UDC 681.3

V. Larin, A. Korotenko, D. Baiush, A. Ivanichenko

*Ivan Kozhedub Kharkiv National Air Force University, Kharkiv*

# A METHOD FOR CONSTRUCTING A COMBINED COMPRESSION SYSTEM AND ENCRYPTION OF VIDEO DATA

*Held justify that for improving the efficiency of processing and delivery of video data using real-time communication systems required to implement cryptographic encryption simultaneously with the organization of compact representation. It is shown that the existing compression methods do not ensure the implementation of dispersion and mixing technologies which are fundamental for the construction of cryptographic transformations. It outlines the steps of building a methodology for creating cryptographic transformations on the basis of data compression methods.*

***Keywords:*** *steganography, quality indicators, resistance, algorithm of embedding.*

## Formulation of the problem

In modern conditions the information has become a unique strategic resource, which characterizes the potential of the state, along with its material and other resources. Therefore, there is a saying about "who owns the information, controls the situation."

However, the increased vulnerability of the information that has made it necessary to pay more attention to protect it. One of the priorities in ensuring information security is " the establishment of protection against unauthorized access to information resources and disruption of the functioning of computer - telecommunication networks ". The cost of providing the development of information security by modern standards account for about 60% of all costs associated with the development of automation. Most of these funds is based on special cryptographic data conversion techniques. Data encryption scheme presented in fig. 1.

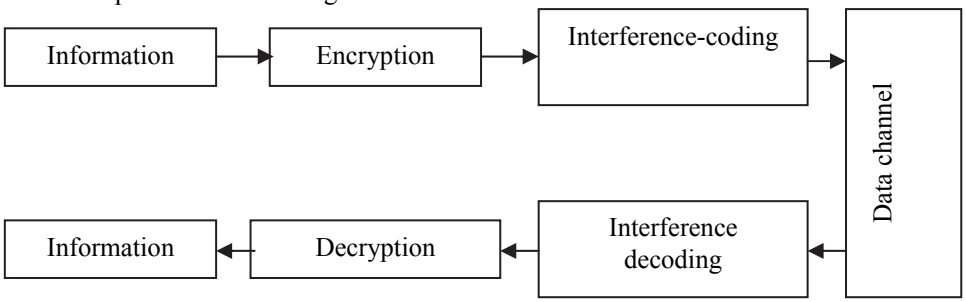


Fig. 1. The scheme of data encryption

In all information's flow, which is circulating in the information space of the state, it is increasing the share of video. This is due to the following reasons:

1) by the development of aerospace monitoring systems. In this case, the image received from the satellites, manned and unmanned aircraft and airbuses;

2) by the creation of a new generation infocommunication systems in which the basic type of information are transmitted multimedia data.

Existing transmission systems can not efficiently transmit a large volume of video data, and for long-term storage of images require large amounts of memory on the respective devices. One of the main ways to reduce the volume of data sent and stored video data is their compact representation.

In this case, the information supplied on the encryption will be digitized image. The critical information systems required to provide security. Therefore, the data processing and transmission processes in modern communication systems include compression stages, encryption and error-correcting coding (fig. 2).

In the process of forming a compact description of data transmission is achieved increasing the informativeness of structures and reducing the initial volume. This allows:

– to get rid of redundancy, which is peculiar to any plaintext and, therefore, to reduce the amount of information which can be used in cryptanalysis;

– to reduce the encryption time by reducing the length of messages being processed.

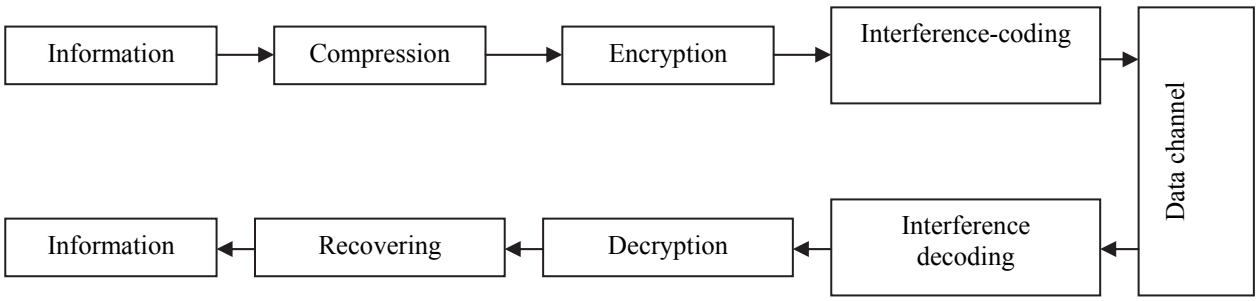


Fig. 2. Structuraly-functional diagram of the data processing in infocommunications components

Therefore, in practice, it is organized the sharing of compression and encryption information.

Technologies of video compression, in most cases, include coding techniques that reduce redundancy. During such coding codewords formed of two types, namely, information and overhead components. Information component carries information about processed messages, while the utility is a component of the auxiliary for one-one forward and reverse compression transformations. Given that the structural-functional diagram of processing of the information shown in fig. 2, can take one of the options considered in fig. 3–5.

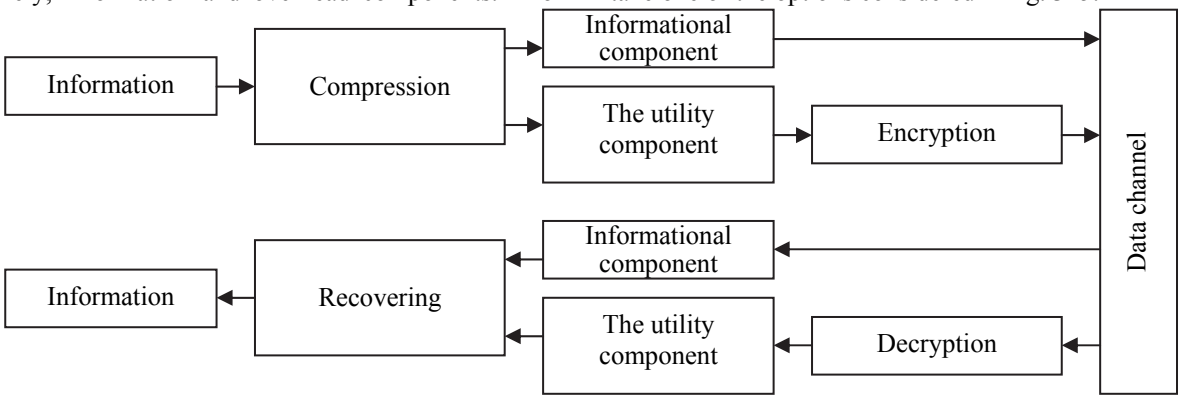


Fig. 3. Scheme of combined system of compression and encryption video

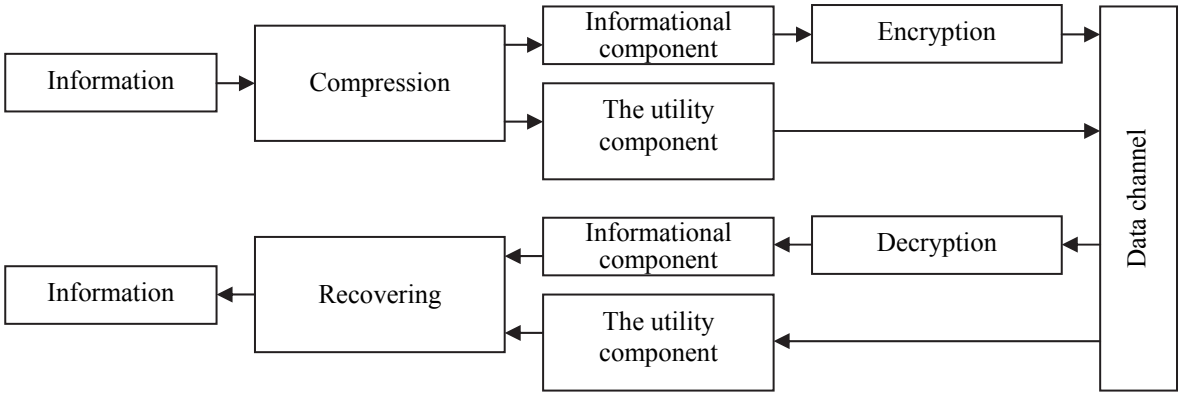


Fig. 4. Scheme of combined system of compression and encryption video

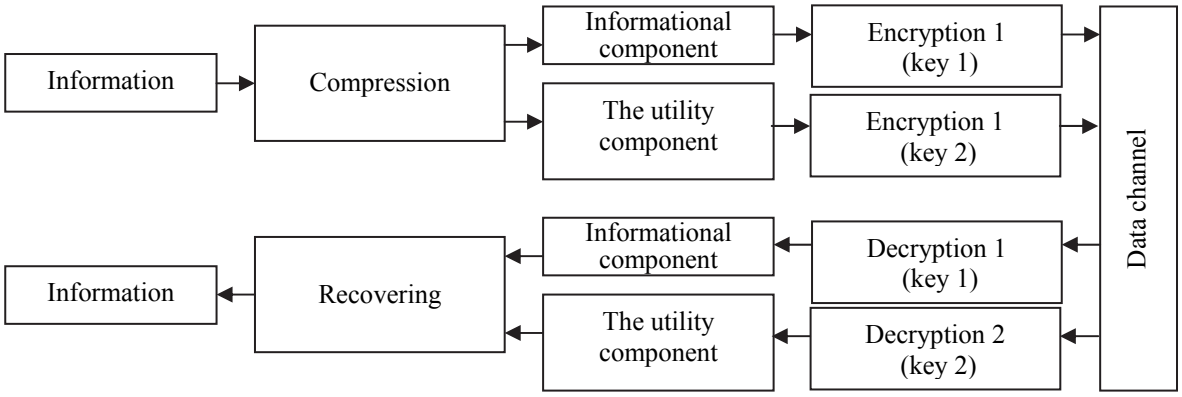


Fig. 5. Scheme of combined system of compression and encryption video

Consider the characteristics of the assessment process to protect video for wireless IR.

Assessment of information stealth messages carried on the following parameters:

1. Safety time $T_б$:

$$T_б = \min_{1 \le i \le M}\{T_{бi}\}.$$

Here $T_б$ — safe operation time of the algorithm, that implements the method of cryptanalysis, which evaluates as $T_{бi} = S_{бi} / \varphi S_{обр}$; $S_{бi}$ – time complexity of the algorithm that implements method of cryptanalysis; $S_{обр}$ – the performance of the computing system available to the enemy.

2. Measures of information stealth, defined as the probability $P_{inf}$ of a $P_к = \max_{1 \le i \le M}\{P_{кi}\}$.

1) the probability $P_i$ of a correct recovery of plaintext

$$P_i = \max_{1 \le i \le M}\{P_{i_i}\}$$

reliable decoding (recognition) of the message, which consists of:

2) the probability $P_к$ of a correct secret key data recovery here $P_{кi}$ $P_{i_i}$ – the probability of correct recovery respectively of the secret key and open the information part, in the case of an intruder method of cryptanalysis.

For the image processing option is directly proportional to the peak value of the signal / noise ratio in the case of unauthorized access $P_{inf} \sim h_н$. This is because the probability $p_{вро}$ of detection and identification of the object of observation depends on the characteristic of detail d on the ground (resolution), which provides a photographic aboard UAVs (depending on the height detachably focal length, the number of elements in the CCD array, tabl. 1.

In turn, the actual resolution and the ability to relatively reliable decoding (recognizers) image objects is determined to set parameters photographic quality of the reconstructed images. As such a measure used by the magnitude of the peak signal / noise ratio (POSSH). Therefore, the information secrecy measure in the case of image protection is determined POSSH value, which is formed in the case of unauthorized access.

3. The video data processing time $T_{obp}$, comprising the steps of direct $T_{sd}$ and reverse $T_{dsd}$ cryptographic encryption. encryption time is determined performance computing system operations and the amount spent for the encryption. Given the total delivery time T for encryption of video is defined by

$$T = T_{obp} + T_{ps},$$

where $T_{obp}$ – the processing comprising

$$T_{obp} = T_{sd} + T_{dsd} /$$

Here $T_{ps}$ – the transfer of encrypted data on ICS.

Table 1

Requirements for the resolution of images capacity

| Objects | Resolution, м | | | | |
|---|---|---|---|---|---|
| | Detection | Recognition of the type (total) | Recognition model (accurate) | Detailed description | State analysis |
| Ground vehicle | 1,5 | 0,6 | 0,3 | 0,05 | 0,025 |
| Railroad supply | 1,5 – 3 | 0,6 | 0,3 | 0,03 | 0,025 |
| Single-floor buildings | 3 | 1,5 | 0,9 | 0,15 | 0,025 |
| The ploat. means | 7,6 – 15 | 4,5 | 0,6 | 0,3 | 0,013 |
| Single house | 6 | 2 | 1,2 | 0,3 | 0,075 |
| Roads | 6 – 9 | 6 | 1,8 | 0,6 | 0,15 |
| Bridge | 6 | 4,5 | 1,5 | 1 | 0,3 |
| Railway components | 15 – 30 | 15 | 6 | 1,5 | 0,6 |
| Ports and supply points | 30 | 15 | 6 | 3 | 0,3 |
| Settlements | 60 | 30 | 3 | 3 | 0,3 |
| Terrain | – | 9,1 | 4,5 | 1,5 | 0,15 |

## Conclusions

1. It is proved that in order to increase the efficiency of processing and delivering of video data using real-time communication systems it is required to implement cryptographic encryption simultaneously with the organization of compact representation. This allows, on the one hand, to reduce the time required for processing, and on the other, to increase the cryptographic ciphers.

2. Existing compression methods do not ensure the implementation of dispersion and mixing technologies, which are fundamental for the construction of cryptographic transformations.

## Literature

*1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.*

*2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: «МК-Пресс», 2006. – 288 с.*

*3. Тарасов Д.О.. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д.О. Тарасов, А.С. Мельник, М.М. Голобородько // Інформаційні системи та мережі. Вісник НУ "Львівська політехніка". – Львів, 2010. – № 673. – С. 365-374.*

*4. Kutter M. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc.Of the SPIE Storage and Retrieval for Image and Video Databases V. 1997. – Vol. 3022. – P. 518-526.*

*5. Darmstaedter V. Low Cost Spatial Watermarking / V. Darmstaedter, J.-F. Delaigle, J.J. Quisquater, B. Macq // Computers and Graphics. – 2008. – Vol. 5. – P. 417-423.*

*Надійшла до редколегії 20.03.2017*

**Рецензент:** д-р техн. наук проф. В.В. Бараннік, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

### МЕТОД СТВОРЕННЯ ОБ'ЄДНАНОЇ СИСТЕМИ КОМПРЕСІЇ ТА ШИФРУВАННЯ ВІДЕОДАНИХ

В.В. Ларін, А.Ю. Коротенко, Д.О. Баюш, А.С. Іваніченко

*Проводиться обґрунтування того, що для підвищення оперативності обробки і доставки відеоданих з використанням інформаційно-комунікаційних систем реального часу потрібно здійснювати криптографічне шифрування одночасно з організацією компактного представлення. Описується, що існуючі методи компресії не забезпечують впровадження технологій розсіювання і перемішування, які є базовими для побудови криптографічних перетворень. Розкриваються етапи побудови, методологія формування криптографічних перетворень на базі методів стиснення даних.*

***Ключові слова:*** *стеганографія, показники якості, стійкість, алгоритм встроювання.*

### МЕТОД ПОСТРОЕНИЯ ОБЪЕДИНЕННОЙ СИСТЕМЫ СЖАТИЯ И ШИФРОВАНИЯ ВИДЕОДАННЫХ

В.В. Ларин, А.Ю. Коротенко, Д.А. Баюш, А.С. Иваниченко

*Проводится обоснование того, что для повышения оперативности обработки и доставки видеоданных с использованием инфокоммуникационных систем реального времени требуется осуществлять криптографическое шифрование одновременно с организацией компактного представления. Показывается, что существующие методы сжатия не обеспечивают реализацию технологий рассеивания и перемешивания, которые являются базовыми для построения криптографических преобразований. Излагаются этапы построения, методология формирования криптографических преобразований на базе методов сжатия данных.*

***Ключевые слова:*** *стеганография, показатели качества, стойкость, алгоритм встраивания.*