Methods for Decoding Informational Codes of Crypto-compression Codegrams to Improve Information Security

Vladimir Barannik[a], Serhii Sidchenko[b], Natalia Barannik[a], Dmitriy Barannik[c], and Sergii Shulgin[c]

[a] *V. N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, 61022, Ukraine*
[b] *Ivan Kozhedub Kharkiv National Air Force University, 77/79 Sumskaya str., Kharkiv, 61023, Ukraine*
[c] *Kharkiv National University of Radio Electronics, 14 Nauky ave., Kharkiv, 61166, Ukraine*

Abstract

The analysis of the main threats (risks) to information security in video surveillance and video conferencing systems. Ensuring information security of video data (static and dynamic) resources should be organized with the preservation of the specified quality while maintaining the specified availability. The article develops methods for decoding information codegrams of images formed on the basis of floating coding schemes with a decrease in the original volume of video data. Decoding methods have six main steps. At the first stage, the restoration of the service components of cryptocompression codegrams, presented in encrypted form, is carried out. In the second step, the number of elements that will be reconstructed from the corresponding information code is determined. At the third stage, the information code is extracted from the general code stream of the information component. At the fourth stage, the decoding of the information component code is organized. Then the third and fourth stages are repeated until all codes of the information component are completely decoded. At the fifth and sixth stages, the restoration of image segments and the reconstruction of the image based on them are organized. Without knowing the correct base system, the attacker cannot correctly establish a correspondence between the generated codegrams and the number of elements involved in their formation, and also cannot correctly position uneven codegrams in the general code stream. As a result, the attacker cannot decode the image correctly. Due to the additional use of uncertainty, an increase in the level of cryptographic resistance of the generated codegrams is achieved. Images are reconstructed without loss of quality, that is, bit by bit. In the process of cryptocompression coding, in addition to ensuring information security, a decrease in the volume of cryptocompression image representation is achieved, which ensures an increase in their availability.

Keywords

Cryptocompression image representation, information security, information security, encryption, encoding, image compression, confidentiality, floating circuits, differentiated basis.

1. Introduction

Threats (risks) associated with the compromise of video surveillance and video conferencing systems, from the point of view of reflexive control, enable an attacker (the opposing side) to be one rank of reflection higher. The main threats to security breaches include:

1. intercepting a signal from CCTV cameras or obtaining the possibility of direct information retrieval from them by an attacker, which will enable him to conduct reconnaissance without using his means.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: vvbar.off@gmail.com (A.1); sidserg72@gmail.com (B.2); barannik11121972@gmail.com (A.3); d.v.barannik@gmail.com (C.4); sssh.sergey@gmail.com (C.5)
ORCID: 0000-0002-2848-4524 (A.1); 0000-0002-1319-6263 (B.2); 0000-0001-9098-360X (A.3); 0000-0003-4235-300X (C.4); 0000-0001-5174-290X (C.5)

2. Substitution of a true signal from CCTV cameras for a false one, which can contribute to the introduction of inaccurate information, misleading the decision-maker, and making an erroneous decision.

3. Unauthorized activation (gaining access) of video conferencing facilities, which will enable the enemy to use them for intelligence purposes.

4. Intercepting a video signal in a video conferencing system or gaining access to equipment, which contributes to the disclosure of the confidentiality of negotiations, and due to the fact that the information circulating in crisis management systems, in aggregate, can take the characteristics of information with limited access, this can lead to leakage critical information.

5. Suppression of signals from video surveillance systems and video conferencing, which can lead to a complete or partial loss of video information and/or delays in its transmission.

Illegal disclosure (interception) of video information transmitted through transmission channels or stored in video recording equipment and databases can lead to a large number of threats to the security of an object (person, enterprise, structure, system, state, etc.), including:

- Violation of individual rights and freedoms.
- Disclosure of personal data, including medical secrets.
- Disclosure of bank secrets and commercial secrets of the enterprise.
- Disclosure of the secrets of the investigation and legal proceedings, as well as the results of operational-search activities.
- Opening the patrol system and/or the location at a given time of patrol detachments (on foot and by road) of the National Police and the National Guard of Ukraine, which is critical in crises and, especially, in the areas of the operation of the combined forces (anti-terrorist operation).
- The transfer of the commission of offenses to other places not equipped with open video cameras, and, therefore, efforts aimed at reducing the level of offenses will lead to a change in the place, method, and time of the offense.
- Opening of routes (system) of movement and/or location at a given time of mobile (operational-search) groups, as well as columns and individual samples of weapons, special and military equipment.
- Disclosure of information about cargo transportation (including their location at a given time) by road, sea (river), rail, and air transport for the needs of the security and defense sector of the state, as well as critical (important) infrastructure of the state (region).
- Opening the security system of the critical (important) infrastructure of the state (region) and protected objects of different property rights, as well as opening the state of the protected object at a given moment in time.
- Opening of border and customs control systems, their weak points, and state at the current time.
- Opening the grouping of their troops, elements of the battle order, the system of protection and defense of checkpoints (positions, areas, borders), as well as the composition of forces and means allocated for these events and/or located in places of permanent deployment.
- Compromise (disclosure, interception by the enemy) of intelligence received by means of special reconnaissance and video surveillance, which can contribute to a change in the deployment of enemy forces, the substitution of false targets and demonstration of false intentions, as well as a change in their designs and plans.
- Compromising the work of monitoring missions and disclosing information to the opposing side (group), etc.

There are various approaches to ensuring information security of images, which are organized both for the original (pre-compressed) images and images presented in the compressed form [1–42]. They include:

- Cryptographic protection methods are based on data encryption [1–16].
- Cryptographic methods of protection are based on scrambling for reversible distortion of images or their critical areas [1, 5–9, 17–24].
- Methods of steganography image processing to ensure the safety of both embedded data and video data itself [25–36].
- Secret sharing technology to ensure the security of one or more images [1, 37–41].
- Methods that implement access rights management and privacy policies [1, 8].

- Transformations that remove critical areas in images [1].
- Geometrically reversible image distortion [42].

They are characterized by the following problematic disadvantages:

- Ensuring the confidentiality of video data without using compression technologies leads to a significant decrease in its availability.
- Ensuring the confidentiality of images using compression technologies after and/or between the stages of the data compression process is based on the separation of the encryption and compression functionality. This also leads to a decrease in the availability of video data.

In the process of ensuring the information security of video data, it is necessary to solve a significant problem related to the fact that it must be organized with the preservation of given image quality while maintaining a given availability.

To solve this problem in [43, 44], approaches to cryptocompression coding of images are presented, which ensure the integration of compression and encryption technologies, which allow solving the identified problem. However, the processes of decoding the codegrams of the cryptocompression representation of images are not considered.

Therefore, the purpose of the article is to develop methods for error-free decoding of information components of the cryptocompression representation of images generated on the basis of floating coding schemes.

2. Main Part

The codegram of the cryptocompression representation of the image consists of two components:

- Information component, which consists of code sequences N variable length and formed as a result of convolution of values of a variable number of elements of the original image A and service data systems S rule-based $f(\cdot)$:

$$N = f(A; S);$$

- A set of service components that depend on the selected coding scheme. Thus, the scheme of cryptocompression coding in the basis along the upper bounds as service data assumes the presence of the base system $G^{(m)} = \{g_i\}$. Scheme of cryptocompression coding in a differentiated basis except for the base system $G^{(m)} = \{g_i\}$ requires a system of lowering dynamic range values $Z^{(m)} = \{z_i\}$.

The service data system in the cryptocompression representation is encrypted S_c and requires preliminary decryption using a cryptographic transformation $D(\cdot)$ on the key of transformation K:

$$S = D_K(S_c),$$

where S is decoded representation of the radix system.

If to perform direct $E(\cdot)$ and vice versa $D(\cdot)$ the cryptographic conversion used an authentic conversion key K (the same session key for symmetric systems or a secret and corresponding public conversion key for asymmetric encryption systems), as well as encrypted data S_c have not been deliberately or erroneously modified, then the decrypted data S will be identical to the original cryptocompression representation service components S bit to bit, i.e. $S = S$:

$$S = D_K(S_c), \text{ i.e. } S = D_K(E_K(S)).$$

The generalized scheme for decoding the floating scheme of the cryptocompression image representation is shown in Fig. 1. The decoding process of the information component of the cryptocompression representation is organized in the reverse order with respect to the encoding process and has its characteristics depending on the selected scheme.

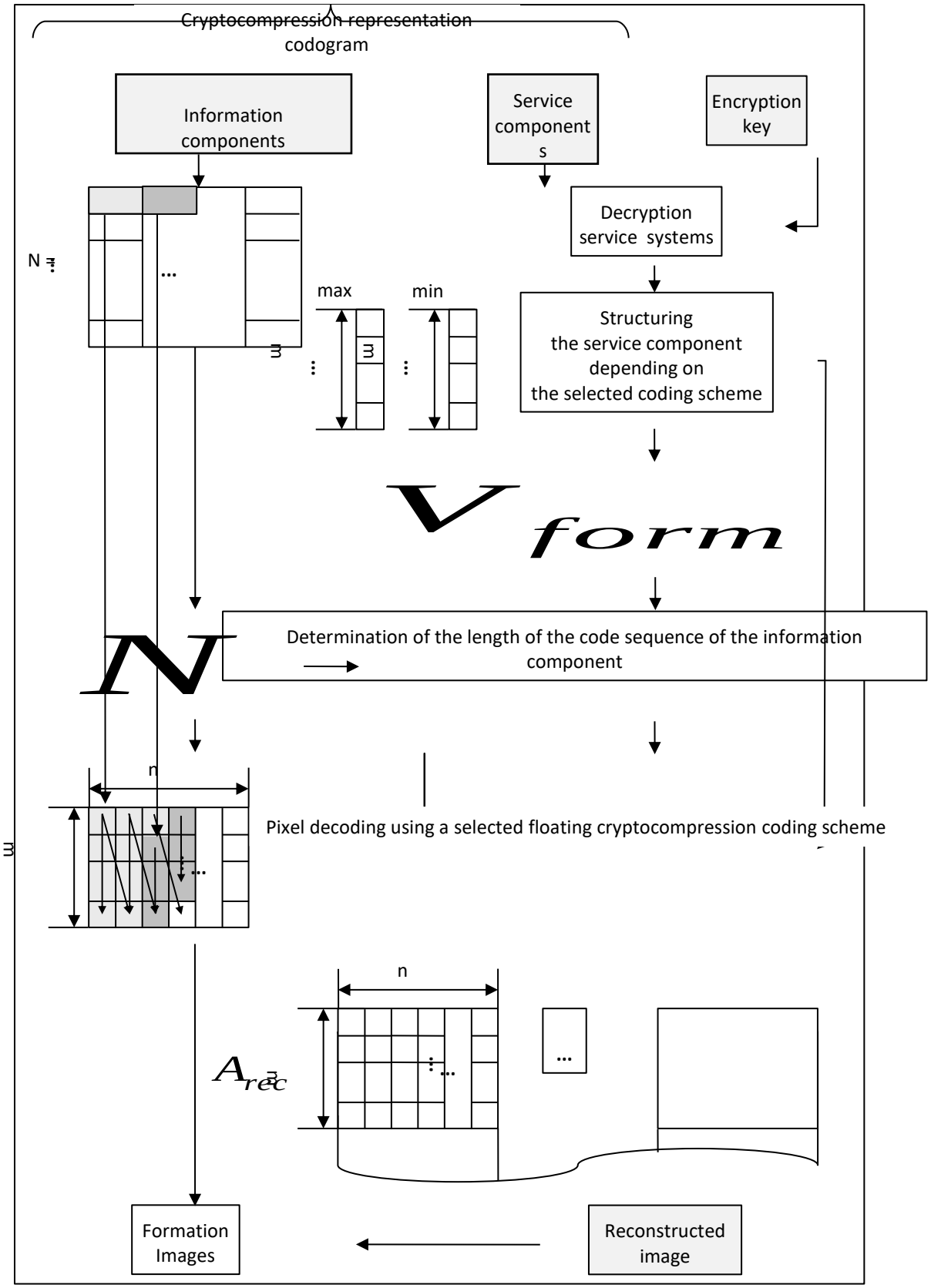

Figure 1: Generalized scheme for decoding the floating scheme of cryptocompression representation of images

Let us consider the features of the process of decoding the information component of the cryptocompression representation for floating coding schemes in the basis along with the upper bounds and the differentiated basis.

The process of decoding the information component of the cryptocompression representation of images based on a floating coding scheme in the basis along the upper boundaries is organized on the basis of performing the following steps.

Stage 1. Expansion of the service component of the cryptocompression representation $G^{(m)} = \{g_i\}$, $i = \overline{1,m}$, up to the power of the original image fragment in a one-dimensional vector form $S^{(m\times n)} = \{s_\tau\}$ based on the formula:

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

where τ is the linear coordinate of the element; m is the number of lines in the image segment into which the original image was split during the encoding process; n is the number of columns in the image segment; [ ] is the whole part.

Stage 2. From the analysis of the service component of the cryptocompression representation $S = \{s_\tau\}$ the number of elements is determined V_{form}, on the basis of which the code values, were generated Ninformation component of the cryptocompression representation. To do this, use the formula:

$$V_{\text{form}} = \underset{V}{\text{argmax}}\left(\prod_{\xi=1}^{V} s_\xi\right) = \underset{V}{\text{argmax}}\left(\prod_{\xi=1}^{V} g_{\xi - m\left[\frac{\xi-1}{m}\right]}\right)$$

given that

$$\prod_{\xi=1}^{V} s_\xi = \prod_{\xi=1}^{V} g_{\xi - m\left[\frac{\xi-1}{m}\right]} \le 2^M - 1,$$

where V is a floating number of elements of the service component participating in the formation of the code of the information part of the cryptocompression representation based on the floating scheme, taking into account the check for overflow of the code word; ξ is the linear coordinate of service data; $(2^M - 1)$ is the largest number that can be stored in a codeword of length$M$ elements.

Stage 3. Determination of the length of the code sequence N information component is carried out on the basis of service component elements $S = \{s_\tau\}$ taking into account the number of elements V_{form} images that formed the information component using the formula:

$$Q_N = [\log_2(\prod_{\xi=1}^{V_{\text{form}}} s_\xi)] + 1 = [\log_2(\prod_{\xi=1}^{V_{\text{form}}} g_{\xi - m\left[\frac{\xi-1}{m}\right]})] + 1.$$

Reading the code sequence from the information component of the cryptocompression representation N length Q_N bit.

Stage 4. Formation of the vector of weight coefficients W whose elements W_τ ($\tau = \overline{1, Q_{\text{пр}}}$) are defined as the product of the elements of the service component of the cryptocompression representation $S = \{s_\tau\}$ that are in positions following the position τ, based on the formula:

$$W_\tau = \begin{cases} \prod_{\xi=\tau+1}^{V_{\text{form}}} s_\xi = \prod_{\xi=\tau+1}^{V_{\text{form}}} g_{\xi - m\left[\frac{\xi-1}{m}\right]}, & \tau < V_{\text{form}}\text{mn}; \\ 1, & \tau = V_{\text{form}}\text{mn}. \end{cases} \quad (2)$$

Stage 5. Reconstruction of the elements of the code number $A^{(\gamma;\chi)} = \left\{a_\tau^{(\gamma;\chi)}\right\}$ in vector form from the code sequence N the information component of the cryptocompression representation is given by the formula:

$$a_\tau^{(\gamma;\chi)} = \left[\frac{N}{W_\tau}\right] - \left[\frac{N}{W_\tau \times s_\tau}\right] \times s_\tau, \tau = \overline{1, V_{\text{form}}}. \quad (3)$$

Stages 4 and 5 can be combined and, taking into account formulas (1) and (2), formula (3) will take the form:

$$a_\tau^{(\gamma;\chi)} = \left[\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} s_\xi}\right] - \left[\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} s_\xi\, s_\tau}\right] \times s_\tau =$$

$$= \left[\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} g_{\xi - m\left[\frac{\xi-1}{m}\right]}}\right] - \left[\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} g_{\xi - m\left[\frac{\xi-1}{m}\right]} g_{\tau - m\left[\frac{\tau-1}{m}\right]}}\right] \times g_{\tau - m\left[\frac{\tau-1}{m}\right]}.$$

Stage 6. Reconstruction of a segment of the original image with dimensions$m \times n$ is carried out on the basis of vector transformation $A^{(\gamma;\chi)} = \left\{a_\tau^{(\gamma;\chi)}\right\}$ into a two-dimensional form based on the ratios:

$$A^{(\gamma;\chi)} = \left\{a_\tau^{(\gamma;\chi)}\right\}_{\tau=\overline{1,Q_{\text{пр}}}} =, i = \overline{1,m}, j = \overline{1,n}, \tag{4}$$

$$i = \begin{cases} \tau - [\frac{\tau}{m}]m, \text{ if } [\frac{\tau}{m}] < \frac{\tau}{m}; \\ m, \text{ if } [\frac{\tau}{m}] = \frac{\tau}{m}, \end{cases} \tag{5}$$

$$j = \begin{cases} [\frac{\tau}{m}] + 1, \text{ if } [\frac{\tau}{m}] < \frac{\tau}{m}; \\ [\frac{\tau}{m}], \text{ if } [\frac{\tau}{m}] = \frac{\tau}{m}, \end{cases} \tag{6}$$

where $a_{i,j}^{(\gamma;\chi)}$ is i^{th} element j^{th} column $(\gamma;\ \chi)^{\text{th}}$ recovered segment $A^{(\gamma;\chi)}$ images.

Step 7. Merging the reconstructed segments $A^{(\gamma;\chi)}$ into the image A . If the codegrams of the cryptocompression representation of the image have not been subjected to deliberate or unintentional modification, then the image is reconstructed accurately bit by bit, i.e. $A = A$.

If the cryptocompression representation used a floating coding scheme on a differential basis, then the restoration of image elements A from the information component of the cryptocompression representation N is carried out taking into account the decrease in dynamic ranges, provided that the service component of the cryptocompression representation consists of a system of bases (maximum values of the dynamic range) $G^{(m)} = \{g_i\}$ and the system of reducing (minimum) values of the dynamic range $Z^{(m)} = \{z_i\}$. Decoding of the information component of the cryptocompression representation is set in the following stages.

Stage 1. Preparatory actions are carried out:

- Expansion of the service component of the cryptocompression representation $G^{(m)} = \{g_i\}$ and $Z^{(m)} = \{z_i\}$, $i = \overline{1,m}$, up to the power of the original image segment in a one-dimensional vector form $S^{(m\times n)} = \{s_\tau\}$ and $R^{(m\times n)} = \{r_\tau\}$ based on formulas:

$$S^{(m\times n)} = \{s_\tau\} = \left\{g_{\tau - m\left[\frac{\tau-1}{m}\right]}\right\}, \tau = \overline{1,\text{mn}}, \tag{7}$$

$$R^{(m\times n)} = \{r_\tau\} = \left\{z_{\tau - m\left[\frac{\tau-1}{m}\right]}\right\}, \tau = \overline{1,\text{mn}}; \tag{8}$$

- Lowering the dynamic range of elements of the extended base system $S^{(m\times n)} = \{s_\tau\}$ based on the formula:

$$p_\tau = s_\tau - r_\tau, \tau = \overline{1,\text{mn}}, \tag{9}$$

where p_τ is an element of the base system in a low dynamic range.

Stage 2. From the analysis of the base system, taking into account the decrease in the dynamic range $P = \{p_\tau\}$, the number of elements is determined V_{form}, on the basis of which the informational component of the cryptocompression representation was formed, using the formula:

$$V_{\text{form}} = \underset{V}{\text{argmax}}\left(\prod_{\xi=1}^{V} p_\xi\right) = \underset{V}{\text{argmax}}\left(\prod_{\xi=1}^{V}(s_\xi - r_\xi)\right)$$

subject to limitation

$$\prod_{\xi=1}^{V} p_\xi = \prod_{\xi=1}^{V}(s_\xi - r_\xi) \le 2^M - 1.$$

Stage 3. Determination of the length of the code sequence N the information component is carried out using the formula:

$$Q_N = [\log_2(\prod_{\xi=1}^{V_{\text{form}}} p_\xi)] + 1 == [\log_2(\prod_{\xi=1}^{V_{\text{form}}}(s_\xi - r_\xi))] + 1.$$

Reading the code sequence from the information component of the cryptocompression representation N length Q_N bit.

Stage 4. Decoding of the code of the information component of the cryptocompression representation image in a differentiated basis is given by the formula:

$$a_\tau^{(\gamma;\chi)} = [\frac{N}{W_\tau}] - [\frac{N}{W_\tau \times p_\tau}] \times p_\tau + r_\tau, \tau = \overline{1, V_{\text{form}}} \tag{10}$$

taking into account the formation of the elements of the vector of weight coefficients W_τ based on the formula:

$$W_\tau = \begin{cases} \prod_{\xi=\tau+1}^{V_{\text{form}}} p_\xi = \prod_{\xi=\tau+1}^{V_{\text{form}}} (s_\xi - r_\xi), & \tau < Q_{\text{пр}}\text{mn}; \\ 1, & \tau = Q_{\text{пр}}\text{mn}. \end{cases} \quad (11)$$

Taking into account formulas (7)–(9) and (11), formula (10) for the restoration of the segment $A^{(\gamma;\chi)} = \left\{a_\tau^{(\gamma;\chi)}\right\}$ images in vector form from the information component of the cryptocompression representation N will take the form:

$$a_\tau^{(\gamma;\chi)} = [\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} p_\xi}] - [\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} p_\xi\, p_\tau}] \times p_\tau + r_\tau =$$

$$= [\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} (s_\xi - r_\xi)}] - [\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} (s_\xi - r_\xi)\,(s_\tau - r_\tau)}] \times (s_\tau - r_\tau) + r_\tau =$$

$$= z_{\tau - m\left[\frac{\tau-1}{m}\right]} + [\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} (g_{\xi - m\left[\frac{\xi-1}{m}\right]} - z_{\xi - m\left[\frac{\xi-1}{m}\right]})}] - -[\frac{N}{\prod_{\xi=\tau+1}^{V_{\text{form}}} (g_{\xi - m\left[\frac{\xi-1}{m}\right]} - z_{\xi - m\left[\frac{\xi-1}{m}\right]}) \times (g_{\tau - m\left[\frac{\tau-1}{m}\right]} - z_{\tau - m\left[\frac{\tau-1}{m}\right]})}] \times$$

$$(g_{\tau - m\left[\frac{\tau-1}{m}\right]} - z_{\tau - m\left[\frac{\tau-1}{m}\right]}).$$

Stage 5. Restoration of a segment of the original image is carried out on the basis of vector transformation $A^{(\gamma;\chi)} = \left\{a_\tau^{(\gamma;\chi)}\right\}$ into a two-dimensional form based on formulas (4)–(6).

Stage 6. Merging the reconstructed segments $A^{(\gamma;\chi)}$ into the image $A = A$.

The results of evaluating the quality of compression of images of different degrees of saturation for the developed in [43, 44], the method of cryptocompression coding of images in a differentiated basis based on deterministic and non-deterministic code formation are shown in Fig. 2. The comparison was carried out with the most commonly used image compression technologies without loss of information quality, which are implemented in the TIFF and PNG data presentation formats, which implement various combinations of RLE series length coding algorithms, LZ77 sliding window code, and LZW and Huffman prefix codes.

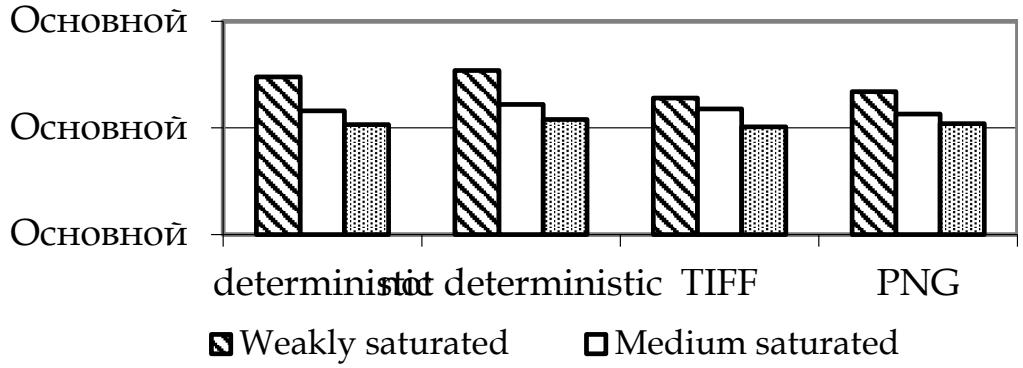

Figure 2: Results of evaluating the quality of image compression

From the analysis of the data in Fig. 6 that the best result in terms of the degree of image compression was shown by the method of cryptocompression coding of images on a differentiated basis based on non-deterministic code generation when processing video data of different degrees of saturation. The average value of the compression ratio for it is at the level of 1.08 for highly saturated images, 1.22 for moderately saturated, and 1.54 for weakly saturated images. This is on average 4–5.2% better compared to the deterministic approach, 3–20% better than the TIFF data format, and 4 * 15% better than the PNG format. Although the use of additional overhead in the method of cryptocompression image coding on a differential basis can reduce the gain by 2–3% in relation to the presentation of data in TIFF and PNG formats.

Formation of code structures of non-deterministic length:

- From the standpoint of ensuring confidentiality—provides uncertainty in the positioning of uneven codegrams in the general code stream, which eliminates the possibility of their unauthorized decryption.

- From the standpoint of ensuring accessibility—provides a decrease in the volume of cryptocompression representation of images relative to the original video data on average from 1.08 to 1.54 times, depending on the degree of their saturation.

3. Conclusion

Methods for decoding information components of cryptocompression representation of images generated on the basis of floating coding schemes have been developed, namely:

- Floating coding scheme based on the upper bounds.
- Floating coding scheme in a differential basis.

There are six main steps in decoding methods:

1. Restoration of service components of cryptocompression codegrams presented in encrypted form;
2. Determining the number of elements that will be reconstructed from the corresponding information code;
3. The selection of the information code from the general code stream of the information component;
4. Decoding the code of the information component of the cryptocompression representation;
5. Restoration of image segments;
6. The formation of a reconstructed image.

Methods for decompression of cryptocompression codegrams developed in this work allow:

- To reconstruct images from cryptocompression codegrams obtained on the basis of floating coding schemes. That is, the code constructions are formed on a non-deterministic number of elements of the original image and the base system. Formed non-deterministic length of code structures. Without knowing the correct base system, an attacker cannot correctly establish a correspondence between the generated codegrams and the number of elements involved in their formation, and he also cannot correctly position uneven codegrams in the general code stream. As a result, the attacker cannot decode the image correctly. Due to the additional use of uncertainty, an increase in the level of cryptographic resistance of the generated codegrams is achieved.
- To reconstruct the original images without losing their quality, that is bit by bit. The volume of cryptocompression representation of images relative to the original video data was, on average, reduced from 1.08 to 1.54 times, depending on the degree of their saturation. In the process of cryptocompression coding, in addition to ensuring information security, a decrease in the volume of the cryptocompression representation of the image is achieved, which ensures an increase in their availability.

4. References

[1] S. Ramakrishnan, et al., Cryptographic and Information Security Approaches for Images and Videos. CRC Press, 2018, doi: 10.1201/9780429435461.

[2] Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication, 197, 2001.

[3] DSTU 7624:2014: Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm. Order of the Ministry of Economic Development of Ukraine № 1484, 2014.

[4] DSTU GOST 28147:2009: Information processing system. Cryptographic protection. Cryptographic transformation algorithm GOST 28147-89, 2008.

[5] F. Dufaux, T. Ebrahimi, Toward a Secure JPEG, in: Applications of Digital Image Processing XXIX 6312, 2006, doi: 10.1117/12.686963.

[6] M. Farajallah, Chaos-based crypto and joint crypto-compression systems for images and videos, 2015. URL: https://hal.archives-ouvertes.fr/tel-01179610.

[7] T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, T. Fujino, Hierarchical image-scrambling method with scramble-level controllability for privacy protection, in: IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), 2013, pp. 1371-1374. doi: 10.1109/MWSCAS.2013.6674911.

[8] Information technology—JPEG 2000 image coding system: Secure JPEG 2000. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807, 2007.
[9] Sh. Ji, X. Tong, M. Zhang, Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator, 2012. URL: https://arxiv.org/abs/1208.0999.
[10] JPEG Privacy & Security Abstract and Executive Summary, 2015. URL: https://jpeg.org/items/ 20150910_privacy_security_summary.html.
[11] R. L. Rivest, A. Shamir, L. M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978) 120–126, doi: 10.1145/359340.359342.
[12] R. Sharma, S. Bollavarapu, Data Security using Compression and Cryptography Techniques. International Journal of Computer Applications 117(14) (2015) 15-18, doi: 10.5120/20621-3342.
[13] V. B. Vasiliev, et al., Video data compression and protection in UAV information exchange radio channels, in: Scientific and practical conference on Prospects for the development and use of complexes with unmanned aerial vehicles, 924 State Center for Unmanned Aviation of the Ministry of Defense of the Russian Federation, 2016, pp. 202–204.
[14] K. Wong, K. Tanaka, DCT based scalable scrambling method with reversible data hiding functionality, in: 4th International Symposium on Communications, Control and Signal Processing (ISCCSP), 2010, pp. 1-4, doi: 10.1109/ISCCSP.2010.5463307.
[15] L. Yuan, P. Korshunov, T. Ebrahimi, Secure JPEG Scrambling enabling Privacy in Photo Sharing, in: 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 2015, pp. 1-6, doi: 10.1109/FG.2015.7285022.
[16] K. M. Faraoun, A parallel block-based encryption schema for digital images using reversible cellular automata, Engineering Science and Technology 17 (2014) 85–94, doi: 10.1016/j.jestch.2014.04.001.
[17] S. Auer, et al., Bitstream-based JPEG Encryption in Real-time, in: International Journal of Digital Crime and Forensics (2013), doi: 10.4018/jdcf.2013070101.
[18] H. Kobayashi, H. Kiya, Bitstream-Based JPEG Image Encryption with File-Size Preserving, in: IEEE 7th Global Conference on Consumer Electronics (GCCE), 2018, pp. 1-4, doi: 10.1109/gcce.2018.8574605.
[19] K. Minemura, et al., JPEG image scrambling without expansion in bitstream size, in: 19th IEEE International Conference on Image Processing, 2012, pp. 261-264, doi: 10.1109/ICIP.2012.6466845.
[20] A. Phatak, A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. International Journal of Image, Graphics and Signal Processing 8(6) (2016) 64-71, doi: 10.5815/ijigsp.2016.06.08.
[21] Ch.-L. Tsai, Ch.-J. Chen, W.-L. Hsu, Multi-morphological image data hiding based on the application of Rubik's cubic algorithm, in: IEEE International Carnahan Conference on Security Technology (ICCST), 2012, pp. 135-139, doi: 10.1109/CCST.2012.6393548.
[22] K.-W. Wong, Image encryption using chaotic maps, Intelligent Computing Based on Chaos . 184 (2009) 333–354. doi: 10.1007/978-3-540-95972-4_16.
[23] Yu. Wu, S. Agaian, J. Noonan, Sudoku Associated Two Dimensional Bijections for Image Scrambling, in: IEEE Transactions on multimedia, 2012. URL: https://arxiv.org/abs/ 1207.5856v1.
[24] Y. Yang, et al., Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. EURASIP Journal on Information Security 2007 (2008), doi: 10.1155/2007/56365.
[25] V. Barannik, et al., Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System, in: 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET, 2020, pp. 699-702, doi: 10.1109/TCSET49122.2020.235522.
[26] V. Barannik, V. Barannik, Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones, in: 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET, 2020, pp. 775-780, doi: 10.1109/TCSET49122.2020.235540.

[27] V. Barannik, et al., Development Second and Third Phase of the Selective Frame Processing Method, in: 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 54-57, doi: 10.1109/AIACT.2019.8847897.
[28] V. Barannik, T. Belikova, P. Gurzhii, The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents, in: 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), 2019, pp. 656-661, doi: 10.1109/ATIT49449.2019.9030432.
[29] V. V. Barannik, et al., The technology of the video stream intensity controlling based on the bit-planes recombination, in: 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 2018, pp. 25-28, doi: 10.1109/IDAACS-SWS.2018.8525560.
[30] V. V. Barannik, Yu. N. Ryabukha, O. S. Kulitsa, The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems, Telecommunications and Radio Engineering 76(9) (2017) 785-797, doi: 10.1615/TelecomRadEng.v76.i9.40.
[31] V. Barannik, S. Shulgin, The method of increasing accessibility of the dynamic video information resource, in: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 2016, pp. 621-623. doi: 10.1109/TCSET.2016.7452133.
[32] V. Barannik, D. Tarasenko, Method coding efficiency segments for information technology processing video, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications, 2017, pp. 551-555. doi: 10.1109/INFOCOMMST.2017.8246460.
[33] Ch.-Ch. Chen, W.-J. Wu, A secure Boolean-based multi-secret image sharing scheme, Journal of Systems and Software 92 (2014) 107-114, doi: 10.1016/j.jss.2014.01.001.
[34] T.-H. Chen, Ch.-S. Wu, Efficient multi-secret image sharing based on Boolean operation, Signal Processing 91(1) (2011) 90-97, doi: 10.1016/j.sigpro.2010.06.012.
[35] M. Deshmukh, N. Nain, M. Ahmed, An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic, in: IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 690-697, doi: 10.1109/aina.2016.56.
[36] M. Naor, A. Shamir, Visual Cryptography, in: Proceedings of the Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science 950, 1995, pp. 1-12, doi: 10.1007/bfb0053419.
[37] Ch.-N. Yang, Ch.-H. Chen, S.-R. Cai, Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and Softwar 116, 2016, pp. 22-34, doi: 10.1016/j.jss.2015.01.031.
[38] P. Korshunov, T. Ebrahimi, Using warping for privacy protection in video surveillance, in: 18th International Conference on Digital Signal Processing (DSP), 2015, pp. 1-6, doi: 10.1109/ICDSP.2013.6622791.
[39] A. N. Alimpiev, V. V. Barannik, S. A. Sidchenko, The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space, Telecommunications and Radio Engineering 76(6) (2017) 521-534, doi: 10.1615/TelecomRadEng.v76.i6.60.(2017).
[40] S.O. Sidchenko, D.V. Barannik, The method of cryptosemantic representation of an image based on a floating scheme of polyadic coding system in a differential basis, Science-baised technologies 1(33) (2017) 46-53, doi: 10.18372/2310-5461.33.11558.