UDC 004.056.5

METHOD OF IMAGE RECONSTRUCTION BASED ON TWO-LEVEL DECODING OF LINEAR TRANSFORMS

Vladimir Barannik, Sergey Turenko

This paper deals with the main stages of developing the method of image segment reconstruction on the basis of decoding of truncated double tuple vectors. It has been proved that the method must include the following distinctive stages: installation of code design; decoding of code values of the component of double tuple truncated vectors; reconstruction of double tuples based on decoding the biadic numbers. Installation process, which includes the following actions, is created: selection of an auxiliary part; decomposition of an information part of code design, namely determination of: number of code words; last codegram of non-uniform length; withdrawal of code words.

Key words: *image reconstruction, codegram installations, tuple vector decoding.*

Introduction. The modern development of information communications suggests a need of developing video and information services as a key component [1; 2]. Therefore, actual scientific applied researches are researches in encoding space of information sources and digital image processing methods. One of the priority directions herein consists in creation of image processing strong technologies for reduction of their volumes [3; 4].

For this purpose, it is required to develop the approaches, which are based on coding of transformed images with detection of double tuple vectors. One of effective approaches is the technology of double tuple vector coding on the basis of the enlarged positional coding [5; 6]. However, a key point of these technologies is the creation of reconstruction method, ensuring acquisition of decompressed image data with the specified time and qualitative characteristics. Therefore, the objective of research of this paper is to develop a method of image reconstruction based on two-level decoding of linear transforms.

Results and discussion. Basic requirements that are specified at the stage of developing a method of reconstruction of the compressed images are as follows:

– to avoid uncontrolled loss of information;

– to ensure restoration of images with the appropriate visual perception quality by using only that information which is generated in the compression process;

– to organize the reconstruction of images, using for this the number of transactions not exceeding the number of operations required for compression.

In this case, the features of the process of frame sequence compression must be considered. The main features are as follows:

1) formation of an unknown in advance number of combined codegrams, namely the first type is one with a predetermined limited length, and the second type is unknown in advance irregular lengths;

2) code representation of a truncated double tuple vector is formed as a code of an aggregated positional number by two-level scheme;

3) code value is formed for the variable length of a component of aggregated positional number;

4) double tuples are encoded as two-element biadic numbers;

5) the linear transform has the composition form on the basis of double tuple vector containing length of a zero component chain and a significant component;

6) processing of transform components is carried out with reference to correction of their values to the features of image visual perception.

The first stage of the recovery process is the installation of code construction. To avoid uncontrolled loss of information the following is required:

– to identify, first, service and information parts of the code structure of current compressed image segment in the entire video stream;

– to determine, then, variable number Ψ of codegrams formed for code representation of truncated double tuple vectors, and length $V(\tilde{P}')_{\Psi}$ of the non-uniform codegram.

The first stage of the installation of code construction is provided by separating the service part. The following arrangement features of code words of the service part are considered:

– code representation of value matrix is formed as for a binary sequence of the predetermined length. This enables to know in advance about the length of the code word for compressed representation of value matrix;

– the number of bits to represent the score of the quality loss factor is a constant value, taking into account the limited number of modes in which the quantization process is set;

– code word length for the DC-component is determined on the basis of static tables, known at both the transmitting and receiving side.

This properties of the service part determine the start position of information part of the code structure of a compressed image segment representation.

Further, the second phase of the code structure installation is implemented.

The information part of image code construction represents a codegram for the truncated double tuple vector. This codegram includes both the service and information part. The service part of codegram is formed by the following code fields:

1) code field containing the information on number $n_{крт}$ of double tuples;

2) code field containing the information on the base $\lambda(\ell)$ of first tuple component;

3) code field containing the information on the base $\lambda(c)$ of second tuple component.

For the known image segment size n, the lengths of the code fields are known at the receiving side using no additional information. For example, if $n=8$, then the lengths of the code fields of the service part are selected due to the following principles:

– the maximum number of tuples for the truncated vector will be $n_{крт} \le 62$. Therefore, the length of the code field is chosen to be 6 bits;

– the maximum length of zero component chain shall not exceed $\ell_{\max} \le 63$. Therefore, the length of the relevant code field is to be 6 bits;

– the maximum value of the significant component except for DC-component shall be placed into a 8-bit sequence. A code field, respectively, for representation of the base is to be 8 bits.

It allows setting the initial position of the codegram information part containing information about the code representation of truncated DC vector.

Decomposition of the codegram information part contains a variable number of code words $G(P')_{\psi}$, carrying information about the code value $E(A)_{\nu_{\psi}}$ of a component of aggregated positional number. Therefore, a key step of the decomposition is to define as follows:

1) number Ψ of code words;

2) non-uniform length $V(P')_{\Psi}$ for Ψ codegram.

This information is determined using the following one on:

– the base $\lambda(\ell)$ and $\lambda(c)$, respectively, for the lengths of zero component chains and significant component of the linear transform (transmitted as part of the code structure);

– the maximum specified length $V_{\max}$ of the codegram (this information is known at both the transmitting and receiving sides).

Knowing this information and using technology and non-uniform distribution of tuple number over the codegrams, the corresponding sequence is found: Ψ; $\{\nu_1;...;\nu_{\psi};...\nu_{\Psi}\}$.

Hence, the length $V(P')_{\Psi}$ for Ψ non-uniform codegram is determined, namely:

$$V(P')_{\Psi} = [\ell og_2 W^{(\nu_{\Psi})}]+1 = [\ell og_2(\lambda(\ell)\cdot\lambda(c))^{\nu_{\Psi}}]+1.$$

Further, the code words $G(P')_{\psi}$ are withdrawn and the relevant code values $E(A)_{\nu_{\psi}}$ are decoding. We must consider that the decoding process is carried out by a two-level scheme, and the elements of the aggregated positional number are code values $E(\Theta_{\alpha}^{(2)})$ of two-element biadic numbers formed for the corresponding tuples $\Theta_{\alpha}^{(2)}$.

Let's consider the upper decoding level of the aggregated positional numbers. It is necessary to perform the following stages (using a code $E(A)_{\nu_{\psi}}$ processing as an example):

1. Calculation of weighting coefficient $W(A^{(\alpha)})$ for IF amplifier element α, using a formula

$$W(A^{(\alpha)}) = (\lambda(\ell)\lambda(c))^{\nu_{\psi}-\alpha},$$

where ν_{ψ} – is a number of tuples, involved in the code $E(A)_{\nu_{\psi}}$ formation.

2. Recovery of code $E(\Theta_{\alpha}^{(2)})$ value for the biadic number, constructed for the tuple $\Theta_{\alpha}^{(2)}$. For this purpose, the following relation shall be done:

$$E(\Theta_{\alpha}^{(2)}) = [E(A)_{\nu_{\psi}} / W(A^{(\alpha)})] -$$
$$[E(A)_{\nu_{\psi}} / \lambda(\ell)\lambda(c) W(A^{(\alpha)})]\lambda(\ell)\lambda(c).$$

3. Decoding process at the upper level ends after restoring the last element $E(\Theta_{\nu_{\psi}}^{(2)})$ of the IF amplifier. As a result, we obtain an aggregated positional number

$$A = \{E(\Theta_2^{(2)}); ...; E(\Theta_{\alpha}^{(2)}); ...; E(\Theta_{n_{крт}-1}^{(2)})\}.$$

Elements $E(\Theta_{\alpha}^{(2)})$ of an aggregated positional number are codes of the relevant two-element biadic numbers.

Therefore, the reconstruction of double tuples $\Theta_{\alpha}^{(2)} = \{\ell_{\alpha}; c_{\alpha}\}$ requires decoding the corresponding codes of biadic numbers. This is implemented at the lower level of the general process of decoding the IF

amplifier codes. The following stages shall be performed:

1. Determination of the component $[E(\Theta_\alpha^{(2)})/\lambda(c)]$.

2. The use of component $[E(\Theta_\alpha^{(2)})/\lambda(c)]$ determines the value $[E(\Theta_\alpha^{(2)})/\lambda(\ell)\cdot\lambda(c)]\lambda(\ell)$.

3. Further, the first tuple component ℓ_α is restored through obtaining a high-order element of biadic number with bases equal to $\lambda(\ell)$ and $\lambda(c)$, namely

$$\ell_\alpha = [E(\Theta_\alpha^{(2)})/\lambda(c)] - [E(\Theta_\alpha^{(2)})/\lambda(\ell)\cdot\lambda(c)]\lambda(\ell).$$

4. Recovery of the second tuple component c_α (significant LT component) is implemented through obtaining a low-order element of biadic number. Therefore, based on the known value $[E(\Theta_\alpha^{(2)})/\lambda(c)]$, we obtain

$$c_\alpha = E(\Theta_\alpha^{(2)}) - [E(\Theta_\alpha^{(2)})/\lambda(c)]\lambda(c).$$

All other tuple components are restored in the same way. Recovery results in truncated double tuple vector P'.

The next stage of reconstructing an image segment is the recovery of a full DC vector. For this purpose, we shall obtain the following:

1) information on the length $\ell_{n_{крт}}$ of the last zero component chain;

2) information on the low-frequency transform component c_1.

Due to formation of the linear transform, the length of the last zero component chain is determined based on the known chain lengths for truncated DC vector, i.e.

$$\ell_{n_{крт}} = n^2 - 1 - \sum_{\alpha=2}^{n_{крт}-1} \ell_\alpha,$$

where $\sum_{\alpha=2}^{n_{крт}-1} \ell_\alpha$ – the total number of LT components for which truncated DC vector is formed.

Let's consider reconstruction of DC-component. Here, we use the information about that a low-frequency component codegram consists of two parts, namely the master binary code $[e(c'_{1,r})]_2$ and a complement code $[\mu(c'_{1,r})]_2$, i.e. $[c'_{1,r}]_2 = \{[e(c'_{1,r})]_2; [\mu(c'_{1,r})]_2\}$.

Therefore, the decoding process of DC-component lies in the determination of the master and complement binary code words. Further, we obtain a differential representation of the current low-frequency component by using static code tables. After receiving the information about the value c_1, the formation process of double tuple vector P is completed, i.e.

$$P = \{c_1; (\ell_2; c_2), \dots, (\ell_\alpha; c_\alpha), \dots, (\ell_{n_{крт}-1}; c_{n_{крт}-1}); \ell_{n_{крт}}\}.$$

Block of the subsequent stages of the recovery process of an image segment lies in re-transforming and reproducing the segments for the original representation color model.

The material presented suggests that the method of image segment reconstruction on the basis of decoding of truncated double tuple vectors has been developed. The method includes the following distinctive stages: installation of code structure of compressed image segment representation; decoding of code values of the component of double tuple truncated vectors; reconstruction of double tuples based on decoding the biadic numbers.

Conclusions. The method of image segment reconstruction on the basis of decoding of truncated double tuple vectors has been developed. It includes the following distinctive stages:

1) implementation of code structure installation. To avoid uncontrolled loss of information the following is required: to identify, first, service and information parts of the code structure of current compressed image segment representation in the entire video stream; to determine, then, variable number of codegrams formed for code representation of truncated double tuple vectors, and length of the non-uniform codegram. Installation includes the following actions: selection of an auxiliary part; decomposition of an information part of code design, namely determination of: number of code words; last codegram of non-uniform length; withdrawal of code words.

2) decoding of code values of the components of a truncated double tuple vector. The decoding process is carried out by a two-level scheme, and the elements of the aggregated positional number are code values of two-element biadic numbers formed for the corresponding tuples;

3) reconstruction of double tuples based on decoding of biadic numbers.

REFERENCES

[1]. Olifer V.G., Olifer N.A. (2006) Computer Networks. Principles, Technologies, Protocols: College textbook, St.P.: Piter, 958 p.

[2]. Gonzales R.C., Woods R.E. (2002) Digital image processing, Prentice Inc. Upper Saddle River, New Jersey, 779 p.

[3]. Barannik V., Polyakov V. (2010) Encoding of transformed images within information and communication systems, Kh.: KAFU, 212 p.

[4]. Barannik V., Stasev Yu., Turenko S. (2013) Justification of problematic deficiencies of the technology of component coding of transformed images for telecommunication facilities, *Modern special equipment*, №4, pp. 17-26.
[5]. Barannik V., Turenko S. (2013) Combinatorial model of double tuple vector for the assessment of informative value of truncated linear transform, *ACS and automatic control equipment*, No.163, pp. 17-26.
[6]. Barannik V., Turenko S. (2013) Method of verification of tuple vector codec in the keyframe compression system in the information communications, *ACS and automatic control equipment*, No.165, pp. 22-30.

ЛИТЕРАТУРА

[1]. Olifer V.G., Olifer N.A. (2006) Computer Networks. Principles, Technologies, Protocols: College textbook, St.P.: Piter, 958 p.
[2]. Gonzales R.C., Woods R.E. (2002) Digital image processing, Prentice Inc. Upper Saddle River, New Jersey, 779 p.
[3]. Баранник В. В., Поляков В. П. Кодирование трансформированных изображений в инфокоммуникационных системах: монография – Х. : ХУПС, 2010. – 212 с.
[4]. Баранник В. В. Обоснование проблемных недостатков технологии компонентного кодирования трансформированных изображений для средств телекоммуникаций / В. В Баранник, Ю. В. Стасев, С. В. Туренко // Сучасна спеціальна техніка – ДНДІ, К., 2013. – 4. – С. 17-26.
[5]. Баранник В. В. Комбинаторная модель вектора двухкомпонентных кортежей для оценки информативности усеченной линиаризированной трансформанты / В.В. Баранник, С.В. Туренко // АСУ и приборы автоматики. – ХНУРЕ, Харьков, 2013. – № 163. – С. 17-26.
[6]. Barannik V., Turenko S. (2013) Method of verification of tuple vector codec in the keyframe compression system in the information communications, *ACS and automatic control equipment*, No.165, pp. 22-30.

МЕТОД РЕКОНСТРУКЦІЇ ЗОБРАЖЕННЯ НА ОСНОВІ ДВОРІВНЕВОГО ДЕКОДУВАННЯ ЛІНІЙНИХ ПЕРЕТВОРЕНЬ

Розвиток інфокомунікацій висуває необхідність вдосконалення ринку відеоінформаційних послуг. У зв'язку з чим актуальними науково-прикладними дослідженнями є вишукування в області кодування джерел інформації та методів цифрової обробки зображень. Тут пріоритетний напрямок полягає у створенні потужних технологій обробки зображень для зменшення їх обсягів. Одним з ефективних підходів є технологія кодування векторів двокомпонентних кортежів на основі збільшеного позиційного кодування. Тому основний матеріал досліджень статті присвячується розробці методу реконструкції зображень на основі дворівневого декодування лінеаризованих трансформант. У розділах статті викладаються основні етапи розробки методу реконструкції сегментів зображення на основі декодування усічених векторів двокомпонентних кортежів. Обгрунтовано, що метод повинен включати в себе наступні відмітні етапи: інсталяцію кодової конструкції; декодування кодових значень складових усіченого вектора двокомпонентних кортежів; реконструкцію двокомпонентних кортежів на основі декодування біадичних чисел. Створюється процес інсталяції , що включає в себе наступні дії: виділення службової частини; декомпозиція інформаційної частини кодової конструкції, а саме: визначення кількості кодових слів; останньої кодограми нерівномірної довжини; вилучення кодових слів.

Ключові слова. Відеоінформаційні послуги, реконструкція зображень, технології компресії, інсталяції кодограм, декодування векторів кортежів, кодування без втрати інформації.

МЕТОД РЕКОНСТРУКЦИИ ИЗОБРАЖЕНИЯ НА ОСНОВЕ ДВУХУРОВНЕВОГО ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ

Развитие инфокоммуникаций выдвигает необходимость совершенствования рынка видеоинформационных услуг. В связи с чем, актуальными научно-прикладными исследованиями являются изыскания в области кодирования источников информации и методов цифровой обработки изображений. Здесь приоритетное направление заключается в создании мощных технологий обработки изображений для уменьшения их объемов. Одним из эффективных подходов является технология кодирования векторов двухкомпонентных кортежей на основе укрупненного позиционного кодирования. Поэтому основной материал исследований статьи посвящается разработке метода реконструкции изображений на основе двухуровневого декодирования линеаризированных трансформант. В разделах статьи излагаются основные этапы разработки метода реконструкции сегментов изображения на основе декодирования усеченных векторов двухкомпонентных кортежей. Обосновано, что метод должен включать в себя следующие отличительные этапы: инсталляцию кодовой конструкции; декодирование кодовых значений составляющих усеченного вектора двухкомпонентных кортежей; реконструкцию двухкомпонентных кортежей на основе декодирования биадических чисел. Создается процесс инсталляции, включающий в себя следующие действия: выделение служебной части; декомпозиция информационной части кодовой конструкции, а именно определение: количества кодовых слов; последней кодограммы неравномерной длины; изъятие кодовых слов.

Ключевые слова. Видеоинформационные услуги, реконструкция изображений, технологии компрессии, инсталляции кодограмм, декодирование векторов кортежей, кодирование без потери информации.

Баранник Владимир Викторович, доктор технических наук, профессор, начальник кафедры Харьковского университета Воздушных Сил.
E-mail: barannik_v_v@mail.ru.
Баранник Володимир Вікторович, доктор технічних наук, професор, начальник кафедри Харківського університету Повітряних Сил.
Barannik Vladimir, Dr. of Technical Science, Chief of Department, professor at Kozhedub Air Force university, Kharkiv.
Туренко Сергій Вікторович, аспірант Харківського національного університету радіоелектроніки**.**
E-mail: barannik_v_v@mail.ru.
Туренко Сергей Викторович, аспирант Харьковского национального университета радиоэлектроники.
Turenko Sergey Viktorovich, postgraduate student of Kharkiv national university of radioelectronics.

УДК 004.056.55

АРИФМЕТИКА С ОТЛОЖЕННЫМ ПЕРЕНОСОМ ДЛЯ ЦЕЛЫХ ЧИСЕЛ

Андрей Охрименко

Криптографические преобразования с открытым ключом широко используются и положены в основу направленного шифрования, выработки общего секрета и электронной цифровой подписи. Поэтому, задача повышения производительности криптографических преобразований с открытым ключом является актуальной. Повысить производительность можно за счет увеличения производительности операций над целыми числами. Предлагается DCF представление целых чисел, в котором число разбивается на машинные слова, где в каждом машинном слове отводится блок под представление самого числа и блок под последующие переносы в старшие разряды, либо займы из старших разрядов. Приводятся алгоритмы основных арифметических операций с отложенным переносом, даются рекомендации по эффективной программной реализации арифметических операций (сложение, вычитание).
Ключевые слова: *DCF представление, отложенный перенос, целые числа, целочисленная арифметика, программная реализация, распараллеливание.*

Введение. Информационно-телекоммуникационные системы основательно вошли в жизнь современного общества, переведя его в новую эпоху информационного общества. Тем не менее, само общество задается вопросом о конфиденциальности персональных данных, личной информации, и т.д. Подобное волнение связано с информацией опубликованной рядом информационных агентств по материалам предоставленных Эдвардом Сноуденом. Для обеспечения защиты информации, которая циркулирует, создается, модифицируется, хранится и уничтожается, создаются системы защиты информации, ядром которых являются методы криптографической защиты информации. Криптографические преобразования с открытым ключом занимают особое место среди криптографических алгоритмов и положены в основу направленного шифрования, выработки общего секрета и электронной цифровой подписи. Актуальность задачи повышения производительности криптографических преобразований с открытым ключом, подтверждает тот факт, что преобразования с открытым ключом существенно уступают в производительности симметричным преобразованиям.

Сейчас получили широкую популярность криптографические преобразования, основанные на сложности решения следующих математических задач [4]:

– Факторизация большого числа.

– Дискретный логарифм в поле целых чисел и в поле полиномов.

– Дискретный логарифм в группе точек эллиптической кривой над полем целых чисел и в поле полиномов.

– Дискретный логарифм в якобиане дивизоров гиперэллиптической кривой над полем целых чисел и в поле полиномов.

– Поиска кратчайшего вектора в Эвклидовом пространстве, и т.д.

Алгоритмы решения данных задач имеют субэкспоненциальную сложность, поэтому при определенных размерах ключей, их решение считается невозможным на современном этапе развития вычислительной техники.

Следует заметить, что среди перечисленных задач, большинство используют операции над целыми числами. Поэтому, предлагается повысить производительность криптографических