрования одного блока открытого текста, использованием вычислений с плавающей точкой и сложных хаотичных схем. 2) *Какая схема должна использоваться?* Большинство хаотичных шифров должны использовать особые схемы для гарантии надежности, что ограничивает возможность широкого их применения. Желательно, чтобы шифр мог исправно работать с обширным множеством хаотичных схем. 3) *Как реализовывать хаотичные шифры, аппаратно или программно?* Хороший CC должен элементарно реализовываться как аппаратной так и программной частью, с низкими издержками.

Существует два основных способа создания цифровых CC:

1. Генерируя псевдо-случайные потоки ключей используя хаотичную систему для шифрования открытого текста.
2. Используя открытый текст и/или секретный ключ как начальные условия и/или управляющие параметры; применяя n раз прямую/обратную хаотичную схему для получения шифротекста. Первый способ соответствует поточному шифру, а второй блочному.

Исследуя существующие на настоящий момент цифровые СС можно выделить 3 факта:

1. Большинство блочных СС требуют многократного применения хаотичной системы шифрования для получения независимого шифротекста из открытого, что заметно снижает скорость шифрования.
2. Большинство поточных СС используют одну единственную хаотичную систему для генерации псевдо-случайных чисел для сокрытия открытого текста, что может снизить возможность потенциальных атак.
3. Поточные СС производят операцию шифрования гораздо быстрее блочных СС.

Схема CVES является композицией поточного и блочного СС. В ней заложены следующие основные принципы:

1. *Использование вычислений с фиксированной точкой вместо плавающей*. Это увеличивает скорость шифрования и, кроме того, упрощает аппаратную реализацию(т.е. снижает издержки) и улучшает портативность между различными платформами и аппаратными структурами.
2. *Использование простейших хаотичных алгоритмов.*
3. *Использование более масштабных единиц шифрования.* Для блочных шифров это означает увеличение размеров блока, для поточных – увеличение размера единичного ключа в потоке.

Схема хаотичного шифрования видео(CVES) изображена на рис. 3. Исходное видео зашифровывается кластер за кластером, причем кластер может составлять от одного до нескольких кадров. Естественно, мы можем рассматривать видео поток как непрерывный битовый поток безотносительно к каким-либо форматам считать фиксированное число бит исходным кластером.

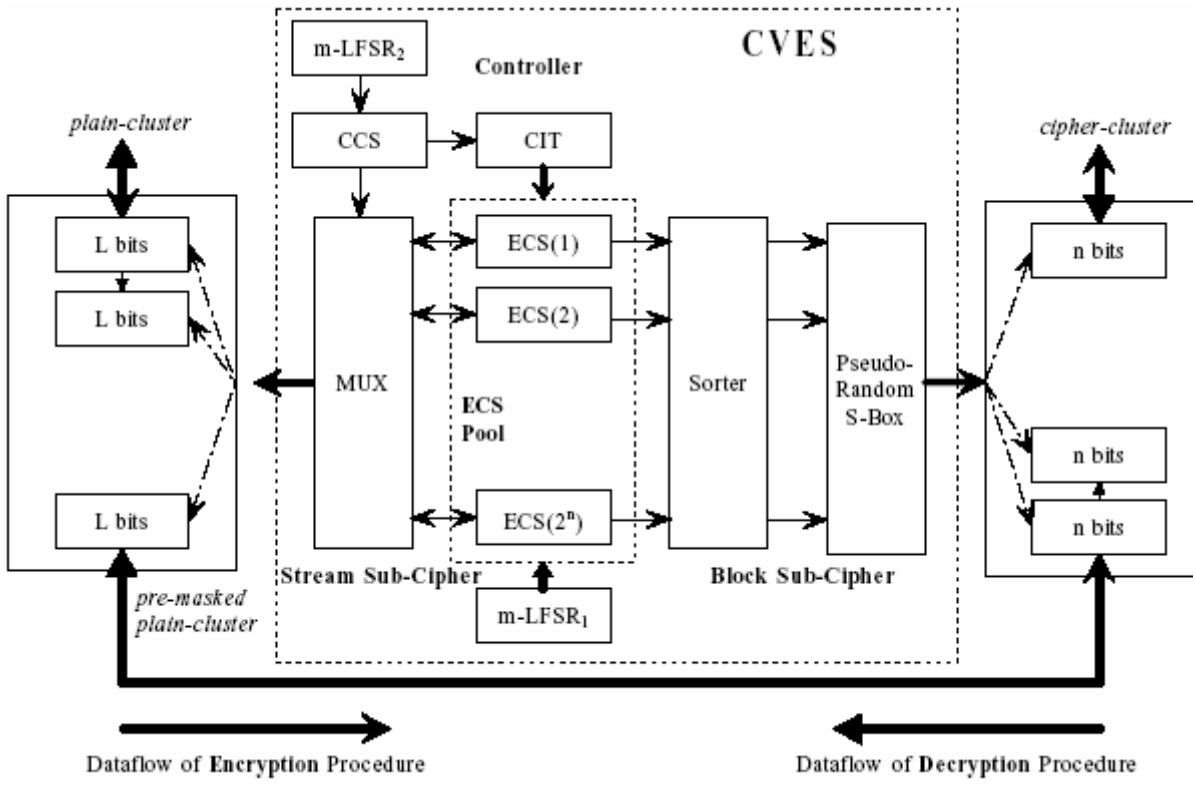


Fig. 3. Encryption and Decryption Procedure of CVES

Схема CVES содержит в себе следующие компоненты:

1. **ECS Pool** (Encryption Chaotic Systems): 2^n цифровых хаотичных систем составляют ядро CVES.
2. **CCS** (Control Chaotic Systems): Используются для управления инициализацией и применением 2^n алгоритмов ECS.
3. **CIT** (Control Information Table): Используется для хранения информации в CVES.
4. **Stream Sub-Cipher**: 2^n x 1 MUX управляемый CCS выбирает ECS для генерации L-битных хаотичных ключей.
5. **Block Sub-Cipher**: 2^n x 2^n L-битный сортировщик и 2^n n-битных единиц памяти составляют псевдо-случайный S-Box генератор.

На рис.4 изображен сравнительный анализ одного исходного кадра и зашифрованного кадра.

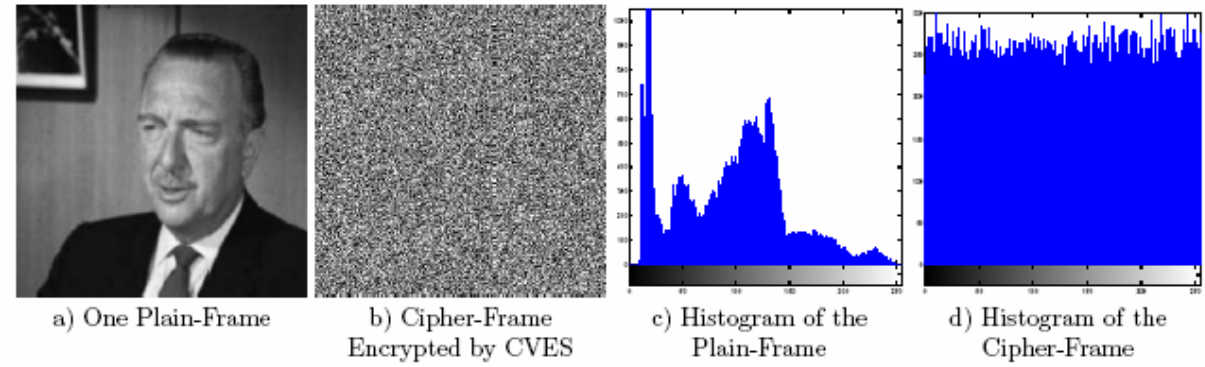


Fig. 4. Uncompressed Digital Video Encrypted with CVES

Заключение.

Мы рассмотрели различные методы защиты цифрового видео от разного рода атак на примере системы Perceptual Encryption и схемы CVES. Они имеют ряд преимуществ и усовершенствований, что отличает их от их предшественников и, кроме того, являются достаточно надежными для защиты от атак и поэтому находят широкое применение в видео индустрии, особенно для технологии MPEG.

Ссылки:

1. Shujun Li, Guanrong Chen, "On The Design of Perceptual MPEG-Video Encryption Algorithms": arxiv.org/pdf/cs.MM/0501014
2. Shujun Li, Xuan Zheng, Xuanqin Mou and Yuanlong Cai, "Chaotic Encryption Scheme for Real-Time Digital Video": www.hookee.com/Papers/WebRecords/ISTPRecord_SPIE_EI2002.htm
3. Carsten Griwodz, Oliver Merkel, "Protecting VoD the Easier Way" heim.ifi.uio.no/~griff/papers/58.pdf