УДК 681.3

ВЫБОР АЛГОРИТМА ПРЕОБРАЗОВАНИЯ, ОБЕСПЕЧИВАЮЩЕГО ИЗМЕНЕНИЕ СТРУКТУРЫ ИЗОБРАЖЕНИЯ

С. В. Беззатеев,
канд. техн. наук, доцент
М. Ю. Литвинов,
соискатель
Б. К. Трояновский,
доцент
Г. П. Филатов,
соискатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассматривается проблема выбора эффективного алгоритма преобразования видеоинформации в видеосистемах встраиваемого класса, обеспечивающего ее конфиденциальность при передаче и хранении. Предлагается модификация алгоритма VEA, позволяющая повысить защищенность информации в условиях атак по перехваченной преобразованной информации и выбранному исходному изображению и обеспечивающая эффективное уничтожение структуры передаваемой видеоинформации.

The authors studys the choice of an effective algorithm for the transformation of videoinformation in embidded video systems that ensures its confidentiality on keeping and transmission. A modification of the VEA algorithm is proposed. This modification increases the protection level of the information against the interception attacks and ensures an efficient destruction of the transmitted information.

Введение

Для решения задачи обеспечения конфиденциальности передаваемой и хранимой информации традиционно используется специальное преобразование, устойчивое к различного типа атакам. В контексте данной задачи наиболее эффективными и опасными являются атаки по парам исходное — преобразованное изображение и по выбранному исходному изображению. Кроме того, следует отметить необходимость предотвращения атак, связанных со спецификой исходной информации, — изображения, которое изначально содержит характерные фрагменты (контуры) и тем самым уже по умолчанию предполагает возможность атаки по парам исходное — преобразованное изображение. Задача выбора алгоритма преобразования осложняется спецификой видеосистем встраиваемого класса — существенными ограничениями на свободные вычислительный ресурс и объем оперативной памяти.

Потоковые и блоковые преобразования

Все преобразования условно разделяют на два типа — потоковые и блоковые. К потоковым преобразованиям относятся системы, использующие ключевые последовательности, генерируемые регистрами сдвига, и системы хаотичного преобразования (CVEC). Такие системы обеспечивают высокую скорость обработки информации, однако они неустойчивы к атакам с использованием перехваченных образцов обработанного и исходного изображения [14]. Системы блокового преобразования, в свою очередь, можно разделить на системы полного и частичного преобразования. Системы частичной обработки видеоинформации, использующие так называемые методы селективного преобразования, делятся на системы, учитывающие структуру видеоформата и ориентированные на обработку форматов сжатого изображения [1–6, 8–12], и системы, предназначенные для обработки несжатой информации [13]. Рассмотрим особенности этих подходов на примере нескольких наиболее известных алгоритмов.

1. Video Encryption Algorithm by Okao and Nahrstedt [8]. Основной идеей алгоритма является изменение статистических свойств видеоформата MPEG. Преобразование представляет собой аналог одного раунда сети Фейстейла. Первоначально весь информационный поток разбивается на блоки одинаковой длины (например, на байты), таким

а) *б*) *в*)

■ ***Рис. 1.*** *Пример использования алгоритма RVEA (а), алгоритма Video Encryption Algorithm (б) к исходному изображению (в)*

образом получается два списка — четные и нечетные байты. Результатом преобразования являются байты, полученные как побайтная сумма по модулю два (исключающее ИЛИ) четных и нечетных байт, и преобразованные с использованием симметричного алгоритма (AES, DES, ГОСТ 28147–89 и т. п.) нечетные или четные байты. Следует отметить недостаточную защищенность данного алгоритма при его использовании для обработки последовательности кадров и возможность применения атаки по выбранному исходному видеофрагменту. Очевидно, что данный недостаток может быть легко преодолен, если в алгоритме обработки использовать несколько раундов сети Фейстейла.

2. Одним из характерных примеров систем частичного преобразования, использующих структуру видеоформата, является семейство алгоритмов, ориентированных на стандарт MPEG [3]. Наиболее защищенным из этого семейства алгоритмов считается алгоритм RVEA, который обеспечивает защиту от атак как по перехваченному преобразованному изображению, так и по выбранному исходному изображению. В отличие от остальных алгоритмов этого семейства RVEA преобразует не только знаковые биты коэффициентов DCT, но и знаковые биты векторов движения формата MPEG. В общей сложности RVEA подвергает обработке около 10% всего объема MPEG-файла. Однако сравнение результатов обработки реального изображения алгоритмами, приведенными в работах [3, 8], наглядно демонстрирует преимущества первого алгоритма в случае, если стоит задача разрушить структуру передаваемого изображения (рис. 1).

3. Использование подхода частичного преобразования несжатого видеоизображения рассмотрено в работе [13]. Основной идеей является обработка не всего информационного блока для отдельной точки изображения, а только старших (одного или двух) бит для каждого блока. Для преобразования старших бит используются стандартные симметричные алгоритмы типа AES, DES, ГОСТ 28147–89 и т. п. Очевидно, что такой подход дает существенный выигрыш по затратам на обработку изображения. К сожалению, сами авторы отмечают достаточную устойчивость этого алгоритма к атакам по перехваченному изображению, подвергавшемуся преобразованию, лишь в случае, когда обрабатывалось не менее 50 % от объема каждого информационного блока.

Основываясь на проведенном анализе свойств существующих систем и учитывая требования, предъявляемые к системе преобразования видеопотока:

- защищенность к атаке по известному открытому изображению;
- полное разрушение структуры видеоинформации;
- защищенность от атаки по парам исходная — преобразованная видеоинформация;
- независимость от используемого видеоформата —

следует выбрать систему непрерывного, полного преобразования всего объема видеоинформации, используя потоковый или блоковый алгоритм. Кроме того, учитывая условие старения информации (ее актуальности), определяемое временным периодом до нескольких дней, можно использовать упрощенный вариант известных алгоритмов (таких как AES, DES, ГОСТ 28147–89).

Блоковое преобразование и его модификация

Для того чтобы блоковый алгоритм преобразования обладал свойством разрушения структуры видеоинформации, должно выполняться, по крайней мере, следующее свойство: одинаковые блоки исходного изображения должны преобразовываться в существенно отличающиеся друг от друга блоки обработанной информации, т. е. для любых $I_j = I_k$ $E(I_j) \neq E(I_k)$. Такое свойство для преобразования $E(*)$ может быть достигнуто двумя способами: постоянно меняющейся функцией $E(*)$ или использованием для преобразований функции от двух переменных — $E(*, K)$, где K — некоторый параметр, меняющийся для каждого нового блока исходного изображения. Рассмотрим возможные методы реализации каждого из перечисленных способов.

1. Постоянное изменение функции преобразования $E(*)$ может быть достигнуто либо с исполь-

зованием детерминированного алгоритма изменения функции $E(*)$, который должен сохраняться в тайне, либо с использованием некоторого случайного преобразования. Первый вариант, очевидно, сводится к введению дополнительного секретного параметра, позволяющего менять вид функции. Во втором варианте необходимо найти такое случайное преобразование, результат применения которого можно было бы легко восстановить, не зная самого преобразования. Одним из методов такого преобразования является использование помехоустойчивого кода в качестве детерминированной части преобразования $E(*)$, при этом секретом будет эффективный алгоритм декодирования (исправления ошибок) для выбранного кода. Случайной частью преобразования $E(*)$ будет генерация случайного вектора ошибки, вес Хэмминга которого не должен превышать числа ошибок, исправляемых кодом. В общем виде такое преобразование можно записать следующим образом:

$$p\mathbf{AGP} \oplus \mathbf{e} = c,$$

где p — информационный блок изображения длины k; $\mathbf{G}$ — порождающая матрица (n, k, d)-помехоустойчивого кода (здесь k — длина информационного блока, n — длина кодового слова, d — минимальное расстояние кода); $\mathbf{A}$ — матрица $(k \times k)$, имеющая обратную; $\mathbf{P}$ — матрица перестановок $(n \times n)$; $\mathbf{e}$ — случайный вектор ошибки длины n, $wt(\mathbf{e}) \le (d-1)/2$, являющийся в данном случае параметром K для выполняемого преобразования.

Для восстановления исходного блока изображения p первоначально используется алгоритм декодирования с исправлением случайного вектора ошибки $\mathbf{e}$, а затем из полученного кодового слова восстанавливается значение информационного блока. Устойчивость такого метода к различным атакам подтверждается безопасностью алгоритма Мак Эллиса, использующего такой же подход в несимметричных системах. Этот метод обработки видеоинформации может быть модифицирован, если использовать идею неравнозначных бит в информационном блоке [13] и, соответственно, помехоустойчивые коды с неравной защитой позиций в кодовом слове [15].

2. В данной статье предлагается использовать функцию от двух переменных, в качестве которой может выступать любой симметричный алгоритм блокового преобразования типа ГОСТ. Для обеспечения быстрой синхронизации при потере пакетов в распределенных IP-системах начальное значение параметра K_{i0} для пакета с номером i может быть установлено, например, следующим образом:

$$K_{i0} = F(K_0, i),$$

где K_0 — начальное значение параметра.

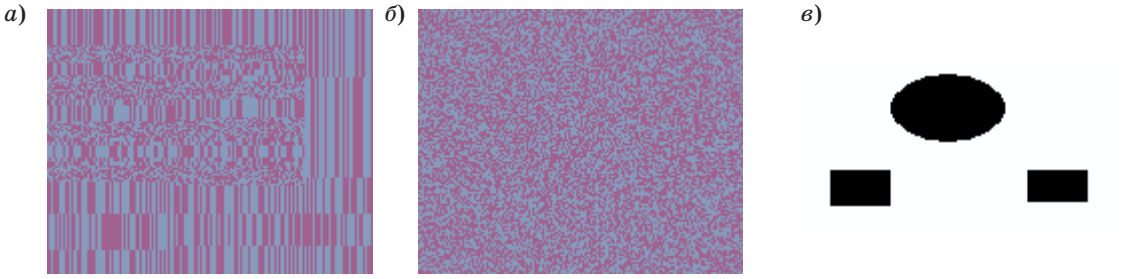
В качестве функции $F(*, *)$ может быть выбрано простое арифметическое сложение 256 битных чисел с игнорированием разряда переполнения.

Пример использования модифицированного блокового преобразования

Рассмотрим более подробно предлагаемый в данной работе блоковый алгоритм преобразования, адаптируемый по параметру защищенность/сложность реализации. За его основу взята модификация алгоритма VEA [8] и сеть Фейстейла со стандартным размером входного информационного блока в 64 бита и длиной параметра K 256 бит. На каждом раунде выполняются простейшие (аналогичные ГОСТ 28147–89) операции замены и перестановки. Число раундов можно изменять от 8 до 16 в зависимости от требуемого соотношения защищенность/сложность реализации. Для согласования алгоритма с требованиями использующего его приложения преобразованию подвергаются пакеты данных, длина которых может лежать в некотором ограниченном диапазоне, но последовательные пакеты могут иметь разные длины и не обязательно кратные длине информационного блока в 64 бита. Функция $K_{i0} = F(K_0, i)$ быстрой синхронизации реализована в виде, не зависящем от длины пакета, и использует некоторое, заранее фиксированное, количество операций арифметического сложения с игнорированием переполнения. Алгоритм был реализован в виде приложения на языке С и тщательно тестировался на различных изображениях. Проверялась эффективность алгоритма по изменению структуры аудиоданных.

а) *б*) *в*)

■ ***Рис. 2.*** *Пример использования предложенного алгоритма при одной модификации ключа на пакет длиной 1200 байт (а), на блок длиной 64 бита (8 байт) (б) для исходного изображения (в)*



■ ***Рис. 3.*** *Пример использования предложенного алгоритма при одной модификации ключа на пакет длиной 1200 байт (а), на блок длиной 64 бита (8 байт) (б) к исходному монохромному изображению (в)*

Примеры работы предложенного алгоритма по изменению структуры изображения представлены на рис. 2.

Более сложный случай — монохромные, высококонтрастные изображения (рис. 3).

Для получения достоверных оценок сложности программной реализации предлагаемого алгоритма программа была протестирована в инструментальной среде разработки Code Composer Studio ver. 3.1 фирмы Texas Instruments для 32-битного сигнального процессора семейства TMS64XX. Использовались только средства оптимизации компилятора языка С.

В качестве оценки сложности алгоритма выступает количество тактов на байт преобразуемой информации.

Характеристики вычислительной сложности

Количество раундов в алгоритме ГОСТ	8	16	32
Сложность (такты/байт)	25	47	91

Так, при 8 раундах преобразования процессор с тактовой частотой 600 МГц способен в реальном времени преобразовывать поток 24 Мбайт/с.

Заключение

Предложенная в работе модификация блокового преобразования с изменяющимся параметром позволяет обеспечить эффективное искажение структуры изображения и тем самым предотвратить наиболее распространенные методы атак. Само преобразование выполняется с использованием хорошо известной схемы сетей Фейстейла с не менее чем восьмью раундами, устойчивой ко всем известным в настоящее время атакам. Очевидным направлением повышения качества предложенного здесь метода является нахождение алгоритма случайной генерации параметра K блокового преобразования при обработке изображения, позволяющего выполнить обратное преобразование без знания значения K. Таким образом, представляется эффективным решение, которое позволило бы объединить преимущество схемы Мак Эллиса, использующей случайный параметр — вектор ошибки **e**, с простотой описанного в данной работе модифицированного блокового преобразования.

Литература

1. **Agi, Gong L.** An empirical study of secure MPEG video transmissions // ISOC Symposium on Network and Distributed Systems Security. San Diego, California. 1996. P. 137–144.
2. **Alattar M., Al-Regib G. I., Al-Semari S. A.** Improved selective encryption techniques for secure transmission of MPEG video bit-streams // International Conference on Image Processing (ICIP'99): Proc. of the 1999 IEEE. (IEEE Signal Processing Society. 1999).
3. **Bhargava B., Shi C., Wang Y.** MPEG Video Encryption Algorithms. http://raidlab.cs.purdue.edu/papers/mm.ps
4. **Cheng H., Li X.** On the application of image decomposition to image compression and encryption // Communications and Multimedia Security: Second Joint Working Conference on Communications and Multimedia Security, CMS'96. Chapman & Hall. Essen, Germany. Sept. 1996. P. 116–127.
5. **Cheng H., Li X.** Partial encryption of compressed images and videos // IEEE Transactions on Signal Processing. 2000. 48(8):2439–2451.
6. **Pommer, Uhl A.** Selective encryption of wavelet packet subband structures for obscured transmission of visual data // 3rd IEEE Benelux Signal Processing Symposium (SPS 2002): Proc (IEEE Benelux Signal Processing Chapter). Leuven, Belgium. Mar. 2002. P. 25–28.
7. **Qiao L., Nahrstedt K.** Comparison of MPEG encryption algorithms // International Journal on Computers and Graphics (Special Issue on Data Security in Image Communication and Networks). 1998. 22(3):437–444.
8. **Qiao L., Nahrstedt K.** A New Algorithm for MPEG Video Encryption. Proc. of the 1st International Conference on Imaging Science (Systems and Technology (CISST '97). Las Vegas, NV. July 1997. P. 21–29.
9. **Schneck P. A., Schwan K.** Authenticast: An adaptive protocol for high-performance, secure network applications: Technical report / Georgia Institute of Technology. Atlanta, GA, USA. 1997.

10. **Shi C., Bhargava B.** A fast MPEG video encryption algorithm: Proc. of the ACM Multimedia 1998. Boston, USA. 1998. P. 81–88.
11. **Skrepth C. J., Uhl A.** Selective encryption of visual data: Classification of application scenarios and comparison of techniques for lossless environments // Advanced Communications and Multimedia Security: Sixth Joint Working Conference on Communications and Multimedia Security CMS'02. Kluver Academic Publishing. Portoroz, Slovenia. Sept. 2002.
12. **Tang L.** Methods for encrypting and decrypting MPEG video data efficiently: Proc. of the ACM Multimedia 1996. Boston, USA. Nov. 1996. P. 219–229.
13. **Podesser M., Schmidt H.-P., Uhl A.** Selective bitplane encryption for secure transmission of image data in mobile environments. http:/www.cosy.sbg.ac.at/~uhl/norsig_slides.pdf
14. **Li S., Li C., Chen G.** Cryptanalysis of the RCES/RSES Image Encryption Scheme: Elctronic preprint. IACR's Cryptology ePrint Atchive: Report 2004/376. 2004.
15. **Bezzateev S., Shekhunova N.** Generalized Goppa codes for correcting localized errors: Proc. of ISIT-98. Boston, USA. 1998. P. 377.

СВЯЗЬ. АВТОМАТИЗАЦИЯ. ЭЛЕКТРОНИКА. ИНДУСТРИЯ БЕЗОПАСНОСТИ-2007 СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА

20–23 марта 2007 г.

Место проведения: 644033, Россия, г. Омск, ул. Красный Путь, 155, корп.1

Организаторы

Международный выставочный центр «ИНТЕРСИБ»
Правительство Омской области
Администрация города Омска

Направления работы выставки

Связьинфо. Интернет-техком

Специализированный салон системных решений информационных технологий, сети, сетевые телекоммуникационные и Интернет/интранет-технологии
Автоматизированные системы связи и системы управления связью
Системы и аппаратура радиосвязи, спутниковой и космической связи
Средства телевидения и радиовещания
Системы и аппаратура передачи данных, коммутационное оборудование
Системы и оборудование для обеспечения контроля и безопасности систем и сетей связи и т. д.
Радиоизмерительная техника
Периферийное оборудование для обработки данных
Рабочие и прикладные программы любого назначения
Сети
Сетевое оборудование и комплексные системы обеспечения телекоммуникационных систем связи
Оборудование и комплексные решения для внешних и локальных сетей связи
Комплексные решения по коммуникационной поддержке деятельности предприятий малого и среднего бизнеса

Автоматизация

Системы и технологии автоматизации производства, проектирования и управления
Технические средства, системы и компоненты автоматического контроля и управления
Периферийное оборудование
Лазерная техника
Обработка изображений в промышленном процессе
Обеспечение и контроль качества
Информационные технологии и программное обеспечение

Электроника

Электронные компоненты
Полупроводники
Встроенные системы
Микропроцессоры
Сенсоры и микросистемы
Печатные платы
Компоненты и субсистемы
Технологии, оборудование и материалы для электронных производств
Оптическое, лазерное и радиоэлектронное оборудование
Электромеханические компоненты и соединительные технологии
Электронная техника

Технологии безопасности. Средства МЧС

Системы контроля и управления доступом; считыватели и идентификаторы; домофоны; устройства для персонализации и защиты карт СКУД; антикражные системы
Системы охранной сигнализации; периметральные средства обнаружения; приемно-контрольная аппаратура; средства оповещения; вспомогательное оборудование
Системы телевизионного наблюдения; устройства усилительные и аккумулирующие; аппаратура приема, регистрации, обработки и передачи изображения; вспомогательные аксессуары и др.

Дополнительная информация

http://www.exponet.ru/exhibitions/by-id/industrysecurityom/industrysecurityom2007/index.ru.html