УДК 621.327

С.А. Сидченко

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ОБОСНОВАНИЕ ЕДИНСТВЕННОСТИ СИСТЕМЫ ОСНОВАНИЙ ДЕШИФРИРУЕМО-СТОЙКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ

Обоснована возможность организации дешифрируемо-стойкого представления изображений на этапе их кодового представления на основе двумерной полиадической системы. Доказано, что ошибка хотя бы в одном основании полиадической системы приведет к неправильному восстановлению как минимум одного элемента двумерного полиадического числа. Исходное двумерное полиадическое число без ошибок можно восстановить по заданному коду-номеру только для соответствующей системы оснований.

Ключевые слова: *дешифрируемо-стойкое представление, двумерное полиадическое число, полиадический код.*

Введение

Постановка проблемы и анализ литературы. В современных условиях организация представления информации с заданной степенью дешифрируемой стойкости относительно несанкционированного доступа определяется эффективностью ее обработки на разных уровнях информационно-телекоммуникационной системы [1; 2]. **Актуальной научно-прикладной тематикой исследований** является построением систем представления мультимедийной и компьютерной информации с заданным уровнем дешифрируемой стойкости [3; 4].

Существующие технологии компрессирования базируются на использовании энтропийных кодовых конструкций, которые строятся на основе префиксного принципа для отдельных элементов исходного сообщения. В этом случае формируемая служебная информация, а именно пакеты вероятностных характеристик, допускают наличие бесконечного множества допустимых комбинаций, обеспечивающих взаимооднозначное декодирование [2]. Поэтому служебная информация энтропийных кодовых конструкций не может использоваться в качестве ключевой для организации дешифрируемо-стойких систем. Это приводит к необходимости обоснования и создания принципиально новых подходов относительно кодового представления мультимедийной информации в ИТС. Одним из таких подходов является организация кодирования информации на основе интегрированных кодовых конструкций. Отсюда **цель исследований** заключается в обосновании дешифрируемой стойкости двумерных полиадических конструкций в случае формирования ключевой информации на основе системы оснований.

Изложение основного материала

Построение комбинированного дешифрируемо-стойкого представления (ДШСП) изображений обеспечивается в случае формирования ключевой информации на основе вектора служебной составляющей [3; 4]. Для полиадической системы служеб-

ные данные образуются на базе динамических диапазонов элементов двумерного полиадического числа (ДПЧ). Система служебных данных ДПЧ обладает следующим свойствами:

а) оказывает значимое влияние на процесс формирования кодограммы информационной части;

б) существенно характеризует содержание конкретного обрабатываемого локального фрагмента изображения. Динамический диапазон является конкретной характеристикой обрабатываемого фрагмента изображений, и зависит от его семантического содержания (следовательно, влияет на его смысловое содержание). Он определяет яркостную составляющую, а в некоторых случаях характеризует позицию и величину контурного перепада. Действительно, если фрагмент изображения информативный, т.е. содержит на основном фоне контур или мелкие объекты, то это приведет к наличию элементов изображений, имеющих различные диапазон. Отсюда динамический диапазон в строках, столбцах и основаниях ДПЧ будут неравномерными.

Однако использование системы оснований G ДПЧ как базовой информации для построения ключа в технологии комбинированного ДШСП требует наличие следующих свойств, а именно:

1) единственности и взаимооднозначности декодирования для варианта безошибочного восстановления всех компонент служебных данных. Это означает необходимость выполнения условий:

$$f^{(-1)}(N;G') = \begin{cases} A, \to G' = G; \\ A', \to G' \neq G, \end{cases} \qquad (1)$$

где $f^{(-1)}(N;G')$ – обратный оператор получения ДПЧ $A = \{a_{ij}\}$ по значению кода-номера N и системе оснований G'; G' – система оснований ДПЧ.

Под условием $G' = G$ понимается случай, когда основания всех элементов ДПЧ восстановлены без ошибок. Наоборот если $G' \neq G$, то найдется хотя бы одно основание G', для которого выполняется условие $g'_{ij} \neq g_{ij}$. Аналогичным образом под A' понимается ДПЧ, содержащее хотя бы один элемент, для которого выполняется условие $a'_{ij} \neq a_{ij}$.

Условие (1) указывает на наличие свойства гарантированного искажения как минимум одного элемента исходного изображения в случае неверного восстановления хотя бы одного основания элемента ДПЧ;

2) появление ошибки ε_{ij} в процессе восстановления элемента a_{ij} ДПЧ, основание g_{ij} которого декодировано неверно, т.е.

если $g'_{ij} \neq g_{ij}$, то $a'_{ij} = a_{ij} \pm \varepsilon_{ij}$, где $|\varepsilon_{ij}| \neq 0$,

где g'_{ij}, g_{ij} – значения оснований для восстановленного и исходного $(i;j)$-го элемента ДПЧ. Понятно, что для $|\varepsilon_{ij}| \neq 0$ выполняется неравенство $a'_{ij} \neq a_{ij}$;

3) наличие лавинно-связывающего эффекта, состоящего в появлении ошибок в последовательности восстанавливаемых элементов изображения в результате неверно восстановленного основания одного элемента ДПЧ, т.е.

если $g'_{ij} \neq g_{ij}$, то $|\varepsilon_{\eta\xi}| \neq 0$, где $\eta, \xi \in \Omega$, $|\Omega| = \theta \geq 2$,

где Ω – множество позиций элементов ДПЧ, для которых выполняется условие $a'_{\eta\xi} \neq a_{\eta\xi}$.

Другими словами ошибка в процессе восстановления одного основания должна привести к возникновению ошибок в нескольких элементах фрагмента изображения. Понятно, что ошибки при восстановлении оснований возникают вследствие несанкционированного доступа.

Рассмотрим **теорему о единственности системы оснований**. Если значение первого элемента ДПЧ не равно нулю, т.е. $a_{11} \neq 0$, то:

1) для фрагмента изображения $A = \{a_{ij}\}$ и системы оснований $G = \{g_{ij}\}$ можно сформировать единственное значение кода-номера N;

2) по значению кода-номера N, восстановление исходного ДПЧ $A = \{a_{ij}\}$ без ошибок возможно только для одной системы оснований $G = \{g_{ij}\}$.

Доказательство. Начнем с первой части теоремы. Допустим, что найдется хотя бы два равных по значению кода-номера N и N', которые получаются для двух систем оснований G и G', отличающихся значением как минимум одной компоненты $g'_{ij} \neq g_{ij}$. От величины основания $(i;j)$-го элемента зависят значения весовых коэффициентов предыдущих элементов ДПЧ. Тогда на основе выражения

$$N = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}V_{ij}$$

получим

$$N = \sum_{\eta=1}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi}V_{\eta\xi} + \sum_{\xi=1}^{j-1} a_{i\xi}V_{i\xi} + a_{ij}V_{ij} + \sum_{\xi=j+1}^{n} a_{i\xi}V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi}V_{\eta\xi};$$

$$N' = \sum_{\eta=1}^{i-1}\sum_{\xi=1}^{n} a_{\eta\xi}V'_{\eta\xi} + \sum_{\xi=1}^{j-1} a_{i\xi}V'_{i\xi} + a_{ij}V_{ij} + \sum_{\xi=j+1}^{n} a_{i\xi}V_{i\xi} + \sum_{\eta=i+1}^{m}\sum_{\xi=1}^{n} a_{\eta\xi}V_{\eta\xi}.$$

Без потери общности допустим, что $g_{ij} > g'_{ij}$. Тогда, поскольку по предположению выполняется равенство $N = N'$, то вычитая из первого выражения второе, получим следующее соотношение

$$a_{11}(V_{11} - V'_{11}) = \sum_{\xi=2}^{n} a_{1\xi}(V_{1\xi} - V'_{1\xi}) +$$

$$+\sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n}a_{\eta\xi}(V_{\eta\xi}-V'_{\eta\xi})+\sum_{\xi=1}^{j-1}a_{i\xi}(V_{i\xi}-V'_{i\xi}).$$

Отобранные элементы соответствуют старшим элементам ДПЧ, то разделив каждое слагаемое данного равенства на величину весового коэффициента V_{ij} младшего элемента, получим

$$a_{11}\prod_{\gamma=2}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})=$$

$$=\sum_{\xi=2}^{n}a_{1\xi}\prod_{\gamma=\xi+1}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})+$$

$$+\sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n}a_{\eta\xi}\prod_{\gamma=\xi+1}^{n}g_{\eta\gamma}\prod_{\ell=\eta+1}^{i-1}\prod_{\gamma=1}^{n}g_{\ell\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})+$$

$$+\sum_{\xi=1}^{j-1}a_{i\xi}\prod_{\gamma=\xi+1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij}). \qquad (2)$$

В связи с тем, что величина $(g_{ii}-g'_{ij})$ является константой для всех слагаемых выражения (2), то его можно рассматривать как запись соотношения для определения кода-номера ДПЧ, количество элементов которого равно $n(i-1)+(j-1)$. Младшим элементом будет элемент исходного ДПЧ, имеющего координаты $(i;j-1)$. В тоже время на основе свойств полиадической системы между весовым коэффициентом первого элемента и правой частью выражения (2) должно выполняться неравенство

$$\prod_{\gamma=2}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})>$$

$$>\sum_{\xi=2}^{n}a_{1\xi}\prod_{\gamma=\xi+1}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})+$$

$$+\sum_{\eta=2}^{i-1}\sum_{\xi=1}^{n}a_{\eta\xi}\prod_{\gamma=\xi+1}^{n}g_{\eta\gamma}\prod_{\ell=\eta+1}^{i-1}\prod_{\gamma=1}^{n}g_{\ell\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})+$$

$$+\sum_{\xi=1}^{j-1}a_{i\xi}\prod_{\gamma=\xi+1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij}). \qquad (3)$$

С другой стороны согласно принятому предположению $g_{ij}>g'_{ij}$. Отсюда выполняется неравенство

$$a_{11}\prod_{\gamma=2}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}(g_{ii}-g'_{ij})\geq$$

$$\geq\prod_{\gamma=2}^{n}g_{1\gamma}\prod_{\eta=2}^{i-1}\prod_{\gamma=1}^{n}g_{\eta\gamma}\prod_{\gamma=1}^{j-1}g_{i\gamma}.$$

Однако данное неравенство противоречит условию (3). Откуда получаем, что принятое предположение относительно $g'_{ij}\neq g_{ij}$ неверно. Значит, для заданных элементов ДПЧ и фиксированной системы оснований в случае, когда $a_{ij}\neq 0$ можно получить только одно значение кода-номера. Первая часть теоремы доказана.

Докажем вторую часть теоремы. Покажем единственность обратного преобразования, т.е. если $a_{ij}\neq 0$, то по заданному значению кода-номера N, восстановление исходного ДПЧ $A=\{a_{ij}\}$ без ошибок возможно только для одной системы оснований $G=\{g_{ij}\}$. В противном случае, если найдется хотя бы одно основание, для которого $g'_{ij}\neq g_{ij}$, то при фиксированном N будет получено ДПЧ $A'=\{a'_{ij}\}$, так что как минимум для одного элемента будет выполняться неравенство $a'_{ij}\neq a_{ij}$.

Доказательство будем проводить от противного. Допустим, что для $g'_{ij}\neq g_{ij}$ будет получено ДПЧ без искажений, т.е. для всех восстановленных элементов выполняется равенство $a'_{ij}=a_{ij}$, $i=\overline{1,m}$ и $j=\overline{1,n}$, т.е. найдется как минимум две системы оснований, отличающиеся минимум одной компонентой, так, что по заданному значению кода-номера будет без ошибок получено исходное ДПЧ. Тогда в соответствии с выражением (1) для одного и того же ДПЧ на основе двух различных систем оснований $G=\{g_{ij}\}$ и $G'=\{g'_{ij}\}$ можно сформировать как минимум два одинаковых по значению кода-номера. Но это утверждение противоречит утверждению, доказанному в первой части теоремы.

Следовательно, для условия когда $a_{11}\neq 0$, по заданному коду-номеру и имеющейся системе оснований можно восстановить, только одно ДПЧ. Ошибка хотя бы в одном основании полиадической системы приведет к неправильному восстановлению как минимум одного элемента ДПЧ. Исходное ДПЧ без ошибок можно восстановить по заданному коду-номеру только для соответствующей системы оснований. Теорема доказана полностью.

На основе доказанной теоремы вытекает следующее следствие.

Следствие. В случае если первый элемент ДПЧ равен нулю, т.е. $a_{11}=0$, то выводы теоремы не выполняются. В этом случае различные системы оснований, отличающиеся основанием первого элемента, т.е. $g'_{11}\neq g_{11}$ будут приводить к получению одинаковых кодов-номеров.

Доказательство следствия вытекает на базе того, что основание первого элемента не участвует в получении значения кода-номера. Поэтому нулевое значение первого элемента приводит к возможности выбора произвольного целочисленного основания, величина которого не будет оказывать влияние на код-номер.

В тоже время надо отметить, что данный случай не влияет на снижение уровня дешифрируемой стойкости изображений. Это обусловлено тем, что:

– нулевое значение соответствует черному цвету, т.е. с точки зрения яркостных характеристик не несет информацию о смысловой нагрузке обрабатываемого фрагмента изображения;

– на идентификацию остальных элементов ДПЧ такое условие не оказывает влияния, т.е. значение кода-номера для остальных элементов без учета первого будет уже единственным;

– вероятность появления нулевого элемента в начале полиадического числа маловероятна.

Отсюда видно, что для безошибочного дешифрирования исходных данных требуется информация о значении кода-номера N и системе оснований ДПЧ $G = \{g_{ij}\}$. Полиадическое кодирование обладает свойством взаимооднозначности, т.е. для последовательности элементов $A = \{a_{ij}\}$ при $a_{ij} \neq 0$ и заданной системы оснований $G = \{g_{ij}\}$ можно сформировать только один код-номер N и наоборот. Поэтому в случае применения криптопреобразования для последовательности оснований ДПЧ восстановление исходных элементов невозможно.

Выводы

Обосновано возможность организации ДСШП изображений на этапе ее кодового представления на основе ДПЧ. Разработанный подход базируется на:

1) формировании системы служебных данных на базе динамических диапазонов элементов ДПЧ, что обеспечивает:

– создание условия для значимого влияния служебных данных на процесс формирования кодограммы информационной части;

– то, что служебные данные характеризуют содержание конкретного обрабатываемого локального фрагмента изображения. Данное свойство основано на том, что динамический диапазон является конкретной характеристикой обрабатываемого фрагмента изображений, и зависит от его семантического содержания (следовательно, влияет на его смысловое содержание). Динамический диапазон определяет как яркостную составляющую, которая имеет наибольшее значение с позиции восприятия изображения зрением человека, а в некоторых случаях характеризует позицию и величину контурного перепада, содержащегося в обрабатываемом фрагменте изображения;

2) обосновании взаимной однозначности полиадического представления, а именно:

– для заданного фрагмента изображения и системы оснований можно сформировать единственное значение кода-номера;

– по заданному значению кода-номера, восстановление исходного ДПЧ без ошибок возможно только для одной системы оснований.

Следовательно, для условия когда $a_{11} \neq 0$, по заданному коду-номеру и имеющейся системе оснований можно восстановить, только одно ДПЧ. Другими словами ошибка хотя бы в одном основании полиадической системы приведет к неправильному восстановлению как минимум одного элемента ДПЧ. Исходное ДПЧ без ошибок можно восстановить по заданному коду-номеру только для соответствующей системы оснований.

Список литературы

1. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1073 с.

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

3. 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.

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.

Поступила в редакцию 5.01.2011

Рецензент: д-р тех. наук, проф. В.В. Баранник, Харьковский университет Воздушных Сил имени И. Кожедуба, Харьков.

ОБҐРУНТУВАННЯ ЄДНОСТІ СИСТЕМИ ОСНОВ ДЕШИФРОВАНО-СТІЙКОГО ПРЕДСТАВЛЕННЯ ЗОБРАЖЕНЬ

С.О. Сідченко

Обґрунтовано можливість організації дешифровано-стійкого представлення зображень на етапі їх кодового представлення на основі двовимірної поліадичної системи. Доведено, що помилка хоча б в однієї основі поліадичної системи приведе до неправильного відновлення як мінімум одного елемента двовимірного поліадичного числа. Вихідне двовимірне поліадичне число без помилок можна відновити по заданому коду-номеру тільки для відповідної системи основ.

Ключові слова: *дешифровано-стійке представлення, двовимірне поліадичне число, поліадичний код.*

GROUND OF UNICITY OF SYSTEM OF BASIS OF DECODED-PROOF PRESENTATION OF IMAGES

S.A. Sidchenko

Possibility of organization of decoded-proof presentation of images is grounded on the stage of their code presentation on the basis of the two-dimensional poliadical system. It is well-proven that an error even in one foundation of the poliadical system will result in wrong renewal at least of one element of two-dimensional poliadical number. Initial two-dimensional poliadical number without errors it is possible to recover on the set code-number only for the proper system of basis.

Keywords: *decoded-proof presentation, two-dimensional poliadical number, poliadical code.*