УДК 681.3

ИСПОЛЬЗОВАНИЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ ДЛЯ ШИФРАЦИИ ВИДЕОИНФОРМАЦИИ

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

Рассматривается вариант модификации схемы Мак Элиса для преобразования видеоинформации с целью обеспечения ее конфиденциальности при передаче и хранении. Предлагаемая схема позволяет решить специфическую задачу уничтожения контуров и фоновых текстур в процессе обработки исходного изображения и в то же время исключить необходимость синхронизации приемного и передающего устройств.

In this article, a variant of the Mac Eliece scheme for modification of video information with the purpose to provide its secure transmission and storage is discussed. The suggested scheme allows for solving the specific task of destroying the outlines and background textures of the original image during processing without necessity to synchronize the receiver and the transmitter.

Введение

В настоящее время проблема обеспечения конфиденциальности при хранении видеоизображения получила дальнейшее развитие в связи с широким использованием корпоративных цифровых копировальных аппаратов (http://www.sharpusa.com/files/cop_dow_Security_Solutionsbro.pdf). Для того чтобы исключить «узнаваемость» контуров или фоновых текстур в зашифрованном сообщении для обработки видеоизображения, принято использовать либо потоковый шифр, либо блоковый шифр в режиме изменяющегося ключа. В работе [1] анализировалась эффективность использования упрощенного алгоритма шифрования ГОСТ 28147–89 с изменяющимся ключом для обработки видеоинформации. Существенной проблемой такого подхода является необходимость обеспечения синхронного использования ключевой последовательности на приемной и передающей стороне и соответственно необходимость синхровставок в передаваемую информацию. Кроме того, в таких системах и передающая, и приемная сторона обладают всей необходимой информацией (ключ, алгоритм, устройство) для шифрации и дешифрации передаваемых и обрабатываемых сообщений. Таким образом, компрометация передающего устройства приведет к раскрытию всей конфиденциальной информации.

Во многих случаях передающее устройство, в отличие от приемного, находится вне контролируемой зоны и соответственно может быть доступно злоумышленнику. При такой постановке задачи особенно важным видится разработка системы обработки (шифрации) видеоинформации, имеющей несимметричную схему, т. е. системы, в которой получение доступа к устройству обработки информации на передающей стороне не приводит к полной компрометации всей системы.

Система Мак Элиса несимметричного шифрования, использующая коды, исправляющие ошибки

Хорошо известно, что задача декодирования помехоустойчивого кода с исправлением случайных ошибок в пределах корректирующей способности кода в общем случае является NP-сложной задачей. Сложность декодирования может быть существенно снижена (до полиномиальной) при наличии у кода конструктивного алгоритма декодирования. Одним из классов кодов, имеющих такой конструктивный алгоритм декодирования, являются коды, предложенные В. Д. Гоппой в 1970 г. [2]. Коды Гоппы задаются двумя объектами — множеством локаторов (нумераторов) позиций L и многочленом Гоппы $g(x)$.

q-ичный вектор длины n $\boldsymbol{a} = (a_1, a_2, ..., a_n)$ является кодовым словом (L, g)-кода Гоппы, если выполняется следующее сравнение:

$$\sum_{i=1}^{n} a_i \frac{1}{x - \alpha_i} \equiv 0 \bmod g(x),$$

где $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\alpha_i \in GF(q^m)$ и $g(x)$ — многочлен с коэффициентами из $GF(q^m)$, не имеющий среди своих корней элементов из L, т. е. $g(\alpha_i) \neq 0$, $q^m \geq n$ и q — простое или степень простого числа.

Для выполнения процедуры кодирования используется порождающая матрица кода **G**. То есть, чтобы получить кодовое слово (n, k)-кода, соответствующее некоторому информационному сообщению $\mathbf{p} = (p_1, p_2, ..., p_k)$, достаточно умножить вектор **p** на порождающую матрицу кода **G**:

$$\mathbf{a} = \mathbf{pG}.$$

Для построения порождающей матрицы (L, g)-кода сначала необходимо построить проверочную матрицу **H**, используя множество L и многочлен $g(x)$:

$$\mathbf{H} = \begin{vmatrix} \frac{1}{g(\alpha_1)} & \frac{1}{g(\alpha_2)} & \cdots & \frac{1}{g(\alpha_n)} \\ \frac{\alpha_1}{g(\alpha_1)} & \frac{\alpha_2}{g(\alpha_2)} & \cdots & \frac{\alpha_n}{g(\alpha_n)} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \frac{\alpha_2^{t-1}}{g(\alpha_2)} & \cdots & \frac{\alpha_n^{t-1}}{g(\alpha_n)} \end{vmatrix},$$

где $t = \deg g(x)$.

Имея проверочную матрицу **H**, легко построить порождающую матрицу кода **G**: $\mathbf{GH}^{\mathrm{T}} = 0$, используя метод Гаусса приведения матрицы **H** к диагональному виду. Для получения матрицы, обеспечивающей шифрующее преобразование, необходимо дополнительно выбрать две матрицы. Произвольную неособую (имеющую обратную) матрицу **A** размером $k \times k$ и произвольную перестановочную матрицу **P** размером $n \times n$.

Таким образом, шифруемая информация будет разбиваться на q-ичные блоки $\mathbf{p} = (p_1, p_2, ..., p_k)$ длиной k и подвергаться следующему преобразованию:

$$c = \mathbf{p} \cdot \mathbf{A} \cdot \mathbf{G} \cdot \mathbf{P} \oplus \mathbf{e},$$

где **A** — неособенная (обратимая) матрица $(k \times k)$; **G** — порождающая матрица кода Гоппы $(k \times n)$; **P** — произвольная перестановочная матрица $(n \times n)$; **e** — случайный вектор ошибки весом $t/2$.

Алгоритм декодирования-дешифрации выглядит следующим образом.

1. Принятое сообщение умножается на матрицу $\mathbf{P}^{-1}$, обратную к перестановочной матрице **P**:

$$c \cdot \mathbf{P}^{-1} = (\mathbf{p} \cdot \mathbf{A} \cdot \mathbf{G} \cdot \mathbf{P} \oplus \mathbf{e})\, \mathbf{P}^{-1} =$$

$$= \mathbf{p} \cdot \mathbf{A} \cdot \mathbf{G} \cdot \mathbf{P} \cdot \mathbf{P}^{-1} \oplus \mathbf{e} \cdot \mathbf{P}^{-1} =$$

$$= \mathbf{p} \cdot \mathbf{A} \cdot \mathbf{G} \oplus \mathrm{e} \cdot \mathbf{P}^{-1} = \mathbf{p}' \cdot \mathbf{G} \oplus \mathbf{e}',$$

где $\mathbf{p}' = \mathbf{p} \cdot \mathbf{A}$ — измененное информационное сообщение; $\mathbf{e}' = \mathbf{e} \cdot \mathbf{P}^{-1}$ – случайный вектор ошибки весом $t/2$.

Таким образом, получится кодовое слово (L, g)-кода, сложенное со случайным вектором ошибки.

2. Зная многочлен Гоппы $g(x)$ и множество локаторов позиций, можно найти и исправить вектор ошибок $\mathbf{e}'$, используя конструктивный алгоритм декодирования (Берликэмпа—Мэсси, Евклида).

3. Зная порождающую матрицу кода **G** и матрицу **A**, легко восстановить сначала измененное информационное сообщение $\mathbf{p}'$, а затем и исходное информационное сообщение **p**:

$$\mathbf{p}' \cdot \mathbf{A}^{-1} = \mathbf{p} \cdot \mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{p}.$$

Модификация схемы Мак Элиса для шифрации видеоизображения

Для эффективного использования описанной схемы необходимо выбрать параметры (L, g)-кода, обеспечивающие эффективную обработку исходной информации и достаточный уровень защищенности. Как известно [3], защищенность такой схемы, даже в случае разглашения информации о параметрах кода (длина кодового слова, длина информационного сообщения и число исправляемых ошибок), определяется числом различных многочленов Гоппы степени t:

$$N = O\left(\frac{q^t}{t}\right),$$

где коэффициенты многочленов Гоппы выбираются из поля $GF(q)$.

Например, при выборе двоичного кода (256, 128, 33) с многочленом Гоппы степени 16 и коэффициентами из $GF(2^8)$ мы получим систему, защищенность которой будет оцениваться величиной $O(2^{124})$.

На передающем (шифрующем) устройстве имеется лишь информация об открытом ключе (матрица $\mathbf{G}' = \mathbf{A} \cdot \mathbf{G} \cdot \mathbf{P}$ и генератор ошибок заданного веса t). Получение информации о шифрующей матрице не позволяет определить многочлен Гоппы, а следовательно, не дает возможности исправлять случайные ошибки, «накладываемые» на передаваемое изображение. Использование такого алгоритма обработки видеоизображения позволяет решить сразу две задачи:

— нет необходимости синхронизировать приемное и передающее устройства (зная многочлен Гоппы на приемном устройстве, всегда можно исправить любые ошибки весом до t);

— передающее устройство не содержит конфиденциальной информации, и его компрометация не позволяет правильно декодировать искаженное видеоизображение.

Следует отметить, что особенностью шифрования видеоизображения является наличие довольно большого числа информационных блоков, имеющих одно и то же значение (фоновые текстуры, контуры и т. д.). Для обеспечения преобразования совпадающих информационных блоков в различные зашифрованные сообщения в рассмотренном выше алгоритме используются векторы ошибок весом до t. Однако при наличии достаточного числа (больше трех) одинаковых информационных блоков можно использовать мажоритарный метод исправления ошибок. Для предотвращения такой атаки можно использовать сгенерированный случайный вектор ошибки для «искажения» значения информационного блока. Легко оценить число таких возможных «искажений»

$$K = \binom{n}{t}.$$

Рассмотрим некоторые способы «искажения» информационного сообщения, аналогичные используемым в схеме Мак Элиса для «искажения» кодового слова.

Схема Rao-Nam [4] предполагает использование для этой цели специального кодового слова, заранее выбранного из общего списка кодовых слов. То есть для каждого вектора ошибки, являющегося лидером смежного класса в таблице стандартной расстановки кода, выбирается соответствующее кодовое слово, список таких кодовых слов является элементом секретного ключа. Процедура шифрования в соответствии со схемой Rao-Nam выглядит следующим образом:

$$c = \mathbf{p} \cdot \mathbf{G}' \oplus \mathbf{e}' \cdot \mathbf{P},$$

где $\mathbf{e}' = \mathbf{e} \oplus l$, l — кодовое слово, соответствующее вектору ошибки $\mathbf{e}$, $wt(\mathbf{e}) \le t$; $\mathbf{G}' = \mathbf{A} \cdot \mathbf{G}$.

Очевидно, что эта процедура может быть переписана в следующем виде:

$$c = (\mathbf{p} \oplus \lambda) \cdot \mathbf{G}' \oplus \mathbf{e} \cdot \mathbf{P},$$

где λ — информационное сообщение, соответствующее кодовому слову l: $l = \lambda \cdot \mathbf{A} \cdot \mathbf{G}$.

Очевидным недостатком данной схемы является необходимость хранить кодовые слова $\{l\}$ или информационные сообщения $\{m\}$, соответствующие всем лидерам смежных классов, как на приемной, так и на передающей стороне.

Второй известной модификацией схемы Мак Элиса является схема, предложенная в работах [5, 6] и использующая структуру схемы Эль Гамаля. В этой схеме зашифрованное сообщение состоит из трех частей c_1, c_2, c_3 и получается следующим образом:

$$c_1 = \mathbf{p} \cdot (\mathbf{G}' \oplus \mathbf{S}_m \cdot \mathbf{D}_m) \oplus \mathbf{e} \cdot (\mathbf{P} \cdot \mathbf{X} \oplus \mathbf{S}_e \cdot \mathbf{D}_e),$$

где $\mathbf{e}$ — случайный вектор ошибки длиной n, $wt(\mathbf{e}) \le t$; $\mathbf{G}' = \mathbf{A} \cdot \mathbf{G} \cdot \mathbf{X}$; $\mathbf{X}$ — несингулярная матрица $n \times n$; $\mathbf{S}_m$ — случайная матрица $k \times n$; $\mathbf{D}_m$ — случайная матрица $n \times n$; $\mathbf{P}$ — случайная перестановочная матрица $n \times n$; $\mathbf{S}_e$ — случайная матрица $k \times n$; $\mathbf{D}_e$ — случайная матрица $n \times n$;

$$c_2 = \mathbf{e} \cdot \mathbf{S}_e;$$

$$c_3 = \boldsymbol{p} \cdot \mathbf{S}_m;$$

$$c = c_1 \| c_2 \| c_3.$$

Открытым ключом, используемым на передающей стороне для преобразования исходной информации $\mathbf{p}$, являются матрицы $\mathbf{G}' \oplus \mathbf{S}_m \cdot \mathbf{D}_m$, $\mathbf{P} \times \times \mathbf{X} \oplus \cdot \mathbf{S}_e \cdot \mathbf{D}_e$, $\mathbf{S}_e$, $\mathbf{S}_m$.

С точки зрения решаемой нами задачи — уничтожения структуры видеоизображения, данная схема оказывается неприемлемой из-за наличия в каждом зашифрованном сообщении компоненты c_3, которая будет иметь одинаковые значения для одинаковых исходных сообщений, т. е. одинаковые фрагменты изображения могут быть легко распознаны по этой компоненте.

Третьим вариантом, также имеющим структуру схемы Эль Гамаля, является вариант схемы Мак Элиса, предложенный в работе [7]. Здесь, так же как и в предыдущем случае, зашифрованное сообщение состоит из трех компонент c_1, c_2, c_3 и получается следующим образом:

$$c_1 = (c_1^1, c_1^2, \ldots, c_1^i, \ldots, c_1^k),\ c_1^i = p_i \beta_i \mod q,$$

где β_i — случайные числа из $GF(q)$;

$$c_2 = \begin{vmatrix} \beta_1 & 0 & 0 & \ldots & 0 \\ 0 & \beta_2 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & \beta_k \end{vmatrix} (\mathbf{G}' \oplus \mathbf{R}') \oplus \mathbf{E} \cdot \mathbf{P}',$$

где $\mathbf{E}$ — случайная матрица $n \times n$, над $GF(q)$ каждая строка которой имеет не более t ненулевых элементов; $\mathbf{R}'$ — случайная матрица $k \times n$ с элементами из $GF(q)$; $\mathbf{P}'$ — случайная перестановочная матрица $n \times n$ с элементами из $GF(q)$; $\mathbf{G}'$, $\mathbf{R}'$ и $\mathbf{P}'$ — матрицы, составляющие открытый ключ;

$$c_3 = \mathbf{T}\mathbf{G}' \oplus \mathbf{E},$$

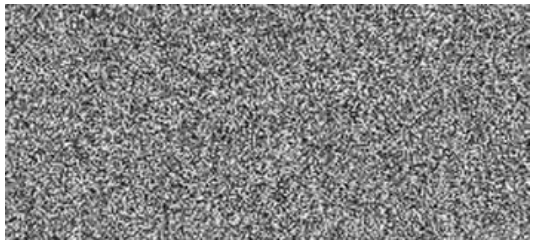
где $\mathbf{T}$ — произвольная матрица $k \times k$ с элементами из $GF(q)$.

Очевидно, что такой вариант модификации схемы Мак Элиса в большей степени подходит для решения нашей задачи — разрушения структуры изображения, однако основным недостатком данной схемы является более чем трехкратное увеличение объема передаваемой информации.

В данной статье для решения поставленной задачи предлагается некоторая модификация схемы Rao-Nam, вариант которой для обеспечения повышения информационной скорости передачи информации и скрытности рассмотрен в работе [8]. Использование такой модификации позволяет избе-

а)

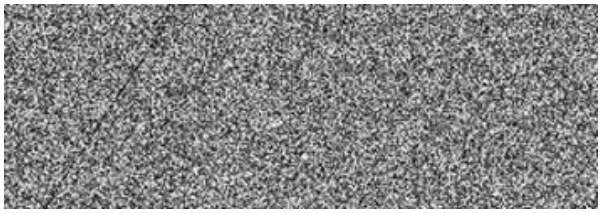
Исходное изображение



Преобразованное изображение

б)

Исходное изображение



Преобразованное изображение

■ *Пример использования модифицированной схемы Мак Элиса*

жать хранения массива кодовых слов на передающей и приемной стороне для их использования в качестве секретного ключа. Вместо хранения такого массива предлагается использовать некоторое преобразование вектора **e** длиной n в вектор **f** длиной k. Простейшим и эффективным вариантом такого преобразования может быть хэш-функция, т. е. предлагаемая схема может быть описана следующим образом [8]:

$$c = (\mathbf{p} \oplus \mathbf{f}) \cdot \mathbf{G}' + \mathbf{e} \cdot \mathbf{P},$$

где $\mathbf{f} = \text{hash}(\mathbf{e})$.

В работе [8] описанный выше метод использовался для повышения информационной скорости передачи зашифрованных данных. Для решения рассматриваемой задачи — максимального изменения структуры изображения возможно также использование случайных чисел, генерируемых в виде векторов ошибки **e**, $wt(\mathbf{e}) \le t$ для создания случайной несингулярной матрицы **A*** размерности $k \times k$: $\mathbf{f}: \mathbf{e} \to \mathbf{A}^*$. Полученную матрицу **A*** можно использовать для преобразования исходной информации следующим образом:

$$c = \mathbf{p} \cdot \mathbf{G}'^* + \mathbf{e} \cdot \mathbf{P},$$

где $\mathbf{G}'^* = \mathbf{A}^* \cdot \mathbf{G} \cdot \mathbf{P}$.

Для рассмотренного выше примера (256, 128, 33) кода Гоппы число возможных различных векторов ошибки весом 16 составляет величину $O(2^{82})$ и соответственно каждый из 2^{128} информационных векторов может быть преобразован с помощью случайного вектора **f** или матрицы **A*** в один из 2^{82} возможных случайных информационных векторов. Очевидно, что такая модификация схемы Мак Элиса позволяет избежать преобразования одинаковых фрагментов видеоизображения в мало отличающиеся (не более чем в $2t$ позициях) зашифрованные сообщения.

Пример работы рассмотренной системы при выбранных параметрах кода изображен на рисунке *а*, более сложный случай — на рисунке *б*.

Литература

1. **Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П.** Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения // Информационно-управляющие системы. 2006. № 6. С. 2–5.
2. **Гоппа В. Д.** Новый класс линейных помехоустойчивых кодов // Проблемы передачи информации. 1970. Т. 6. № 3. С. 24–30.
3. **McEliece R. J.** A public-key cryptosystem based on algebraic coding theory, DSN Progress Report, Jet Propulsion Laboratory, Pasadena, CA. Jan/Feb. 1978. P. 114–116.
4. **T. R. N. Rao, Kil-Myun Nam.** Private-key algebraic-code encryptions // IEEE Trans. on Information Theory. 1989. Vol. 35. N 4. P. 829–833.
5. **Krouk E.** A new public-key cryptosystem: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory. 1993. P. 285–286.
6. **Gabidulin E. M.** Public-key cryptosystem based on linear codes. 1995.
7. **Jian-feng M. A., Teechye Chiam, Kot Chichung Alex.** A novel encryption method with its application in the copyright protection of digital data // Journal of Software. 2002. Vol. 13. N 3. P. 330–334.
8. **Фам Суан Нгиа.** Модификации алгоритма Мак Элиса для повышения показателей качества радиосистем передачи информации: Автореф. дис. ... канд. техн. наук / Рязанский государственный радиотехнический университет. Рязань. 23 мая 2007.