УДК 621.39

В.В. Баранник, доктор технических наук, профессор,
С.А. Сидченко, кандидат технических наук,
М.В. Думанский

МАСКИРОВОЧНОЕ КОДИРОВАНИЕ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ ПЕРЕМЕННОЙ ДЛИНЫ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Розроблено метод маскувального представлення зображень, стійких до дешифрування, на основі плаваючої схеми поліадичного кодування. Він забезпечує: виключення надмірності повідомлень одночасно без внесення погрішності до них; формування кодограм рівномірної довжини на основі змінної кількості елементів початкового зображення; зменшення кількості незначущих елементів на початку кожної бітової послідовності кодів-номерів, що додатково призводить до зниження початкового обсягу зображень від 10 %.

***Ключові слова**: дешифровано-стійке представлення, інформаційне протиборство, кодування, стиснення зображень, поліадичний код.*

Разработан метод маскировочного представления изображений, стойких к дешифрированию, на основе плавающей схемы полиадического кодирования. Он обеспечивает: исключение избыточности сообщений одновременно без внесения погрешности в них; формирование кодограмм равномерной длины на основе переменного количества элементов исходного изображения; уменьшение количества незначимых элементов в начале каждой битовой последовательности кодов-номеров, что дополнительно приводит к снижению исходного объема изображений от 10 %.

***Ключевые слова**: дешифрируемо-стойкое представление, информационное противоборство, кодирование, сжатие изображений, полиадический код.*

Method of camouflage imaging, proof to the decoding, on the basis of the floating scheme of polyadic coding is developed.

***Keywords**: decoded-proof imaging, information antagonism, coding, compression of images, polyadic code.*

Развитие мирового сообщества показало, что в наше время возникла принципиально новая ситуация, при которой информация стала важнейшим государственным ресурсом, влияющим на национальную безопасность, а технологии использования информационных ресурсов стали одним из наиболее значимых показателей уровня развития общества. Причем, построение современных информационно-телекоммуникационных систем и сетей привело к стиранию межгосударственных границ в информационном пространстве.

Стремление Украины быстрее войти в мировое информационное сообщество привело к необходимости использования готовых технологий и аппаратно-программных средства, разработанных иностранными компаниями. Это может привести к потенциальной возможности потери контроля государства над информационными процессами, которые происходят в ее информационном пространстве, и подвергает опасности собственный информационный ресурс [1–3].

Поэтому остро встают вопросы информационной безопасности государства. Одним из важных приоритетов в обеспечении информационной безопасности является создание средств защиты от несанкционированного доступа к информационным ресурсам и от нарушения нормального функционирования информационно-телекоммуникационных систем и сетей [3].

Все это послужило причиной к росту требований относительно качества, достоверности, целостности, доступности и одновременной защищенности информации, обрабатываемой и передаваемой с помощью информационно-телекоммуникационных систем и сетей, а также времени на ее обработку и доставку. Анализ динамики роста глобального IP-трафика, проведенный компанией Cisco, показал, что до 2013 года он увеличится до пяти раз относительно 2008 года. Причем порядка 92 % от всех передаваемых данных будет составлять видеотрафик.

Поэтому *актуальной научно-прикладной задачей* является сокращение времени на цифровую обработку и доставку изображений с обеспечением требуемого уровня защиты семантической информации, передаваемой на основе изображений.

Для решения этой научной задачи в работах [4–6] была предложена технология построения дешифрируемо-стойкого преобразования (ДШСП) изображений, предназначенная для скрытия семантического смысла изображения с учетом как статистических, так и структурных особенностей источника информации. Кроме того, в процессе предложенного подхода для построения ДСШП изображений происходит интеграция нескольких исходных битовых последовательностей в одну последовательность переменной длины.

Результаты частотного теста битовых последовательностей кодов-номеров (представленных в битовом виде) ДШСП с учетом незначимых элементов (незначимых нулевых бит в начале каждой битовой последовательности кодов-номеров) приведены на рис. 1 и 2. На рис. 1 приведены диаграммы зависимости вероятности появления 1 и 0 в тестируемых последовательностях ДШСП ($P(n_1)$ и $P(n_0)$ соответственно) для разной степени насыщенности изображений. На рис. 2 приведены диаграммы распределения среднего количества 1 и 0 (n_1 и n_0 соответственно) в битовом представлении кодов-номеров информационной части ДШСП для разной степени насыщенности изображений.

Из анализа диаграмм на рис. 1 и 2 видно, что количество нулевых бит в последовательностях превышает количество единичных бит. Количество нулевых бит преобладает над единичными битами в битовых последовательностях кодов-номеров средненасыщенных изображений в среднем на 72 % (рис. 3). При этом для средненасыщенных изображений количество 1 в каждой 64-битной подпоследовательности отличаться от количества 0 в среднем на 46 элементов, что превышает эталонное значение на 23 элемента.

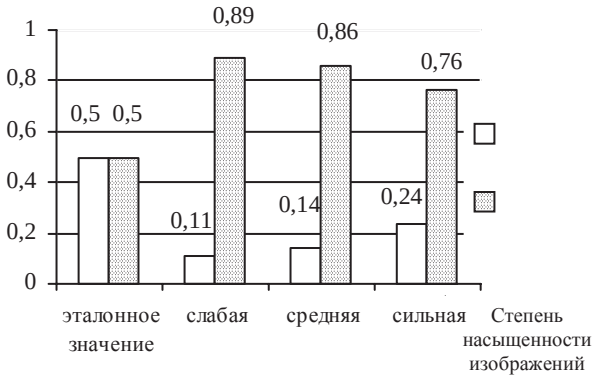

Рис. 1. Диаграмма значений величин $P(n_1)$ *и* $P(n_0)$ *для разной степени насыщенности изображений*

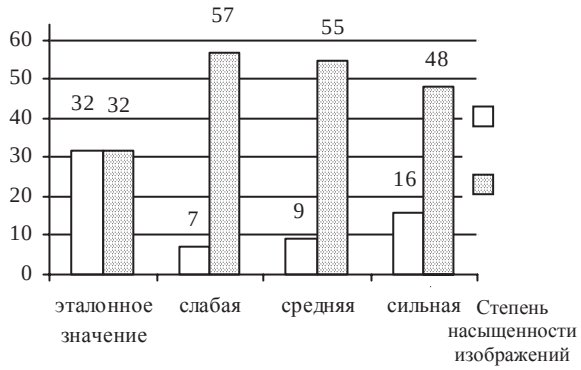

Рис. 2. Диаграмма значений величин n_1 *и* n_0 *для разной степени насыщенности изображений*

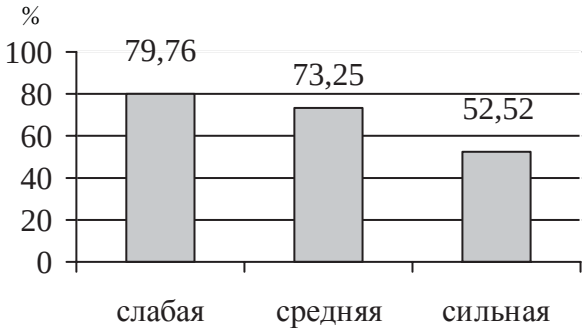

Рис. 3. Процент незначимых элементов в последовательностях кодов-номеров изображений

Можно предположить, что это связано с большим количеством незначимых нулевых элементов в битовых последовательностях информационной части ДСШП, что в свою очередь связано с малыми значениями кодов-номеров. Этот недостаток влияет, с одной стороны, на степень сжатия изображения (выходной объем ДСШП). С другой стороны, он влияет на выходные статистические характеристики дешифрируемо-стойкого представления и на уровень конфиденциальности в целом.

Поэтому для снижения количества незначимых элементов в последовательности кодов-номеров, представленных в битовом виде, предлагается формировать информационную часть последовательности на основе плавающего схемы полиадического кодирования. *Цель исследований* заключается в разработке метода маскировочного представления изображений, стойких к дешифрированию, на основе плавающей схемы полиадического кодирования, обеспечивающего снижение количества незначимых нулевых элементов в начале каждого битового представления кода-номера.

Рассмотрим особенности процесса формирования информационной части дешифрируемо-стойкого представления изображений на основе плавающей схемы кодирования. Метод основывается на последовательном образовании двумерных полиадических чисел по столбцам и по строкам. Код-номер строится путем рекуррентного добавления очередного элемента полиадического числа. Для исключения переполнения машинного слова перед каждым добавлением предлагается проводить проверку на переполнения машинного слова.

Процесс формирования кода-номера с учетом выдвинутых требований состоит из нескольких основных этапов.

Первый этап – формирование кода-номера для отдельного столбца массива видеоданных:

$$N_{1j}=a_{1j}; \qquad N_{ij}=N_{(i-1)}g_{ij}+a_{ij},$$

где N_{kj}, $N_{k-1,j}$ – j-й код-номер для i-го и i–1-го элементов; g_{ij} – динамический диапазон элемента, которым является минимальное значение из двух динамических диапазонов строки g_i и g_j столбца, на пересечении которых он расположен, т.е.

$$g_{ij}=\min(g_i;g_j);$$
$$g_i=\max_{1\le j\le n}\{a_{ij}\}+1; \qquad g_j=\max_{1\le i\le m}\{a_{ij}\}+1.$$

Величина V_{ij}, равная накопленному произведению оснований g_{ij} для элементов, определяется по формуле

$$V_{ij}=\prod_{k=1}^{i} g_{kj}.$$

Тогда при добавлении к коду-номеру $N_{(i-1)j}$ очередного элемента a_{ij} переполнения машинного слова не произойдет, если выполняется неравенство

$$V_{ij}\le 2^M-1,$$

где 2^M-1 – наибольшее число, которое может храниться в машинном слове длиной M элементов.

Поскольку выполняется неравенство $V_{ij}\ge N_{ij}$, тогда $N_{ij}\le 2^M-1$.

Процесс формирования кода-номера N_{mj}, для j-го столбца массива заканчивается тогда, когда будет обработан последний элемент:

$$N_{mj}=N_{(m-1)j}g_{jm}+a_{jm} \text{ при } V_{mj}\le 2^M-1.$$

После получения всех кодов-номеров N_{mj}, для $1\le j\le n$ столбцов, образуется вектор кодов-номеров столбцов массивов видеоданных.

Второй этап вычисления кода-номера массива видеоданных – формирование кода-номера по столбцам. По аналогии с предыдущим этапом процесс формирования $N^{(jm)}$ – кода-номера по столбцам задается следующими соотношениями:

$$N^{(1,m)}=N_{1m}; \quad N^{(j,m)}=N^{(j-1,m)}V_j^{(m)}+N_{mj},$$

где $N^{(j,m)}$, $N^{(j-1,m)}$ – коды-номера соответственно для j и (j−1) столбцов.

В этом случае $V^{(j,m)} = \prod_{\gamma=1}^{j}\prod_{k=1}^{m} g_{\gamma k} = \prod_{\gamma=1}^{j} V_{\gamma i}^{(m)}$.

Выполняется неравенство

$$V^{(j,m)} \le 2^{M} - 1.$$

Исключение переполнения разрядности машинного слова обеспечивается за счет выполнения неравенства

$$V^{(j,m)} \ge N^{(j,m)}.$$

Формирование кода-номера для массива видеоданных заканчивается тогда, когда будет получен код-номер $N^{(n,m)}$ (обработаны все строки в пределах одного столбца), равный

$$N^{(n,m)} = N^{(n-1,m)} V_n^{(m)} + N_n^{(m)},$$

$$\text{при } V^{(n,m)} = \prod_{k=1}^{n} V_k^{(m)} \le 2^{M} - 1.$$

Результаты частотного теста битовых последовательностей кодов-номеров ДШСП на основе плавающей схемы кодирования с учетом незначимых элементов приведены на рис. 4 и 5. На рис. 4 приведены диаграммы зависимости вероятности появления 1 и 0 ($P(n_1)$ и $P(n_0)$ соответственно) в тестируемых последовательностях ДШСП на основе плавающей схемы кодирования для разной степени насыщенности изображений. На рис. 5 приведены диаграммы распределения среднего количества 1 и 0 (n_1 и n_0 соответственно) в битовом представлении кодов-номеров информационной части ДШСП на основе плавающей схемы кодирования для разной степени насыщенности изображений. Из анализа диаграмм на рис. 4 и 5 видно, что количество нулевых бит в последовательностях превышает количество единичных бит и превышает эталонное значение на 8 %, что для 64-битного представления составляет порядка 5 элементов.

В результате применения данного метода количество нулевых незначимых битовых элементов в последовательности кодов-номеров будет составлять в среднем около 18 % (рис. 6), что меньше до 4-х раз относительно исходной схемы формирования информационной части ДШСП на основе простой полиадической схемы.

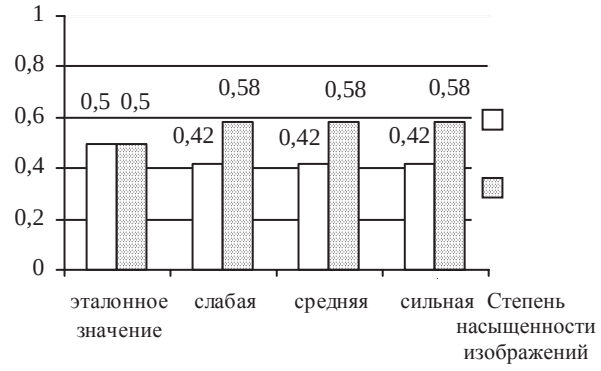

Рис. 4. Диаграмма значений величин $P(n_1)$ и $P(n_0)$ в последовательностях, сформированных на основе плавающей схемы кодирования

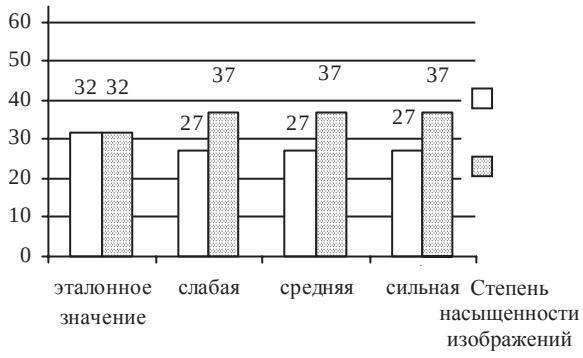

Рис. 5. Диаграмма значений величин n_1 и n_0 в последовательностях, сформированных на основе плавающей схемы кодирования

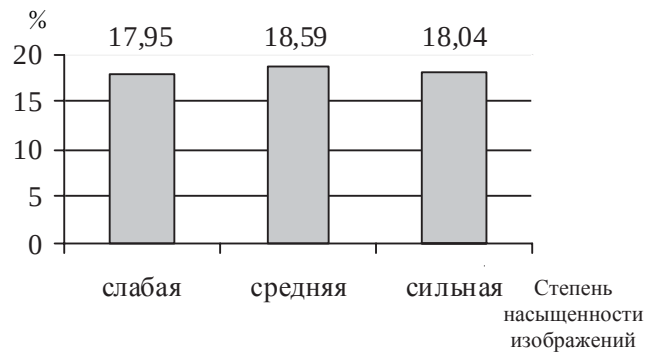

Рис. 6. Процент незначимых элементов в последовательностях, сформированных на основе плавающей схемы полиадического кодирования

Разработанный метод маскировочного представления изображений, стойких к дешифрированию, на основе плавающей схемы кодирования обеспечивает:

– исключение избыточности одновременно без внесения погрешности;

– уменьшение количества незначимых элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов-номеров до 4-х раз относительно исходной схемы формирования информационной части ДШСП;

– формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения;

– дополнительное снижение исходного объема изображений от 10 %.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Толубко В.Б.* Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) / В.Б. Толубко // Монографія. – К. : НАОУ, 2003. – 320 с.

2. *Гриняев С.Н.* Концепция ведения информационной войны в некоторых странах мира / С.Н. Гриняев // Зарубежное военное обозрение. – 2002. – № 2. – С. 11–15.

3. *Толубко В.Б.* Концептуальні основи інформаційної безпеки України / В.Б. Толубко, С.Я. Жук, В.О. Косевцов // Наука і оборона. – 2004. – № 2. – С. 19–25.

4. *Баранник В.В.* Метод криптосемантического представления изображений на основе комбинированного подхода / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2010. – № 3 (22). – С. 33–38.

5. *Баранник В.В.* Метод дешифрируемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2011. – № 1 (24). – С. 24–29.

6. *Баранник В.В.* Методика статистического тестирования дешифрируемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 13–20.

Отримано 16.03.2012