UDK 629.391

METHODOLOGY COMPRESSION OF VIDEOINFORMATION IN THE CRYPTOGRAPHIC SYSTEMS

V. V. Barannik, Dr. Sci. (Eng.), Prof; ***S. A. Sidchenko***, Phd, ***V. V. Larin***

National Aviation University

kszi@ukr.net

У статті показано, що для збільшення ефективності обробки з використанням інфокомунікаційних систем реального часу потрібно в процесі доставки відеоданих одночасно проводити криптографічне шифрування з організацією компактного представлення.

Ключеві слова: захист інформації, криптосемантичні перетворення.

Substantiation of is spent that for increase of efficiency of processing and delivery of the video data with using information communication systems of real time is required to carry out cryptographic enciphering simultaneously with the organization of compact representation.

Keywords: defence information, cryptosemantic transformations.

Raising of problem and analysis of literature

In modern conditions information became a unique strategic resource which characterizes state potential along with its material and other resources. At the same time vulnerability of the information that has led to necessity give is more attention to its protection has raised. Expenses for working out of protection frames of the information to modern measures make about 60 % of all expenses connected with working out to the automated control systems.

Basic material

The all stream of the information circulates in an information field, the video information shares increases. Existing systems of transfer do not allow transferring great volume of the video data operatively. One of the basic ways of decrease in volumes of the transferred video data is their compact representation. Therefore processes of processing and data transmission nowadays are information the communication systems include stages of a compression, enciphering and noiseproof coding. In the course of formation of the compact description of the data increase information capacity transferred designs and reduction of initial volume is reached. It allows:

– to get rid of redundancy which is peculiar to any clear text and consequently, to lower quantity of data which can be used at the cryptographic analysis;

– to lower time of enciphering at the expense of reduction of length of processed messages.

Technologies of a compression of the video data in most cases include the methods of coding providing reduction of redundancy. In the course of such coding code combinations of two types are formed, namely: information and office components. Taking into account what the structurally functional scheme of process of processing of the information, can accept one of variants considered on fig. 1.

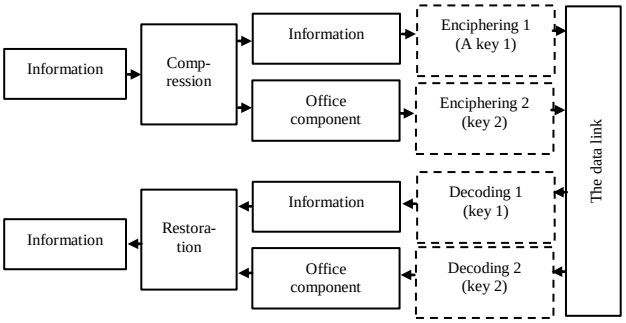

Fig. 1 The scheme of the combined system of compression and enciphering of video data

In case of processing and data transmission in systems of real time compression and enciphering is carried out for the initial data in process of their receipt on processing. Accordingly total time T of delivery of the data is under the formula

$$T = T_{cd} + T_{ecd} + T_{tce},$$

where T_{cd} — the time of compression of the data; T_{ecd} — the time for enciphering of the compressed data; T_{tce} — the time for data transmission after their compression and enciphering.

Depending on a variant of enciphering of the compressed data (fig. 1) enciphering time T_{ecd} will be calculated accordingly under formulas: for enciphering of an office component $T_{ecd} = T_{eoc}$; for enciphering of an information component $T_{ecd} = T_{eic}$; for enciphering of information and office components $T_{ecd} = T_{eic} + T_{eoc}$.

From the analysis of schemes on fig. 1 follows that for the modified processing compression and enciphering processes can be combined on time. It is similarly possible to carry out parallel or conveyor

processing of processes of enciphering and formation of information making code combinations.

In case of absence of a stage of compression of the data on enciphering the volume of the initial data equal arrives W_{id}. After enciphering the volume of the initial does not change, mean $W_{id} = W_{ed}$, where W_{ed} – the volume of the encoded initial data. Therefore transfer time T_{td} — the coded the initial data is estimated under the formula $T_{td} = W_{id} / S_t$, where S_t — the speed of data transmission on information communication to systems. Accordingly time T_{ed} of enciphering of the initial data is as $T_{ed} = W_{id} / S_e$, where S_e — the speed of enciphering of data. In case of use of compression of the data on enciphering the volume of compactly presented data equal arrives W_{cd}. Then taking into account that after enciphering the volume of the data does not vary time of enciphering and transfer of the ciphered compressed data is defined under formulas:

$$T_{ecd} = W_{ced} / S_e = \begin{cases} T_{ecd} = W_{oc} / S_e \to W_{ced} = W_{oc}; \\ T_{eic} = W_{ic} / S_e \to W_{ced} = W_{ic}; \\ T_{eic} + T_{ecd} = W_{cd} / S_e \to W_{ced} = W_{cd}, \end{cases}$$

$T_{ecd} = W_{cd} / S_t$, where W_{ced} — the volume of a component of the compressed representation arriving on enciphering; W_{oc} — the volume of an office component of the compressed representation; W_{ic} – the volume of an information component of the compressed representation.

As a result of redundancy reduction in initial messages and expenses of a time resource T_{cd} for compression of the data the inequality is carried out $W_{cd} \le W_{id}$.

It is clear that the prize on total time of delivery at the expense of use of a compression stage will be when the inequality is carried out:

$$T_{ed} + T_{td} \ge T_{cd} + T_{ecd} + T_{tce}.$$

Lack of the considered approach of data processing is the systems of enciphering do not consider potential possibilities of compression technologies that concerning destruction of semantic structure of the image.

From a position of cryptographic transformations it means additional concealment of messages with use of a source of the information.

It will allow:

– to raise cryptographic firmness of existing systems of enciphering in case of time expenses for processing of the equal $T \le T_{ed} + T_{td}$;

– to lower time expenses for process of enciphering of the compressed data at performance of requirements concerning set cryptographic firmness, mean $T'_{ecd} \le T_{ecd}$, where T'_{ecd} — time of enciphering of the compressed data taking into account features of compression systems concerning change of semantic structure images.

For an possibility estimation of the account of features of compression technologies in enciphering systems it is necessary to consider the basic types of cryptographic transformations over the data.

According to K. Shannon [1], in practical code numbers it is necessary to use two general principles: dispersion and hashing. Dispersion represents distribution of influence of one sign on a clear text on set of signs on the transformed text that allows hiding statistical properties of a clear text. Hashing assumes use of such ciphering transformations which complicate restoration of interrelation statistical properties of the open and coded texts.

For an estimation of firmness of definition ciphering systems methods of cryptographic statistical safety of algorithms are used. The given methods are based on coherence calculation (correlation of blocks) cryptograms among themselves and with entrance blocks of clear texts, and also definition of cryptograms redundancy.

From these positions processes of redundancy reduction provide following transformations: recorrelation both between separate elements, and between adjacent fragments of images; elimination of sequences are identical elements video given (series of the video data); formation of code combinations in which distribution of occurrence elements probabilities aspires to the uniform law.

Modern cryptographic transformations are based on a principle of Kirchhoff which says that privacy of transformation is provided with privacy of a key, instead of cryptographic transformation privacy. Therefore compromise a key conducts to transformation disclosing.

At designing of cryptographic transformation length of a key choose from the assumption that the best attack to it is full search of keys (thus search complexity of all possible keys grows exhibitor with growth of number of bits of a key) taking into account prospects of development of computer facilities. From the statistic point of view, it is necessary to touch about half of possible keys before there will be a correct. Therefore for a key of long 256 bits it is necessary to touch 2^{255} possible variants before there can be a correct key.

Owing to use of the compression, allowing to get rid of redundancy, and architecture of majority construction of the cryptographic transformations, allowing to vary an indicator «speed – firmness», at maintenance of avalanche effect (quantity of

enciphering cycles since which influence of any entrance bit on each target bit is provided) it is possible to reduce quantity of enciphering rounds for transformation of files of codes of the video data.

With reference to cyclic function of cryptographic transformation of GOST 28147-89 which was projected taking into account possible progress of computer facilities for some decades forward and in it the huge stock cryptographic firmness is put, the interrelation of the transformation block size n, the size of a key and k quantity of rounds r of transformation is defined from a parity

$$kz = n / sr , \qquad (1)$$

where s — quantity of semiblocks; z — quantity of times of use of a key in the deployment scheme.

In the standard enciphering of the block in the size of 64 bits, broken on 2 semiblocks, by a key of the long 256 bits, deployment used under the scheme 4 times is provided, at 32 cycles of transformation.

Starting with (1) it is possible to receive parities for the possible sizes of the transformation block n, a key k and quantity of rounds r:

$$n = \frac{kzs}{r}; \quad r = \frac{kzs}{n}; \quad k = \frac{nr}{zs}.$$

Thus the avalanche effect for algorithm of GOST 28147-89 is provided already after $4 – 5$ transformation rounds though initially in their standard it is provided 32 that gives potential possibility for increase in speed at the expense of decrease in quantity of enciphering rounds.

At present developments of enciphering systems their organization on the basis of the codes reducing redundancy, has the limited character. It is connected by that existing and widely used methods of compression at construction of graphic formats and archives have following features (characteristic properties) [2 – 4]:

1. At use of standard archives for information compression it is necessary to consider created by them in the beginning and the end files-archives of the office information. At enciphering of this office information cryptographic analyst receives the additional information and there is possible a cryptographic attack with the dictionary. Enciphering of this information by means of other key and even algorithm therefore is recommended.

2. In the course of coding one kind of statistical redundancy is eliminated. In this case other statistical characteristics are not mentioned. For example, excepting redundancy on the basis of revealing of lengths of series we do not eliminate non-uniformity of distribution, and on the contrary. Therefore at the compressed messages there will be an information which can be used for the cryptographic analysis.

3. The compressed representation is more informative, but code combinations bear the information on structure and semantics of initial messages, i.e. they do not change their structure, namely:

1) methods of the differentiated representation on the basis of differential bear the direct information on the initial message, only with the lowered dynamic range;

2) methods on the basis of Huffman codes provide formation of a code word for each element separately. On them the condition prefix is in addition imposed that allows establishing conformity between code combinations and elements of the initial message;

3) methods of compression on the basis of coding algorithms lengths of series and algorithm LZW bear the important structural information, which: has biunique conformity between a corresponding fragment of the processed image; allows to reconstruct semantic structure of the image without its complete recovery;

4) arithmetic coding provides formation of a code combination for several elements. During the time there is a possibility on the basis of the information on probabilities of elements occurrence of to establish conformity between parts of a code combination and the initial data.

Common faults for methods of compression on the basis of reduction of statistical redundancy are that:

– memberwise statistical codes though reduce redundancy, but do not change structure of each element separately or groups of elements;

– code combinations represent repeating blocks of the information in cases of message elements processing with identical statistical properties;

– in case of processing strongly saturated images on an input of statistical coders the messages which elements have uniform distribution arrive. In this case code combinations will repeat completely the initial message;

– prevalence of one elements comes to light on the basis of probabilities tables and a condition prefix. Besides, the given properties can be homogeneous between the next blocks.

Thus, replacement of one element in the initial message will not lead to change of all code design. The local part of the code combination which are responsible for the given element will change only. Even replacement of several elements will not lead to change of all code design. Hence, the condition of dispersion and elements hashing is not satisfied.

4. The methods of compression on the basis of complex processing with use of images transformation possess following features: allocate significant and insignificant elements, i.e. the quantity of those elements which contain not

significant from a position of semantics the information on the image is reduced; processing of significant components will be organized on the basis of methods of statistical coding and revealing of identical elements series; reconstruction the important objects of the image is provided on the basis of reception of the semantically information on the limited quantity a component; compression is carried out on the basis of serial processing; increases quantities of the office data.

The given features lead to that concerning realizations of enciphering functions there are following lacks:

– lacks base a component of complex process compression remain;

– the increase in quantity of the office data is the additional information at the cryptographic analysis;

– the additional information for restoration of the semantic maintenance of images on the basis of reconstruction only the limited quantity a component contains.

The given features of a compression method limit construction possibilities on their base of cryptographic systems. Compression systems are generally characterized by vulnerability from a creation position enciphering algorithms both at formation of information components, and at formation of office components. It does not allow to organized processes of dispersion and hashing of initial messages. Therefore it will be necessary to develop technologies of a compression on which base possible creation of enciphering functions.

On the basis of the conducted problem research of technologies of a compression of images it is possible to formulate the requirements providing realization of functions of cryptographic transformations.

1. Formation of code designs should be carried out by an integrated principle. In this case formation of code designs is spent to two stages:

– formation of the value *N* bearing the information at once about several elements of the message *A*, mean $N = f(A)$, where N — the value of a code generated for the initial message *A* on the basis of a rule $f(\bullet)$;

– the organisation of code C representation of value *N*, mean formation of a code word not for the nitial message, and for size *N*: $C = f_q(N)$, where $f_q(\bullet)$ — the operator providing allocation *C* of categories quantity for size *N*.

2. The initial message can be restored on the set code only in case of presence of full data on a vector of the office data *S*, mean if $S^{\bullet} = S$ that $A = f^{(-1)}(N)$. Otherwise at absence at least one element of a vector of the office data exact restoration of the initial message would be impossible, mean if $S^{\bullet} \neq S$, that $A \neq f^{(-1)}(N)$, where $f^{(-1)}(\bullet)$ — the return operator of reception of the message *A* on value of a code-number *N*. It is clear that operators $f(\bullet)$ of direct and $f^{(-1)}(\bullet)$ return compressing transformations are known.

3. It is important to notice that in comparison with other kinds of representation of the information of the image differ that:

– have two-dimensional spatial structure;

– there are features of perception of images visual system of the person, consisting that the most important information are the low-frequency components bearing the information on contours and borders of large objects, and also brightness the components having a priority concerning color components.

Conclusion

1. It is proved that for increase of processing and delivery efficiency of the video data with use it is information communication systems of real time it is required to carry out cryptographic enciphering simultaneously with the organization of compact representation. It allows reducing on the one hand time expenses for processing, and on the other hand in addition to raise cryptographic firmness of code numbers.

2. The methodology of formation of cryptographic transformations on the basis of compression methods of the data is developed. On the basis of the offered methodology requirements rather are defined: constructions of a compression technologies realizing functions of dispersion and hashing; reductions of time expenses for processing and data transmission in it is information communication systems.

LITERATURE

1. *Шеннон К. Э.* Теория связи в секретных системах / В кн. К. Э. Шеннона «Работы по теории информации и кибернетике». — М. : ИЛ, 1963. — С. 333–402.

2. *Миано Дж.* Форматы и алгоритмы сжатия изображений в действии: учеб. пособ. / Дж. Миано; пер. с англ. — М. : Триумф, 2003. — 336 с.

3. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. — М. : Техносфера, 2005. — 1073 с.

4. *Королев А. В.* Метод комплексной обработки изображений / А. В. Королев, В. В. Баранник // Інформаційно-керуючі системи на залізничному транспорті. — 1999. — № 5. — С. 10 – 17.

Стаття надійшла до редакції 01.07.2011.