

**Ф. К. Алиев, А. В. Зайцева, В. А. Киселенко** (Москва, ТВП, МГТУ). **О возможности изменения плотности распределения вероятностей амплитуды шума квантования цифрового мультимедийного сигнала при использовании его сжатых образов в стеганографических приложениях.**

В некоторых алгоритмах сжатия мультимедийных сигналов на этапе квантования осуществляется округление до ближайшего целого числа. К таким алгоритмам относятся МРЗ [3], JPEG [7], MPEG-2 [4–6] и другие. Обозначим  $G_i$  ( $i \in \{1, 2, \dots, n\}$ ) —  $i$ -й элемент цифрового мультимедийного сигнала  $X = \{G_1, G_2, \dots, G_n\}$ , представленного в частотной области. Квантованный коэффициент  $g_i$  — это число, получаемое при округлении величины  $G_i/\Delta_i$  до ближайшего целого числа, где  $\Delta_i$  — расстояние между соседними уровнями квантования коэффициента  $G_i$ . При восстановлении мультимедийного сигнала по его сжатому образу вместо элемента  $G_i$  будет получена величина  $g_i\Delta_i$ , что в большинстве случаев будет отличаться от истинного значения  $G_i$ . Разность  $y_i = g_i\Delta_i - G_i$  называется *ошибкой квантования* или *амплитудой шума квантования*, а конечная последовательность  $Y = \{y_1, y_2, \dots, y_n\}$  — *шумом квантования* [1]. Амплитуда шума квантования  $y_i$  попадает в промежуток  $\bar{\Delta}_i = (-0,5\Delta_i, 0,5\Delta_i]$ .

Отметим, что в общем случае в квантователях алгоритмов сжатия, применяемых к мультимедийным сигналам, расстояния между соседними уровнями квантования разных коэффициентов могут не совпадать, т. е. расстояние  $\Delta_i$  между соседними уровнями квантования коэффициента  $G_i$  может не совпадать с расстоянием  $\Delta_j$  между соседними уровнями квантования коэффициента  $G_j$  при  $i \neq j$ . Это влечет за собой то, что  $y_i$  и  $y_j$  при  $i \neq j$  могут быть не одинаково распределенными случайными величинами. Но наряду с этим считается [1], что при малых значениях  $\Delta_i$  ( $i \in \{1, 2, \dots, n\}$ ) имеются основания предполагать, что  $y_i$  — случайная величина, равномерно распределенная от  $-0,5\Delta_i$  до  $0,5\Delta_i$ , т. е. плотность распределения вероятностей  $f_i(y)$  определяется равной  $1/\Delta_i$  для  $y \in \bar{\Delta}_i$  и нулю в противном случае.

Однако в стеганографических приложениях, где в качестве стеганографических контейнеров используются сжатые образы цифровых мультимедийных сигналов, вышеуказанное предположение о том, что компонента  $y_i$  шума квантования  $Y$  является случайной величиной, равномерно распределенной на  $\bar{\Delta}_i$ , не всегда является оправданным. Очень часто распределение амплитуды коэффициентов в частотной области имеет тенденцию концентрироваться вблизи величин заметно меньших, чем половина расстояния  $\Delta_i$  между соседними уровнями квантования при наиболее распространенных в практических приложениях значениях коэффициента сжатия мультимедийных сигналов. Например, при использовании для сжатия цифровых изображений алгоритма JPEG [7] это предположение оправдано только для нескольких (часто трех–четырех) элементов, стоящих в левом верхнем углу каждой матрицы коэффициентов дискретного косинусного преобразования, соответствующей яркостным и цветовым

компонентам изображения. Поэтому представляет практический интерес такой выбор элементов стеганографического контейнера для изменения при внедрении сообщения, подлежащего скрытию, который осуществляется среди указанных элементов. Но и в этом случае в целях исключения достаточно широкого спектра демаскирующих признаков необходимо учитывать возможное изменение плотности распределения вероятностей амплитуд шума квантования при внедрении в стеганографический контейнер сообщения, подлежащего скрытию. Действительно, пусть в массив квантованных коэффициентов внедрено сообщение  $m$  длины  $l$  бит, подлежащее скрытию. Сам пустой массив состоит из  $n$  квантованных коэффициентов  $g_1, g_2, \dots, g_n$ , а заполненный (с использованием стеганографического алгоритма) контейнер состоит из таких целочисленных коэффициентов  $\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_n$ , что для некоторой функции  $H_k$  от  $n$  переменных (заранее выбранной из множества функций  $\{H_k | k \in K\}$ , являющегося структурной компонентой стеганографического алгоритма с пространством ключей  $K$ )  $H_k: \underbrace{Z \times Z \times \dots \times Z}_{n \text{ раз}} \rightarrow \underbrace{\{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}}_{l \text{ раз}}$  справедливо соотношение  $H_k(\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_n) = m$ . При этом коэффициенты  $\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_n$  получают при внедрении в контейнер сообщения, подлежащего скрытию, из коэффициентов  $g_1, g_2, \dots, g_n$  путем изменения некоторых из них прибавлением или вычитанием числа 1 в сторону, противоположную тому, что было сделано стандартом сжатия при округлении после квантования. Предположим для определенности, что среди коэффициентов  $\tilde{g}_1, \tilde{g}_2, \dots, \tilde{g}_n$  ровно  $t$  получены путем изменения, а  $n - t$  не изменены и совпадают с соответствующими коэффициентами из набора  $\{g_1, g_2, \dots, g_n\}$ . Тогда, применив процедуру рандомизации [2], убеждаемся, что  $\tilde{y}_i$  ( $i \in \{1, 2, \dots, n\}$ ) —  $i$ -я амплитуда шума квантования — имеет плотность распределения вероятностей

$$\tilde{f}_i(y) = \begin{cases} \left(1 - \frac{t}{n}\right) \frac{1}{\Delta_i}, & \text{если } y \in (-0,5\Delta_i, 0,5\Delta_i], \\ \frac{t}{n\Delta_i}, & \text{если } y \in [-\Delta_i, -0,5\Delta_i] \cup (0,5\Delta_i, \Delta_i), \\ 0, & \text{в противном случае.} \end{cases}$$

## СПИСОК ЛИТЕРАТУРЫ

1. *Оппенгейм А., Шафер Р.* Цифровая обработка сигналов. М.: Техносфера, 2006, 856 с.
2. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 2. М.: Мир, 1967, 752 с.
3. ISO/IEC (1993) International Standard IS 11172-3 «Information Technology — Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to about 1.5 Mbits/s — Part 3: Audio».
4. ISO/IEC (1994) International Standard IS 13818-1 «Information Technology — Coding of Moving Pictures and Associated Audio Information. Part 1: Systems». /Ed/1, JTS 1/SC 29, 1994.
5. ISO/IEC (1994) International Standard IS 13818-2 «Information Technology — Coding of Moving Pictures and Associated Audio Information. Part 2: Video». /Ed/1, JTS 1/SC 29, 1994.
6. ISO/IEC (1994) International Standard IS 13818-2 «Information Technology — Coding of Moving Pictures and Associated Audio Information. Part 3: Audio». /Ed/1, JTS 1/SC 29, 1994.
7. JPEG digital compression and coding of continuous-tone still images. ISO 10918, 1991.