УДК 621.327:681.5

МЕТОД КРИПТОСЕМАНТИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПЛАВАЮЩЕЙ СХЕМЫ В БАЗИСЕ ПО ВЕРХНИМ ГРАНИЦАМ

БАРАННИК В.В., ТУПИЦА И.М., СИДЧЕНКО С.А.

В целях создания комбинированных систем для скрытия видеоинформационного ресурса на основе технологий устранения избыточности с сохранением целостности и оперативности доставки информации разрабатывается метод криптосемантического представления изображений на основе плавающей схемы системы полиадического кодирования в базисе по верхним границам. Данный метод обеспечивает: одновременное выполнение процессов сжатия и шифрования (кодирования) видеоданных; исключение избыточности одновременно без внесения погрешности; уменьшение количества незначимых элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов-номеров; формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения; дополнительное снижение исходного объема изображений.

Ключевые слова: криптосемантическое представление изображений; защита информации; шифрование; кодирование; компрессия изображения; полиадический код.

1. Введение

Развитие мультимедийных приложений и их внедрение в различные сферы деятельности человека послужило причиной роста требований относительно времени доставки видеоданных, качества их восстановления и обеспечения требуемого уровня конфиденциальности передаваемой информации.

Поэтому актуальной научно-прикладной задачей является сокращение времени на цифровую обработку и доставку видеоданных при обеспечении заданного уровня конфиденциальности семантической информации, передаваемой на основе изображений.

Для повышения эффективности обеспечения безопасности видеоинформации, доводимой в реальном времени, возможны два направления, а именно:

1. Провести модификацию существующих технологий компрессии и криптографических преобразований с позиции их последовательного использования.

2. Разработать принципиально новый подход, который заключается в создании технологий, одновременно обеспечивающих повышение оперативности доведения и защиту видеоинформации на основе методов семантической и синтаксической обработки изображений.

В пользу выбора второго направления указывают следующие преимущества:

– обеспечивается сокращение объемов видеоданных, передаваемых с использованием инфокоммуникационных систем;

– разработка процессов сжатия и шифрования рассматривается как единый этап обработки, что исключает необходимость в организации их совместимости и согласованности;

– исключается возможность несанкционированного доступа к видеоинформации после этапа компрессии;

– существует возможность учитывать для обеспечения информационной скрытности особенности семантического содержания изображений и психовизуального восприятия их зрительной системой. В том числе возможно учитывать и тот факт, что шифрование осуществляется одинаково для всех частей фрагмента изображения, т.е. затрачивается одинаковое количество операций для всех блоков изображения, в то время как разные блоки несут различное количество семантической нагрузки, т.е. разные блоки изображения имеют различную важность и ценность информации. Учет такой семантической неоднородности блоков изображения позволяет сократить вычислительные затраты. Это можно сделать с помощью методов кодирования источников изображений;

– сокращается время обработки за счет слияния двух этапов в один.

Для решения поставленной научно-прикладной задачи в работах [1–4] была предложена технология криптосемантического представления изображений, предназначенная для скрытия семантического смысла изображения с учетом как статистических, так и структурных особенностей источника информации. В [5,6] предложен метод криптосемантического представления изображений на основе статической схемы полиадичского кодирования в двумерном базисе. В работе [7] предложена методика тестирования для оценки статистических характеристик криптосемантического представления изображений и на их основе проведено тестирование последовательностей кодовномеров для статической схемы полиадического кодирования.

Одним из недостатков разработанного метода криптосемантического представления изображений на основе статической схемы полиадического кодирования является построение кода-номера криптосемантического представления изображения на основе одинакового количества исходных элементов фрагмента видеоданных [5,6]. На выходе криптосемантического представления получаются кодограммы разной длины в битовом представлении (меньше длины, выделя-

емой для хранения кодового слова), что приводит к появлению большого количества незначимых нулевых элементов в выходных битовых последовательностях [8]. Этот недостаток влияет, с одной стороны, на степень сжатия изображения (выходной объем криптосемантического представления), а с другой – на выходные статистические характеристики криптосемантического представления и на уровень конфиденциальности в целом.

Поэтому для формирования кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения предлагается формировать информационную часть криптосемантического представления на основе плавающей схемы полиадического кодирования. Для этого в работах [8,9] предложена плавающая схема криптосемантического представления в двумерном базисе по верхним границам. Недостатком данного подхода является то, что сначала формируются промежуточные коды-номера по отдельным столбцам, а уже потом формируется интегрированный код-номер, что в свою очередь может так же привести к появлению кодов-номеров с длиной, меньшей, чем длина выделяемого кодового слова. Это связано с тем, что формирование интегрированного кода-номера происходит на основе больших промежуточных данных. Кроме того, для формирования кода-номера в двумерном базисе необходимо хранить (передавать) двойной комплект оснований (служебных данных), что может привести к увеличению общего выходного объема криптосемантического представления изображения.

Цель исследований заключается в разработке метода кодирования изображений на основе плавающей схемы полиадического кодирования в базисе по верхним границам, обеспечивающего формирование кодограмм равномерной длины на основе переменного (заранее неопределенного) количества элементов исходного изображения.

2. Основная часть

Исходное изображение разбивается на фрагменты размерностью $m \times n$ точек, где m – количество строк фрагмента изображения, а n – количество столбцов. Фрагмент изображения рассматривается как двумерная матрица $A = \{a_{i,j}\}$, $i = \overline{1,m}$, $j = \overline{1,n}$, которую можно преобразовать в одномерный вектор:

$$A = \{a_{i,j}\} = \{a_{\tau}\}_{\tau=\overline{1,mn}} = \{a_{m(j-1)+i}\}, i = \overline{1,m},\ j = \overline{1,n}. \quad (1)$$

На предварительном этапе определяется система оснований $G^{(m)} = \{g_i\}$, $i = \overline{1,m}$, исходного фрагмента изображения по строкам. Основание элементов i-й строки g_i определяется как максимальный элемент строки исходного массива, увеличенный на 1:

$$g_i = \max_{1 \le j \le n}(a_{i,j}) + 1 = \max_{1 \le j \le n}(a_{m(j-1)+i}) + 1. \quad (2)$$

В дальнейшем система оснований будет выступать в роли ключевого элемента (служебных данных) для формирования информационной части криптосемантического представления изображения и должна храниться в секрете или дополнительно шифроваться с использованием одного из стандартов блочного шифрования данных.

Для удобства проведения расчетов и для определения взаимно-однозначного соответствия элементов фрагмента изображения с основаниями предлагается расширить систему оснований до мощности исходного фрагмента изображения в одномерном векторном виде. Для этого воспользуемся формулой:

$$S^{(m \times n)} = \{s_{\tau}\} = \{g_{\tau - m\left[\frac{\tau-1}{m}\right]}\},\ \tau = \overline{1,mn}. \quad (3)$$

Процесс представления данных в полиадической системе в базисе по верхним границам на основе плавающей схемы задается следующими выражениями:

$$N = \sum_{\tau=1}^{Q} a_{\tau} V_{\tau}; \quad (4)$$

$$V_{\tau} = \begin{cases} \prod_{\xi=\tau+1}^{Q} s_{\xi} = \prod_{\xi=\tau+1}^{Q} g_{\xi - m\left[\frac{\xi-1}{m}\right]}, & \tau < Q; \\ 1, & \tau = Q, \end{cases} \quad (5)$$

$$Q \le mn, \quad (6)$$

где Q – плавающее количество элементов, принимающих участие в формировании кода-номера в базисе по верхним границам на основе плавающей схемы с учетом проверки на переполнение кодового слова; $[\bullet]$ – целая часть.

Для контроля переполнения кодового слова при формировании кода-номера N введем дополнительную величину T_Q, равную накопленному произведению оснований для Q элементов, принимающих участие в формировании кода-номера, которая определяется по формуле:

$$T_Q = \prod_{\xi=1}^{Q} s_{\xi} = \prod_{\xi=1}^{Q} g_{\xi - m\left[\frac{\xi-1}{m}\right]}. \quad (7)$$

Переполнения кодового слова не произойдет, если выполняется неравенство:

$$T_Q \le 2^M - 1, \quad (8)$$

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

Действительно, поскольку выполняется неравенство $T_Q \ge N$, тогда: $N \le 2^M - 1$.

Максимальное количество элементов Q_{lim}, принимающих участие в формировании кода-номера, опреде-

ляется как значение аргумента, при котором величина T_Q достигает максимума при условии выполнения неравенства (8) и рассчитывается по формуле:

$$Q_{\lim} = \underset{Q}{\operatorname{argmax}}(T_Q) = \underset{Q}{\operatorname{argmax}}\left(\prod_{\xi=1}^{Q} s_\xi\right). \quad (9)$$

С учетом соотношения (9) выражения (4) и (5) для определения кода-номера примут вид

$$N = \sum_{\tau=1}^{Q_{\lim}} a_\tau V_\tau ; \quad (10)$$

$$V_\tau = \begin{cases} \prod_{\xi=\tau+1}^{Q_{\lim}} s_\xi = \prod_{\xi=\tau+1}^{Q_{\lim}} g_{\xi-m\left[\frac{\xi-1}{m}\right]}, & \tau < Q_{\lim} < mn; \\ 1, & \tau = Q_{\lim} \le mn. \end{cases} \quad (11)$$

Формирование кода-номера возможно и на основе рекуррентной схемы путем добавления очередного элемента фрагмента изображения. Процесс формирования кода-номера задается следующими выражениями:

$$N_1 = a_1 ; \quad (12)$$

$$N_\tau = N_{\tau-1} s_\tau + a_\tau = N_{\tau-1} g_{\tau-m\left[\frac{\tau-1}{m}\right]} + a_\tau , \quad (13)$$

где N_τ, $N_{\tau-1}$ – код-номер для τ-го и $(\tau-1)$-го элементов.

Для исключения переполнения кодового слова перед каждым добавлением к коду-номеру $N_{\tau-1}$ очередного элемента a_τ проводится проверка на переполнение кодового слова, которая с учетом соотношения $\tau = Q$ определяется с помощью дополнительной величины T_τ на основе выражения (7) с учетом выполнения неравенства (8).

Действительно, поскольку выполняется неравенство $T_\tau \ge N_\tau$, тогда $N_\tau \le 2^M - 1$.

Процесс формирования кода-номера N заканчивается тогда, когда будет обработан последний Q-й элемент:

$$N = N_Q = N_{Q-1} s_Q + a_Q = N_{Q-1} g_{Q-m\left[\frac{Q-1}{m}\right]} + a_Q \quad (14)$$

при $T_Q \le 2^M - 1$ и $Q \le mn$.

В данном случае Q-й элемент будет равен максимальному количеству элементов $Q_{\lim}$ фрагмента изображения, принимающих участие в формировании кода-номера, рассчитанному по формуле (9).

3. Выводы

Разработанный метод криптосемантического представления изображений на основе плавающей схемы полиадического кодирования в базисе по верхним границам обеспечивает:

– одновременное выполнение процессов сжатия и шифрования (кодирования) видеоданных;

– исключение избыточности одновременно без внесения погрешности;

– уменьшение количества незначимых элементов (незначимых нулевых бит) в начале каждой битовой последовательности кодов-номеров;

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

– дополнительное снижение исходного объема изображений.

Литература: 1. *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. **2.** *Бараннік В.В.* Методологічні основи криптосемантичного представлення відеозображень в інформаційних комунікаціях / В.В. Бараннік, С.О. Сідченко, В.В. Ларін // Наукоємні технології. К., 2012. № 3(15). С. 78-82. **3.** *Баранник В.В.* Методологическая база криптокомпрессионного представления видеоинформационных ресурсов / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Захист інформації. Квітень–червень 2013. Том 15, № 2. С. 97–104. **4.** *Barannik V.V.* The methodological base of cryptocompression presentation of videoinformation resources / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XII International Conference CADSM'2013 [IEEE The Experience of Designing and Application of CAD Systems in Microelectronics] (Lviv, Ukraine, February 19–23, 2013). Lviv Polytechnic National University, 2013. P. 27–28. **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.** *Barannik V.V.* The Decoded-proof Presentation of Images on the Basis of the Polyadycal Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23 – 25, 2011. P. 182. **7.** *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. **8.** *Сидченко С.А.* Способ представления изображений, стойких к дешифрированию на основе плавающей схемы кодирования / С.А. Сидченко // Системи озброєння і військова техніка. 2011. Вип. 3 (27). С. 68–70. **9.** *Barannik V.V.* Methodology Constructions of Floating Chart of Decoded-proof Presentation of Images / V. V. Barannik, S. A. Sidchenko // International Conference TCSET'2012 [Modern problems of radio engineering, telecommunications and computer science] (Lviv-Slavsko, Ukraine, February 21–24, 2012). Lviv Polytechnic National University, 2012. P. 437.

Транслитерированный список литературы: 1. *Barannik V.V.* Metod kriptosemanticheskogo predstavlenija izobrazhenij na osnove kombinirovannogo podhoda / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Suchasna special'na tehnika. 2010. №3 (22). S. 33 – 38. **2.** *Barannik V.V.* Metodologichni osnovy kryptosemantychnogo predstavlennya videozobrazhen` v informacijnyx komunikaciyax / V.V. Barannik, S.O. Sidchenko, V.V. Larin / / Naukoyemni texnologiyi. K., 2012. # 3(15). S. 78-82. **3.** *Barannik V.V.* Metodologicheskaja baza kriptokompressionnogo predstavlenija videoinformacionnyh resursov / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Zaxy`st informaciyi. Kviten`–cherven` 2013. Tom 15, # 2. S. 97–104. **4.** *Barannik V.V.* The methodological base of cryptocompression presentation of videoinformation resources / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XII International Conference CADSM'2013 [IEEE The Experience of Designing and Application of CAD Systems in Microelectronics] (Lviv, Ukraine, February 19–23, 2013). Lviv Polytechnic National University, 2013. P. 27–28. **5.** *Barannik V.V.* Metod deshifriruemo-stojkogo predstavlenija izobrazhenij / V.V. Barannik, S.A. Sidchenko, V.V. Larin // Suchasna special`na texnika. 2011. #1 (24). S. 24 – 29. **6.** *Barannik V.V.* The Decoded-proof Presentation of Images on the Basis of the Polyadycal Encoding Systems / V. V. Barannik, S. A. Sidchenko, V. V. Larin // XIth International Conference CADSM 2011, The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, Ukraine, Lviv Polytechnic National University, February 23 – 25, 2011. P. 182. **7.** *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. **8.** *Sidchenko S.A.* Sposob predstavlenija izobrazhenij stojkih k deshifrirovaniju na osnove plavajushhej shemy kodirovanija / S.A. Sidchenko // Systemy ozbroyennya i vijs`kova texnika. 2011. Вип. 3 (27). С. 68–70. **9.** *Barannik V.V.* Methodology Constructions of Floating Chart of Decoded-proof Presentation of Images / V. V. Barannik, S. A. Sidchenko // International Conference TCSET'2012 [Modern problems of radio engineering, telecommunications and computer science] (Lviv-Slavsko, Ukraine, February 21–24, 2012). Lviv Polytechnic National University, 2012. P. 437.

Поступила в редколлегию 17.10.2015

Рецензент: д-р техн. наук, проф. Безрук В.М.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 050-303-89-71.

Тупица Иван Михайлович, заместитель начальника учебно-тренировочного комплекса Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 096-795-57-39.

Сидченко Сергей Александрович, канд.техн. наук, старший научный сотрудник научного центра Харьковского университета Воздушных Сил им. И. Кожедуба. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79, тел. 066-299-82-73.

Barannik Vladimir Victorovich, doctor of sciences by technical, professor, chief of department of the Kharkov university of Air Force.

Tupitsya Ivan Mikhailovich, Dep.chief of educational-training centre of the Kharkov university of Air Force.

Sidchenko Sergey Aleksandrovich, philosophy doctor by technical, senior research worker, senior research worker of scientific center of the Kharkov university of Air Force.