# ШИФРОВАНИЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ С СОВМЕСТНЫМ РАНДОМИЗИРОВАННЫМ ЭНТРОПИЙНЫМ КОДИРОВАНИЕМ И ВРАЩЕНИЕМ В РАЗБИТОМ БИТОВОМ ПОТОКЕ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Мельничук О.В.*

*Борискевич А.А – д.т.н., профессор.*

В современном обществе успех любого вида деятельности сильно зависит от обладания определенными сведениями (информацией) и от отсутствия их (ее) у конкурентов. Чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации привело к возникновению индустрии средств ее защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности.

Одна из наиболее важных задач – задача кодирования сообщений и шифрования информации.

В данной работе, проблемы мультимедийного шифрования исследуется под новым углом зрения. Если тщательного сравнивать между мультимедийными процессами сжатия и шифрования с точки зрения теории информации, отметим, что оба могут в целом рассматривается как процесс удаления избыточности, содержащейся во входных данных. Основное различие между ними состоит в том, что секретный ключ контролирует операции шифрования, в то время как все операции по сжатию осуществляются в соответствии с некоторыми стандартами. Новый подход шифрования состоит из двух этапов. Первый этап называется рандомизированное энтропийное кодирование (РЭК). Основная идея РЭК заключается в использовании нескольких энтропийных параметров кодирования или параметров соответствующих случайной последовательности внутри энтропийного кодера. Второй называется вращение в разделенных битовых потоках (ВРБП), которая дополнительно выполняет случайные вращения на выходе стадии РЭК для получения окончательного битового потока. [1]

Алгоритм метода шифрования состоит из следующих шагов:

1. Рандомизированное энтропийное кодирование исходной последовательности символов. Рассмотрим шифрование источника информации $I$ на основе рандомизированных таблиц Хаффмана. В начале генерируется $M = 2^m$ различных кодовых таблиц Хаффмана, пронумерованных от 0 до $M-1$. Данные таблицы могут быть обнародованы. Далее выбирается криптографически безопасный ПБГ (Псевдослучайный битовый генератор). Генерируется случайное число $z$, которое и является ключом шифрования РТХ. $z \leftarrow$ первый результат генератора ПБГ. Затем идет разбивает $z$ на $m$-битные блоки. Записывается $z = t_1 \| t_2 \| \ \dots \ \| t_k, (t_i = 0 \text{ до } M-1)$. Используется $t_i$ таблица Хаффмана для кодирования одного символа ($i = 1$ до $k$). Если $i = k+1$, возвращаемся к выбору криптографически безопасного ПБГ, и повторяем до завершения кодирования.

Законным владелец знает ключ (случайное число $s$). Таким образом, он в состоянии воспроизвести ключ, сгенерированный ПБГ и используемый в шифровании, что в свою очередь, позволит корректно декодировать битовый поток [1].

2. Перемешивание сегментированной кодированной битовой последовательности на основе вращения. Сжатый зашифрованный битовый поток сначала разбивается на блоки заданных (ключом разбиения) размеров, а затем осуществляется круговое случайное вращение в рамках каждого блока.

Многие операции могут быть использованы для изменения порядка бит в блоке. Перестановка всех бит перемешивает порядок бит наиболее полно, но требует много вычислений. Чтобы уменьшить сложность и облегчить битовый поток обработки, мы ограничиваем манипуляции с битами до простого левого вращения.

Для блока $n$ бит $A = (a_1 a_2 \dots a_n)$, $r$-битное левое вращение преобразует $A$ в $(a_{r+1} a_{r+2} \dots a_n a_1 a_2 \dots a_r)$, вращая (перемещая) первые $r$ бит конец $A$.

Пусть $A = (a_1 a_2 \dots a_N)$, битовый поток длиной $N$. $(p, r)$-значения вращения и разделения блоков $A$, обозначаемые $\text{ВБП}(A, p, r)$ с $p = (p_1 p_2 \dots p_m)$, и $r = (r_1 r_2 \dots r_m)$, получают следующие 2 шага:

- Разделение $A$ на $m$ блоков $A_i$ длинной $p_i$, $i = 1, 2, \dots, m, \sum_{i=0}^{m} p_i = N$;
- Выполнение $r_i$-битных левых вращений на каждый блок $i = 1, 2, \dots, m$.

Схема алгоритма вращения в разбитом битовом потоке (ВБП) представлена на рисунке 1.

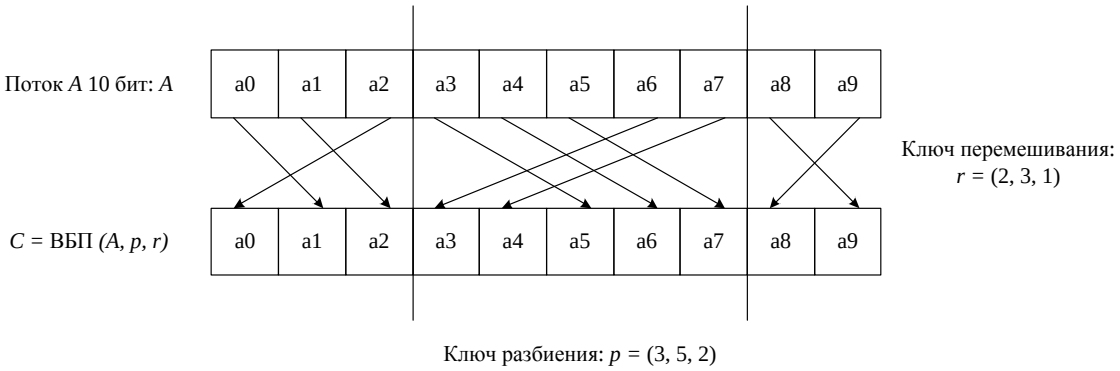
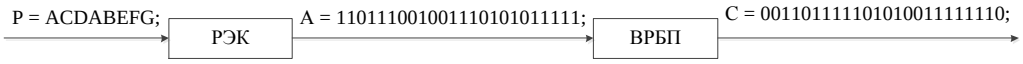



Рис. 1 – Схема алгоритма вращения в разбитом битовом потоке (ВБП)

3. Окончание алгоритма. Конечным результатом работы алгоритма будет являться бинарная последовательность $C$ , первоначально прошедшая через блок РЭК где было осуществлено ее сжатие и кодирование а затем через ВБП для обеспечения более надежного уровня защиты [2].




$P = ACDABEFG$ – входная последовательность символов, составленная из символов $I$ источника входного сигнала; $A = 11011100100111010101111$ – сжатая и закодированная бинарная последовательность на выходе блока РЭК; $C = 00110111110101001111111 10$ – конечная перемешанная бинарная последовательность, полученная на выходе блока ВБП;

Рис. 2 – Схема иллюстрирующая процесс работы алгоритма

РЭК / ВРБП парадигма шифрования имеет несколько преимуществ. Во-первых, конструкция использует структуру энтропии кодера, таким образом, требует незначительной стоимости для реализации в аппаратном или программном обеспечении. Во-вторых, шифрование не ухудшает степень сжатия в том смысле, что размер зашифрованного потока точно такой же, как и при стандартном сжатии. С точки зрения безопасности, предлагаемая нами схема может выдержать различные типы атак. [3]

Список использованных источников:

1. Wuand C.P., Kuo C.C.J. // Efficient multimedia encryption via entropy codec design in Security and Watermarking of Multimedia Contents, vol. 4314 of Proceedings of SPIE, San Jose, Calif, USA, 2001, pp. 128–138.
2. Xie D., Kuo C.-C.J. // EURASIP Journal on Information Security, 2007, Los Angeles, CA 90089-2564, USA, 2007.
3. Bose R., Pathak S., // IEEE Transactions on Circuits and Systems I, vol. 53, no. 4, 2006, pp. 848–857.