DOI: https://doi.org/10.53052/9788367652001.13

Andrii VLASOV[1], Oleksandr SIEVIERINOV[2]

Opiekun naukowy: Gennady KHALIMOV[3]

TECHNOLOGICZNE ASPEKTY PRZETWARZANIA INFORMACJI WIDEO Z KONTROLĄ BEZPIECZEŃSTWA ZASOBÓW INFORMACJI

Streszczenie: W artykule przedstawiono metodyczne podejścia do rozwiązania problemu ochrony zasobu informacji wizyjnej dla komponentu teleinformatycznego infrastruktury krytycznej, z wprowadzeniem ulepszonej technologii przetwarzania zasobu informacji wizyjnej i zapewnienia jego bezpieczeństwa informacyjnego, zwiększającego bezpieczeństwo zarówno zasobu samego siebie i informacje o jego usługach.

Słowa kluczowe: przetwarzanie (kodowanie i szyfrowanie), integralność, przetwarzanie kryptograficzne, ochrona zasobu informacji wideo.

TECHNOLOGICAL ASPECTS OF VIDEO INFORMATION PROCESSING WITH INFORMATION RESOURCE SECURITY CONTROL

Summary: The article presents methodological approaches to solving the problem of protecting a video information resource for the info communication component of a critical infrastructure, with the introduction of an improved technology for processing a video information resource and ensuring its information security, increasing the security of both the resource itself and its service information.

Keywords: processing (encoding and encryption), integrity, cryptographic processing, protection of a video information resource.

1. Abstract

Modern processes of introducing the latest information technologies and modern risks in the information space reinforce the importance of ensuring information security. All the main processes of managing objects of a critical structure use information

[1] Kharkiv National University of Radio Electronics, Department Security Information Technology, Associate Professor, oleksandr.sievierinov@nure.ua
[2] Kharkiv National University of Radio Electronics, Department Security Information Technology, Associate Professor, andrii.vlasov@nure.ua
[3] Kharkiv National University of Radio Electronics, Head of the Department of Security Information Technology, Doctor of Technical Sciences, hennadii.khalimov@nure.ua

communication systems and systems of information collection, processing and transmission.
In the information provision of management processes of objects of a critical structure, today, increased attention is paid to the implementation and effective use of remote information collection and processing systems (video surveillance systems, video conferencing systems, data from on-board and unmanned aerial vehicles, etc.). At the same time, requirements regarding high-quality provision of video data, prompt delivery of video information, ensuring the necessary level of security and protection of video information resources remain relevant. There are organizational and technical contradictions associated with increasing requirements for the quality (resolution) of video information, data processing speed and the use of low-speed communication channels, sometimes outdated video equipment and technical information protection systems.

2. Introduction

These problems and contradictions require the search for technological solutions to the complex task of ensuring the security of an information resource and its protection while minimizing the economic costs of development and implementation. At the same time, these solutions should guarantee their simple practical adaptation when implementing hardware of a higher technological level at critical structure objects.
Therefore, studies related to ensuring information security and protecting the video information resource, which is formed and processed in the interests of management at critical structure objects, are important.
At the same time, as studies show [1 - 5], the most significant security threats to a video information resource are threats to accessibility and integrity, and from the point of view of ensuring protection, interception, opening and recognition of the resource.
To solve this problem, it is proposed to conduct a set of studies in order to develop new technological solutions and improve methods for processing a video information resource:

- automatic selection (masking) of semantically significant information of video frames (based on a cascade (parallel) scheme for processing a video stream);
- evaluation of the information intensity of the video stream, taking into account its structure and classification of semantically significant elements of the video frame (fragments or macroblocks);
- classification (determination) of the degree of semantic saturation of video frames (a structural unit of a video stream) based on their hierarchical clustering (in time and in spectral-spatial domains);
- processing of video frames based on the structural processing of its macroblocks using selective approaches (ensuring the selection of structural units of the base frame) to reduce the intensity of transmitted video data using cascade decision rules in the spectral space (taking into account the identification and closure of significant structural units, as well as the coordination of future code structures (according to the performed classification of semantically significant fragments of video frames));
- processing of video images based on differential processing of the transformed representation of frames according to the classification of semantically significant

fragments (coding with adaptation of parameters depending on the value of the class of semantic saturation);

- protection of a dynamic video information resource with the formation of several channels for processing and transmitting a video stream according to the classification of the semantic content of macroblock elements (for example, a covert transmission channel for transmitting closed information based on block-symmetric coding methods; an open transmission channel for a coded representation of video images with an embedded information container (formed steganographic tabs));
- reconstruction of a video stream (video images) based on the decoding of various channels, taking into account the class of semantic saturation of video image elements (fragments, macroblocks), intra-frame selection of structural units of the base frame, the formed steganographic channel and embedded encryption methods.

3. Methods

Processing can be realized at different stages of formation, processing and transfer of video data, namely:

1) encryption of video stream (all operations on the decline of intensity of stream and anti jamming encryption are executed with the already hidden view data);
2) after compression submission of video data is created (before the coded video stream gets to a communication channel);
3) in the course of coding (algorithms of enciphering are integrated into the standardized process on processing of initial video data for decrease in their intensity).

For the removal of lacks of every variant it is suggested to use selective approach (data are closed in the process of their encryption).

Such realization is real to development and introduction in the handling systems of data, where realization of programmatic additions and their integration are assumed in a video codec. For this option, encoding and encryption are performed for the source data as they are received for processing.

To ensure information security and improve the security of the video information resource when meeting the requirements for efficiency, reliability and confidentiality in the critical structure management system, it is necessary to develop the proposed methods based on the improvement of standardized MPEG technologies and cryptographic protection algorithms, methods for forming steganographic channels.

It is necessary to first evaluate the information intensity of the video stream in its various transmission and processing options in order to assess the possibilities for improving its processing and protection. General indicator taking into account the correspondence of requirements to the processing methods and the hardware is the bandwidth of the processing channel of the information resource in terms of the initial stream and processing technology (encoding, encryption) and video stream transmission.

In Figure 1 presents a structural diagram of the proposed video information processing technology with security control of the information resource in the information and communication component of the critical infrastructure.

From the standpoint of processing technology (encoding, encryption) and transmission, the throughput of a closed video channel for the info communication component of a critical structure system means the intensity of hidden encoded video data corresponding to the number of frames that need to be processed (from the formation of a hidden container) and transferred in the required time while meeting the requirements security and network bandwidth.

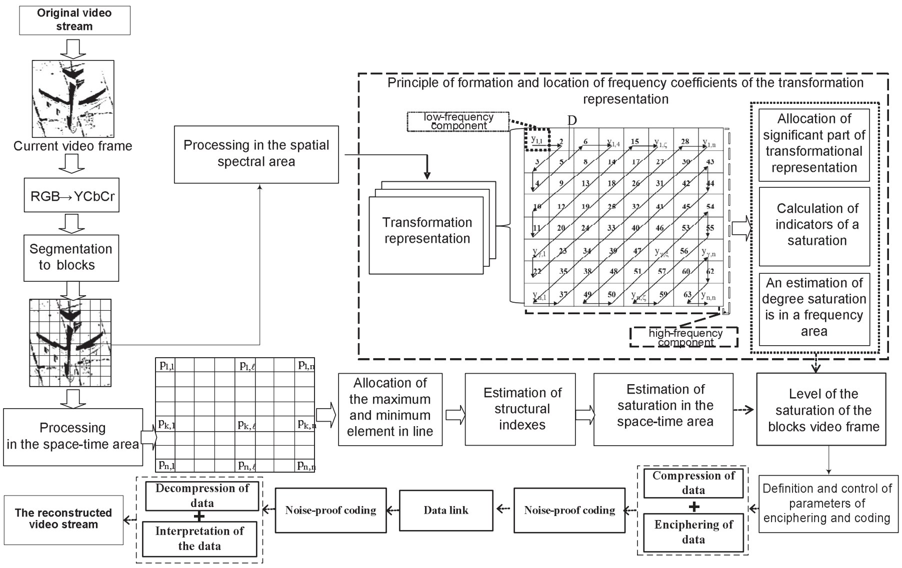

Figure 1. Structural diagram of video information processing technology with information resource security control

The bandwidth of such a video channel depends on:

1) processing time (encoding and encryption) and transmission of the video stream. The shorter the delivery time of the encoded stream, the more frames will be processed and generated in the required time;
2) integrity. The lower the peak signal-to-noise ratio for authorized access, the lower the intensity of the encoded stream and the shorter the delivery time. But this violates the requirement to ensure a given level;
3) the degree of its closure. The lower the peak signal-to-noise ratio for unauthorized access, the higher the degree of closure. The greater the degree of concealment, the more patterns are destroyed during coding and therefore less redundancy is eliminated, and the intensity increases accordingly. This leads to a decrease in the bandwidth of the closed video channel;
4) the degree of saturation of video frames. The higher the degree of saturation, the greater the number of structural units that are processed and closed (encoded according to a given scheme and algorithm according to the assessment of the degree of saturation), and the smaller the number of structural units that are encoded according to the standard algorithm. This leads to an increase in the total intensity, and therefore, to a decrease in the throughput of this video channel.

Hence, in order to fulfill the bandwidth requirements of a closed video channel, it is necessary to reduce the intensity of video data in the context of reducing transmission time, to ensure their safety, protection and delivery for the required time under the necessary conditions of integrity and confidentiality.

To eliminate the maximum amount of redundancy when processing a video stream, it is proposed to use the base I-frame, since it contains the maximum amount of information, and frames of other types contain up to 70% of links to it [1, 2, 4].

At the same time, methods for processing and hiding video data (for a covert channel), which will need to be developed and implemented, should be based on hiding only I-frames (intra-frames contain only independently compressed macroblocks). This ensures complete hiding of the entire video sequence with minimal redundancy.

It is proposed to analyze and process the structural unit of a frame only for its brightness component, and to perform closing (encryption) and encoding procedures for all components (macroblocks) of the frame [4 - 6].

The processing process can be implemented at different stages of the formation, processing and transmission of video data, namely:

1) before encoding the video stream (encryption algorithms are applied to the newly created (uncoded) source video data; all operations to reduce the intensity of the stream and error-correcting coding are performed with already hidden video data);
2) after the compression representation of the video data has been formed (before the encoded video stream enters the communication channel);
3) in the encoding process (encryption algorithms are integrated into a standardized process for processing the original video data to reduce their intensity (at various stages of compression).

The option of encrypting the source data before encoding has the following disadvantages:

- does not take into account the reduction of redundancy in the source video data;
- after encoding, an increase in the initial intensity of the video stream occurs as a result of the destruction of its structure due to pre-encryption;
- an increase in the intensity of encoded encrypted video data entails an increase in the time required to transmit this data in the communication channel.

The option of hiding the video stream after its compression allows reducing the preliminary redundancy of the original video stream and reducing the processing time (including encryption). It provides a high level of information closure, but at the same time they have significant drawbacks:

- error propagation occurs in case of errors in the communication channel;
- cryptographic processing is subject to the entire video information flow, which increases the total processing time of the generated video data on the transmitting side and the processing time of video data on the receiving side.

It is proposed to use a selective approach (an option in which the data is closed in the process of encoding). This approach is real for the development and implementation of data processing systems, where it is possible to implement software add-ons and integrate them into the video codec. For this option, encoding and encryption are performed for the source data as they are received for processing.

In the process of forming a video information flow, when implementing a selective approach, the following is achieved:

- increasing the information content of the transmitted structures and reducing the initial intensity;
- eliminates redundancy (reduces the amount of information) that can be used in cryptanalysis;

- encryption time is reduced by reducing the length of processed messages.
- The options considered also have common disadvantages:
- closing the video stream is not in real time;
- the intensity of the closed video stream is often significantly higher than the intensity of the original.

Therefore, to eliminate these shortcomings, it is proposed to use selective technology (a set of methods in which data is closed during encoding). Such an implementation is real for development and implementation in real-time data processing systems, and it is also possible to implement add-ons (software) and their integration into existing video codecs. For this option, encoding and encryption are performed for the source data as they arrive for processing.

The selection mechanism means closing not the entire video frame, but only its significant components.

In the process of automatic selection of significant components, it is proposed to take into account the structural features of video stream formation.

For the selection of significant structural units are invited to identify the most informative, in terms of structural and semantic content, the components of the base frame. Since the luminance component of the video frame carries the most complete information, it is proposed to identify significant structural units on the basis of the luminance components. Therefore, the decision to close the structural unit is proposed to be carried out according to the results of the analysis of the information component of the aggregate of the blocks of the luminance component.

To determine the energy saturation of blocks, it is proposed to introduce the concept of blocks of three types [2, 4, 6]:

- slightly saturated blocks (blocks in which there are uniform sections of the image);
- average saturation (blocks in which there are minor differences between the pixels, respectively, smooth transitions of contrast are present);
- highly saturated blocks (blocks in which there are sharp transitions of brightness and contrast of the image).

It is proposed to evaluate the structural and semantic information content of the structural unit (macro block) from the standpoint of spectral characteristics [2 - 4] or on the basis of metrics [5, 6].

A system of indicators has been developed for identifying the most significant blocks of the brightness component of a video frame according to the degree of semantic and structural saturation based on the assessment of indicators: in the space-time domain and in the space-spectral domain [2, 6].

To improve the classification of fragments of video frames (macroblocks), it is proposed to use a two-basis principle, which covers the spatial-temporal and spatial-spectral representation of a video frame.

In the course of automatic selection of significant components it is offered to consider structural features of formation of a video stream [2, 4 - 6].

It is offered to apply selective methods of enciphering to increase of a noise stability of all video stream, and owing to simple realization of these methods and small computing expenses. At unauthorized interception of such video stream with mistakes, in process to interpretation the quantity of these mistakes will only increase.

The analysis of various options of selective enciphering showed that the most effective is enciphering after a stage of transformational transformation [1, 2].

To increase the classification efficiency of fragments of video frames (macro blocks), it is proposed to use the two-basis principle, which covers the spatio-temporal and spatial-spectral representation of the video frame. Then, to evaluate the level of saturation in blocks of video frames, it is proposed to use the following indicators:

- in the spatio-temporal region - the structural indicator of the block, which determines the most significant elements of time;
- in the spatial region of the spectrum, the block saturation index , which determines the most significant transformation coefficients in each selected zone.

It is proposed to determine the energy saturation of blocks after a spatial spectral representation (SSR), for example, a discrete cosine transform (DCT). Using SSR, a transition is made from the spatio-temporal representation of the video frame to the spatially spectral one. The components of the SSR transform (DCT) are integral characteristics of the structural content of the image fragment. Moreover, the integral properties of the components depend on their position in the transform.

It is necessary to develop the main stages of formation of a binary code of the ciphered significant structural unit which are based on three technological components for development of a method of coding of significant structural unit (macro blocks of frame):

- the first component consists in formation of a binary code of value components of transformation representation for the image block;
- the second component consists in formation of a code design of the structural unit of the basic video frame which is subject to enciphering;
- the third component consists in formation of matrixes of a binary code of significant structural unit of the same size, as an enciphering key.

It is proposed to develop a method for decoding a closed video stream based on the selection (selection of closed significant structural units) of the base video frame, i.e. it is necessary to decode the closed base video frame taking into account the definition of significant structural units.

It is also necessary to improve the video image compression method based on the differential processing of the transformed frame representation in accordance with the proposed fragment classification and the implementation of coding with the adaptation of compression parameters (depending on the definition of the saturation class and the presence of a built-in steganography container).

To assess the integrity of video frames, it is proposed to use the verified parameters - a measure of structural similarity (SSIM) [3, 7].

A measure of structural similarity SSIM is a comprehensive assessment of the similarity (quality) of images, which has the following components for comparing the input and output images: the correlation coefficient between images, an assessment of the similarity of the average brightness values of the images, an assessment of the similarity of the contrasts of the two compared images.

This criterion takes into account both the number of gaps and the number of missing elements in individual gaps, as well as their slight displacement. The ranges of values for their criteria-based assessment are formed on the basis of experimental data.

4. Conclusions

The article proposes an approach to adapting the degree of coding and unambiguous restoration (decoding) of data depending on the class of semantic saturation of image fragments (video frame) due to the strategy of differential determination (selection) of coding parameters. An increase in the efficiency of compression and coding is guaranteed due to the regularization of the brightness component of images at a given level of integrity of the information resource, namely, the preservation of the original semantic component of video frames.

The strategy for selecting compression and coding parameters includes a method for generating these parameters, a quantization matrix, and a mechanism for adapting them depending on the semantic richness class of the video frame (its fragments). Depending on the class of semantic saturation, the parameters can be calculated automatically (or their choice is determined earlier empirically based on the processing of experimental data).

Thus, the integrated development and application of these methods will allow developing a technology for processing a video information resource and improving the protection of a video information resource and service information in the infocommunication component of a critical infrastructure while ensuring the necessary (not lower than a given) level of confidentiality and accessibility of the resource, as well as maintaining (controlling) the key (semantically meaningful) information.

REFERENCES

1. BARANNIK V., POLYAKOV V.: The encoding of the transformed image in info-communication systems. Kharkiv, 2010.
2. BARANNIK V., KHAKHANOVA G., VLASOV A. and others.: Information technologies for encoding dynamic video information streams. Kharkiv, 2021.
3. SHMATKO O., BALAKIREVA S., VLASOV A. and others.: Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies 3(2020)9(105): Information and controlling system. 6 – 19.
4. VLASOV A., LUKIN V., KOMOLOV D.: Coding of information resources of systems of a video conferencing for increase of their safety. Radio electronics and informatics,2(2013), 44 – 48.
5. KHALIMOV G., SIEVIERINOV O., KOTUKH Y., DIDMANIDZE I., VLASOV A.: Towards three-parameter group encryption scheme for MST3 cryptosystem improvement. Proceedings of the 2021 5th World Conference on Smart Trends in Systems Security and Sustainability, WorldS4 2021. London, United Kingdom. 204 – 211.
6. VLASOV A., SHIRYAEV A.: Method of coding of video images with masking for increase of safety of video information resources. Radio-electronic and computer systems 3(2013), 65 – 73.
7. VLASOV A.: Estimation of quality methods disguise images for detection edge contours. Science-Based Technologies 2(2013)18, 193 – 197.