УДК 004.932

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

МЕТОД ДЕШИФРИРУЕМО-СТОЙКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ

Розроблено метод комбінованого дешифровано-стійкого представлення зображень на базі системи двовимірного поліадичного кодування. Створений метод забезпечує руйнування семантики зображень в результаті декодування кодових конструкцій дешифровано-стійкого представлення на основі помилково підібраних основ.
Ключові слова: *дешифровано-стійке представлення, компактне представлення зображень, поліадичний код.*

Разработан метод комбинированного дешифрируемо-стойкого представления изображений на базе системы двумерного полиадического кодирования. Созданный метод обеспечивает разрушение семантики изображений в результате декодирования кодовых конструкций дешифрируемо-стойкого представления на основе ошибочно подобранных оснований.
Ключевые слова: *дешифрируемо-стойкое представление, компактное представление изображений, полиадический код.*

The method of the combined decoded-firm presentation of images is developed on the base of the system of the two-dimensional poliadical encoding. The created method is provided by destruction of semantics of images as a result of decoding of code constructions of decoded-proof presentation on the basis of erroneous neat grounds.
Keywords: *decoded-proof presentation, compact presentation of images, poliadical code.*

Развитие мультимедийных приложений и их внедрение в различные сферы деятельности человека послужило причиной к росту требований относительно времени получения изображений, качеству их восстановления и обеспечению требуемого уровня конфиденциальности передаваемой информации. Поэтому *актуальной научно-прикладной задачей* является сокращение времени на цифровую обработку и доставку изображений и повышение уровня защиты семантической информации, передаваемой на основе видеоизображений.

Существующие технологии компрессионного преобразования не соответствуют требованиям относительно создания комбинированных систем дешифрируемо-стойкого представления (ДШСП). Поэтому необходимо разработать систему компрессии, обеспечивающую построение ДШСП, что и составляет *цель исследований статьи.*

Разработка базовой структуры дешифрируемо-стойкого преобразования изображений.

Одним из подходов для построения систем ДШСП на основе систем сжатия являются технологии полиадического кодирования [1–4]. В процессе кодирования

формируются кодовые комбинации, состоящие из двух частей, а именно: информационная и служебная составляющие. Информационная составляющая содержит значение кода-номера N. Формирование полиадических кодовых конструкций C(A), образующих информационную часть, осуществляется для двумерного полиадического числа $A = \{a_{ij}\}$, $i=1,m$, $j=1,n$, по интегральному принципу в два этапа. Это создает возможность для организации функции перемешивания. Наличие промежуточного звена позволяет организовать изменение структурного и статистического соответствия между исходным сообщением и кодовой комбинацией на выходе процесса сжатия.

На первом этапе вычисляется значение кода-номера N как взвешенное суммирование величин $a_{ij}V_{ij}$. Кодовая комбинация компактного представления формируется на втором этапе для значения величины N, $C(A)=\{b_0,...,b_\xi,...,b_q\}$, q – длина кодового слова, равная $q=[\lambda \log_2 N]+1$.

Служебная составляющая включает в себя информацию о системе оснований двумерного полиадического числа $G=\{g_{ij}\}$. Основанием элемента двумерного полиадического числа (ДПЧ) является минимальное значение из двух динамических диапазонов строки g_i и g_j столбца, на пересечении которых он расположен, т.е. $g_{ij}=\min(g_i; g_j)$. Отсюда можно заключить, что структура формирования кодограмм полиадической системы позволяет формировать комбинированное дешифрируемо-стойкое представление видеоданных.

Разработка метода построения информационной части дешифрируемо-стойкого представления в системах полиадического кодирования.

Информационная составляющая кодограммы полиадической системы формируется в два этапа, так что:

1. Значение кода-номера является интегрированным, и формируется с учетом служебных данных по оператору $f(A;\ G) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} \prod_{\xi=j+1}^{n} g_{i\xi} \prod_{\eta=i+1}^{m}\prod_{\xi=1}^{n} g_{\eta\xi}$.

2. Исключается прямое соответствие между исходными элементами $A=\{a_{ij}\}$ и элементами $C(A)=\{b_0,...,b_\xi,...,b_q\}$ сжатого представления, поскольку кодовое представление строится для кода-номера исходных элементов.

Рассмотрим процесс формирования битов кодограммы кода-номера с учетом особенностей полиадического кодирования. Для этого необходимо учитывать, что значение кода-номера записывается как накопленная сумма величин $a_{ij}V_{ij}$. Тогда процесс формирования кодограммы кода-номера в полиадической системе можно рассматривать как процесс наслоения (наложения) битовых зон $C_{i+j-2} = \{a_{ij} V_{ij}\}_2$ (рис.1), т.е. $C(A) - N_2 = \sum_{i=1}^{m}\sum_{j=1}^{n} C_{i+j-2}$. Здесь N_2 – двоичная запись значения кода-номера, определяющая содержание выходной кодограммы; $\{a_{11}V_{11}\}^2$ – двоичная запись величины $a_{11}V_{11}$, на базе которой формируется основная нулевая битовая зона C_0 длиной, равной q_0 бит; $\{a_{11}V_{11}\}_2$ – двоичная запись величины $a_{ij}V_{ij}$, определяющая (i+j−2)-ю битовую зону C_{i+j-2} длиной, равной q_{i+j-2} двоичных разрядов. Битовая зона C_{i+j-2} формируется на основе последовательности значимых двоичных разрядов, отводящихся для представления результата умножения значения элемента ДПЧ a_{ij} на весовой коэффициент V_{ij}:

$$C_{i+j-2}=\{a_{ij}V_{ij}\}_2. \qquad (1).$$

В процессе наслоения (наложения) битовых зон друг на друга достигается перемешивание двоичных разрядов. Перемешивание может осуществляться на двух уровнях, а именно:

– на уровне восприятия отдельных пикселей. Значения пикселей изображений рассматриваются как десятичные числа. Соответственно значение кода-номера на логическом уровне также будет десятичным числом;

– на уровне кодового представления. Данный уровень является уровнем физического представления значения кода-номера в информационно-вычислительной системе. Оценка эффективности перемешивания на данном уровне определяется специальными тестами, используемыми в криптографических системах. В этом случае полная информация в доступном виде будет содержаться в двоичном числе, поскольку запись числа в двоичном виде и есть его кодовое представление на физическом уровне.

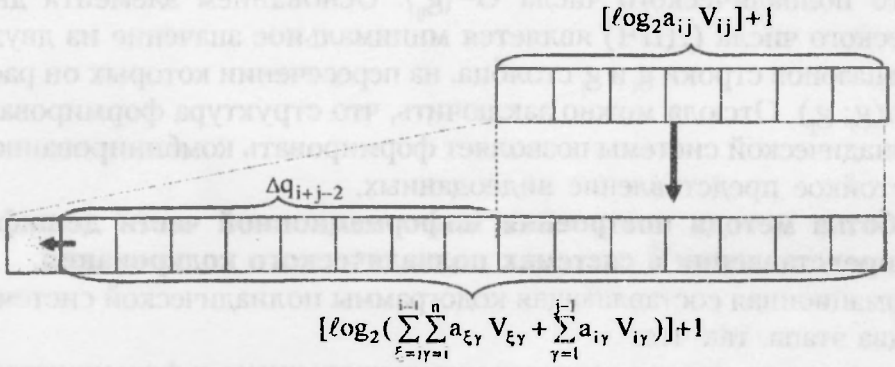

Рис. 1. Схема формирования многослойного наложения зон

Перемешивание на логическом уровне происходит в результате того, что основания элементов ДПЧ будут неравными друг другу $g_{ij} \neq g_{\eta\tau}$, $i \neq \eta$; $j \neq \tau$; $i,\eta = \overline{1,m}$, $j,\tau = \overline{1,n}$, и не кратными десятичным значениям. Отношения весовых коэффициентов между парами элементов ДПЧ также будут неравными друг другу $V_{i,j-1}/V_{ij} = g_{i,i} \neq V_{\eta,\tau-1}/V_{\eta\tau} = g_{\eta\tau}$, где V_{ij-1}, V_{ij} – весовые коэффициенты соответственно для $(i;j-1)$-го и $(i;j)$-го элементов ДПЧ; $V_{\eta\,\tau-1}$, $V_{\eta\tau}$, – весовые коэффициенты соответственно для $(\eta,\tau-1)$-го и (η,τ)-го элементов ДПЧ. Образовывается неравновесное вложение каждого элемента в суммарное значение кода-номера, т. е. $a_{ij}V_{ij} \neq a_{\xi j}V_{\xi j}$, $i \neq \xi$, и $i,\xi = \overline{1,m}$. Обеспечивается перемешивание разрядов кода-номера относительно значений исходных элементов ДПЧ, сформированных на базе исходных фрагментов изображения.

Перемешивание на физическом уровне достигается в результате сложения содержаний кодового представления текущей кодограммы и добавляемой битовой зоны (рис. 1): $\sum_{\xi=1}^{i-1}\sum_{\gamma=1}^{n}\{a_{\xi\gamma}V_{\xi\gamma}\}_2 + \sum_{\gamma=1}^{j-1}\{a_{i\gamma}V_{i\gamma}\}_2 + \{a_{ij}V_{ij}\}_2$, где $\sum_{\xi=1}^{i-1}\sum_{\gamma=1}^{n}\{a_{\xi\gamma}V_{\xi\gamma}\}_2 + \sum_{\gamma=1}^{j-1}\{a_{i\gamma}V_{i\gamma}\}_2$ – битовое содержание текущего значения кодограммы после добавления $(i+j-3)$-й битовой зоны; $\{a_{ij}V_{ij}\}^2$ – $i+j-2$)-я добавляемая битовая зона.

В результате таких наложений формируется многослойная структура кодограммы кода-номера двумерного полиадического числа (рис. 1).

Условием перемешивания на физическом уровне является наличие единичных элементов в младших разрядах битовых зон. Количество θ нулевых младших разрядов должно быть меньшим, чем длина добавляемой битовой зоны, т. е.

$$\theta_{i+j-3} < q_{i+j-2} \qquad (2),$$

где θ_{i+j-3} – количество младших разрядов, содержащих нулевые значения после добавления (i+j−3)-й битовой зоны.

Условие (2) будет выполняться, если при наложении (i;j)-й битовой зоны значения содержания кодограммы не будет кратным величине 2^{qi+j-2}, что гарантирует отсутствие в младших разрядах нулевой цепочки длиной, равной q_{i+j-2}бит. В свою очередь выполнение данного условия обеспечивается в результате неравновесного перемешивания на логическом уровне представления, как кода-номера, так и битовых зон для двумерной полиадической системы, т.е.

$$(\sum_{\xi=1}^{i-1}\sum_{\gamma=1}^{n} a_{\xi\gamma} V_{\xi\gamma} + \sum_{\gamma=1}^{j-1} a_{i\gamma} V_{i\gamma}) \bmod(q_{i+j-2}) \neq 0,$$

где $(\sum_{\xi=1}^{i-1}\sum_{\gamma=1}^{n} a_{\xi\gamma}V_{\xi\gamma} + \sum_{\gamma=1}^{j-1} a_{i\gamma}V_{i\gamma})$ – значение кода-номера после добавления (i,j−1)-го элемента ДПЧ;

в) между значением весового коэффициента текущего элемента ДПЧ V_{ij} и накопленной суммой для младших элементов ДПЧ выполняется неравенство:

$$V_{ij} > \sum_{\xi=j+1}^{n} a_{i\xi} V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi} V_{\eta\xi} \qquad (3),$$

где V_{ij} – весовой коэффициент (i;j)-го элемента ДПЧ; $(\sum_{\xi=j+1}^{n} a_{i\xi}V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi}V_{\eta\xi})$ – накопленная сумма для младших элементов ДПЧ относительно (i;j)-го элемента.

Отсюда вытекает, что если $a_{11}\neq 0$, то согласно (3) выполняется неравенство $a_{11}V_{11} \geq (\sum_{\xi=21}^{n} a_{1\xi}V_{1\xi} + \sum_{\eta=2}^{m}\sum_{\xi=1}^{n} a_{\eta\xi}V_{\eta\xi}) + 1$. Откуда значение величины $a_{11}V_{11}$ будет:

– как минимум в a_{11} раз больше, чем величина $(\sum_{\xi=21}^{n} a_{1\xi} V_{1\xi} + \sum_{\eta=2}^{m}\sum_{\xi=1}^{n} a_{\eta\xi} V_{\eta\xi})$;

– не более чем в 2 раза меньше по сравнению со значением кода-номера N, т.е. в результате добавления остальных слагаемых величина кода-номера относительно значения $a_{11}V_{11}$ увеличится не более, чем в 2 раза.

На логическом уровне, если не учитывать их совокупный семантический характер, то содержание каждой накладываемой битовой зоны будет иметь равнозначный вес при реконструкции отдельных элементов изображения. Однако каждая битовая зона будет еще содержать информацию о семантике фрагмента изображения. И количество такой семантической информации для разных кодограмм и битовых зон будет различной. С этой позиции каждая зона будет вносить различный семантический смысл.

С учетом обоснованных свойств процесса перемешивания в результате наслоения битовых зон возможны следующие механизмы рассеивания двоичных последовательностей:

1) добавочный сдвиг в сторону старших разрядов относительно младших разрядов текущего содержания кодограммы, количество которых равно длине добавляемой битовой зоны;

2) смещение накладываемой битовой зоны относительно соответствующей по длине последовательности младших разрядов кодограммы. Проявляется эффект блуждающих зон, получаемый в результате сдвига добавляемой зоны относительно своего начального уровня наложения.

Смещение может быть двух видов, а именно:

– сжатое смещение; происходит тогда, когда есть перенос в старшие разряды, но количество единиц в смежных разрядах текущего содержания кодограммы меньше чем длины накладываемой битовой зоны, $\vartheta_{i+j-3} < q_{i+j-2}$ и $\Delta q_1 < q_{i+j-2}$, где ϑ_{i+j-3} – количество младших разрядов, содержащих единичные значения после добавления (i+j–3)-й битовой зоны; Δq_1 – длина зоны сдвига в результате наложения второй битовой зоны.

– наоборот когда количество единичных разрядов в смежной зоне будет больше длины наслаиваемой битовой зоны, то происходит ее смещение в виде растяжения, $\vartheta_{i+j-3} > q_{i+j-2}$ и $\Delta q_1 > q_{i+j-2}$.

Под смежной областью понимается область, содержащая двоичные разряды, примыкающие к граничной области относительно добавляемой битовой зоны;

3) добавление старшего разряда кодограммы относительно начальной (нулевой) битовой зоны.

Поскольку элементы ДПЧ имеют неравновесные характеристики, то в общем случае области смещения битовых зон будут неравномерными. Понятно, что наибольшая скорость рассеивания двоичных последовательностей достигается в случае наличия смещения битовых зон с растяжением.

1. Разработан метод комбинированного ДШСП на базе системы двумерного полиадического кодирования, базирующийся на:

– формировании служебных данных, адаптивно учитывающих содержание обрабатываемого фрагмента изображения путем выявления характеристик динамических диапазонов их элементов;

– формировании в два этапа информационной составляющей кодограммы в результате неравновесной криптосемантической свертки исходного фрагмента изображения и оснований элементов ДПЧ, которые оказывают значимое влияние на: формирование значения кода-номера ДПЧ; на процесс образования кодовой конструкции полиадической системы, и используются в виде ключевой информации. Это реализует сжатие по ключу.

– криптографическом шифровании вектора оснований элементов ДПЧ. Это реализует сжатие с последействием.

2. Созданный метод обеспечивает:

1) реализацию механизмов перемешивания и рассеивания. Достигается скрытие статистических свойств открытого в смысловом плане фрагмента изображения.

2) разрушение семантики изображений в результате декодирования кодовых конструкций дешифрируемо-стойкого представления на основе ошибочно подобранных оснований.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Баранник В.В.* Структурно-комбинаторное представление данных в АСУ: Монография / В.В. Баранник, Ю.В. Стасев, Н.А. Королева. – Х. : ХУПС, 2009. – 252 с.

2. *Баранник В.В.* Методология создания криптографических преобразований на базе методов исключающих избыточность / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2009. – № 4. – С. 5–17.

3. *Barannik V.* Methodology of Creation of Cryptographic Transformations on the Basis of Methods Excluding Redundancy / V. Barannik, S. Sidchenko, V. Larin // International Conference TCSET'2009 [IModern problems of radio engineering, telecommunications and computer scienceI] (Lviv-Slavsko, Ukraine, February 23 – 27, 2010) / Lviv Polytechnic National University, 2010. – P. 312.

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.

Отримано 10.03.2011