International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2023 Issue 57 Volume 15 Number 4 Pages 46-53

A NOVEL DIGITAL MODEL FOR VIDEO INFORMATION NETWORK SECURITY

A.K. Lampezhev V.R. Lysenko A.A. Umyskov

Institute of Design and Technology Informatics, Russian Academy of Sciences, Moscow, Russia
abas.lampezhev@mail.ru, lysenko_ras@mail.ru, a.umyskov@list.ru

Abstract- The danger of damage to information data, even considering a whole range of measures aimed at strengthening their protection, is constantly increasing. However, video data streaming in digital format remains the most critical problem. The combination of these factors necessitates detailed estimation of all existing information and solutions related to information security. In addition, it is necessary to conduct a number of comprehensive studies to improve the level of protection against the influence of various distortions and to develop practical tools that can implement full protection of broadcast video data under the influence of various attack options in practice. This work aims to retrofit the tools of the video data protection system from possible negative impacts, and to develop tools that improve the degree of stability of the video data integrity protection system. Solutions to a whole range of essential problems related to the justification of the optimal structure of the system that organizes the video data protection, and its mathematical formalization are proposed. The outlines of promising solutions regarding the creation of the main components of protection systems that ensure the video data integrity from certain negative impact were determined. A detailed justification for the formulation of the problem of creating a promising model capable of organizing a full-fledged video data protection system is given. The scientific novelty of this research lies in the fundamentally novel model developed by the authors, which is capable of organizing the video data protection, relying on the achievements of modern steganography. Its structure includes several modules and is capable of taking on numerous configurations in accordance with the goals set, and physical conditions. The author's model can calculate the increase in the degree of reliability of the protective system from the danger posed by random and targeted distortions.

Keywords: Video Data Broadcasting, Degree of Video Data Protection, Broadcast Video Data Protection, Video Protection Model, Video Streaming Estimation.

1. INTRODUCTION

Currently, the number of works devoted to the improvement and use of intelligent video monitoring systems and analysis of streaming video data in completely different subject areas is increasing [1]. Broadcasting video data on any modern network is one of the key components of information stream for most multimedia applications. This category includes various complexes that conduct surveillance and monitoring, video telephony, systems for recording and broadcasting huge amounts of video data; individualized television broadcasting, etc. [1]. Nowadays, the majority of video systems rely on streaming video data displayed in digital format. Moreover, the popularity of this range of services is growing daily. At the same time, the interest shown in this area, and the significance of the broadcast video data, lead to an increase in possible and very real dangers. They can come from external attackers (imitation of sending any messages; distortion of their meaning, visual sending of them to some recipients and actual sending to others), and from internal ones [2]. Entire streams of video data, and some ordered chains of frames, regular frames, frame contents, the totality of which constitutes groups of frames, can act as objects that are at risk of such a danger. At the same time, the category of attacks on the information content of frames poses the greatest difficulty, because in this case it is semantic content of video data that is attacked.

To organize full-fledged protection from such a danger to video data streams broadcast on the network, a number of highly specialized information systems that ensure the necessary confidentiality (resistance to targeted or unintentional influence) of publicly available video data broadcast on the network are being created and gaining popularity [3]. Alongside with this, even considering the growing popularity of these designs, the likelihood of a targeted and, of course, negative impact on computing equipment poses a serious threat today. Moreover, the almost continuous improvement of existing technologies in this area only increases the risk of causing serious harm or deletion of data, even despite the enormous costs allocated for their protection. The combination of these factors determines the relevance of this research. Its relevance is formed by estimating comprehensively experience and practical achievements in this area, creating information data protection systems, and solving problems associated with the development of effective protective tools.

Regarding the relevance of the area under consideration, the purpose of this research is to retrofit the tools of the video data protection system from possible negative impacts, and to develop tools that improve the degree of stability of the video data integrity protection system. It is necessary to develop a solution to many questions related to the justification of the optimal model capable of organizing the video data protection and formalizing it mathematically.

2. LITERATURE REVIEW

Currently, a wide variety of techniques are presented that can provide the proper level of video data protection [4, 5]. Using these techniques, various security systems are developed and implemented directly, involving the broadcast of senders and recipients' basic data [6]. For this reason, senders and recipients may or may not coincide, and the probability of such coincidence is definitely greater than the specified one. A number of studies are also being conducted to improve basic hybrid system, which successfully combines majority of advanced techniques.

Thus, most symmetric systems can guarantee increased resistance to errors of broadcasting channels [7]. Moreover, they can provide protection from danger that comes only from external attackers. The required level of protection, from both types of attackers, is guaranteed by most asymmetric systems, although the implementation of this category of systems is highly complicated. The technology that ensures the video data integrity is capable of detecting targeted forms of distortion using a family of information characteristics of video data, or using identifiers set on the broadcasting side and then verified by the receiving side. At the same time, it is worth paying attention to "active" techniques based on content, steganography [8, 9], cryptography [10], and their combinations [11]. These techniques can guarantee the proper level of protection against targeted threats.

Techniques that effectively control video data streams have become very popular and widespread today. They represent ordered chains of operations that convert broadcast files characterized by arbitrary dimensions [12-14]. Their classification is shown in Table 1. The methodology under consideration makes it possible to assess the level of negative impact with regard to various characteristics. However, the use of convolution functions can guarantee a better level of protection for specified video segments, for example, along the borders of images. Moreover, the possibility of creating a two-level protective system opens up. Convolution functions will be located on the first level, and DWM sections, which are created using hash codes, will be located on the second level. Thus, if a targeted negative impact occurs, the noise-resistant hash code will first be distorted, after which the digital watermark will be modified.

Considering the type of transformations, and the main characteristics, we can distinguish several noise-resistant convolution functions based on special wavelet transformations [20]; based on single analysis; based on Fourier transforms [21]; based on Radon transforms [22, 23]; and using a number of statistical data in coding. The essence of the most methods for creating a contour of identifiers, and options for their broadcasting to the addressee, tested during the creation of a system that ensures information security of video data, is shown in Tables 2 and 3.

Table 1. Classification of basic techniques enabling to create special functions that can control various video data

Classes that combine convolution functions	Specifics of using convolution functions
Common convolution functions [15]	This category of functions can provide full-fledged control over video data without using text files. However, if the size of the files in question changes even slightly, this can change most of the generated hash code.
Noise-resistant convolution functions [16]	This category of features is designed to protect video data segments that may be accidentally distorted by processing. The created hash code may change insignificantly when performing permitted procedures for processing video data and significantly when exposed to a targeted negative impact.
List of convolution functions in which their hash codes can be deformed by distortions when broadcast using digital watermarks (DWM) [17-19]	These techniques are designed to protect video data segments after deformation of the main hash code. While estimating the nature of the destruction, a conclusion is made: this is a targeted negative impact, or the result of permitted operations.

Table 2. Methods for creating identifiers capable of classifying negative impacts on the network video data streaming

Method for creating an identifier	Identifier specifics
Electronic digital signatures (EDS) developed by cryptographic convolution functions [24]	Identifiers ("fragile" ones) provide message-free security. At the same time, targeted or natural insignificant changes to the created EDS identifier can lead to the collapse of the security system, and there will be no confirmation of integrity. This category of identifiers is characterized by relatively low resistance to negative impacts of a random nature. The majority of systems created using these identifiers are uncapable of assessing the video data integrity, which is necessary to organize protection against imposition of video data on an established recipient.
An option of coding that is resistant to various distortions (message, EDS) [25]	The creation and use of these techniques is necessary to increase the EDS durability. However, identification complexes with acceptable errors are of greatest interest.
A technique based on the scheme proposed by Johanson and adapted to protect video data [26]	Development of "semi-fragile" identifiers is underway. They are built on a list of single identifiers. This version of identifiers is longer, which ensures a high percentage of non-identification of the negative impact of relatively "fragile" identifiers, but with increased reliability.

Currently, protection from various negative impacts is provided by the use of techniques based on cryptographic algorithms. For example, a universal method of an EDS-based security system, which has such advantages as universality, conditional independence from the dimension of messages, a fairly high degree of security, etc. [27]. At the same time, a protection system created on the basis of this technique will be characterized by a low degree of resistance to the accidental negative impact of the protected data, and the identifiers used, since the technique itself will not satisfy such a condition as the immutability of messages and identifiers. Moreover, the EDS dimensionality does not provide the possibility of using several segments of video data due to a significant increase in network congestion. There are also several techniques increasing the EDS resistance that are created on a sequence of single hash codes; however, they cannot guarantee the proper level of resistance of any fragile identifier. The use of noise-resistant coding leads to increased congestion of the broadcasting channel, which obviously reduces the degree of protection. The EDS dimensionality does not guarantee the possible inseparability of the security system from the video data, which is a prerequisite if video data is publicly broadcast on the Internet.

Table 3. Options for broadcasting identifiers to the recipient based on video data segments

Option of identifier broadcasting to the recipient	Specifics of identifier broadcasting
Identifier outside the messages that are protected: it is broadcast using a special channel [28]	This option describes the general case of broadcasting identifiers with regard to video data protection. Its advantages include: 1) ease of implementation: an identifier, or several identifiers can be located side by side as 2 separate files; 2) complete resistance to random negative impacts on the message, therefore, when transcoding or filtering video data, this will not affect the identifier or identifiers; 3) insignificant restrictions on the identifier dimensionality. The disadvantages of this option of identifier broadcasting include several aspects. 1) A number of inconveniences associated with its storage and use. Thus, if any files are broadcast, there is a risk of losing them; in case of recoding, all service data will need to be stored separately. 2) When creating it, it is necessary to use convolution functions. This feature is provided to prevent attackers using this identifier from confirming their own video data by simply attaching this file thereto. 3) There is absolutely no secrecy. However, broadcasting and checking video data fragments requires the use of special software that employs only those identified data that are currently needed and will broadcast them together with the video fragment, or will not broadcast the entire information
Identifier inside messages that are protected: it will be broadcast inside messages. To achieve this goal, the DWM is used [29]	This technique is based on the DWM use. This option implies a number of advantages and disadvantages. The advantages include 1) protection that is transparent for clients, because the usual way of using video data is not distorted; 2) there is no additional congestion on the broadcast channel, because identifiers are embedded in current messages; this option can be implemented without using convolution functions. However, this rather complex technique is limited by the amount of information that can be embedded in the broadcast file
Combined version of identifier broadcasting [30]	This option is characterized by the fact that one segment of the identified data can be broadcast using a reliable channel, while others can simply be embedded in messages

Noteworthy, a number of effective solutions shown in Table 3 are based on the possibility of embedding an identifier along an ordered chain of the identifier DWM within the messages that are being protected, and they have demonstrated their practical effectiveness. Considering this, the prospect of ensuring the inseparability of the identifier from the video data segments that need to be protected opens up, and in addition, there is no need to additionally load broadcast channels, which increases the level of protection from any targeted negative impact.

Basic techniques that ensure the translation of identifiers using DWM algorithms rely on procedures for embedding in any frame, before it is compressed, and procedures that embed something in a frame, but after its compression. Greater efficiency is achieved by using the first technique, which allows for creation of a protection system using standard compression options. This is often done using an ordered chain (and its derivatives), which enables data to be embedded applying pulse range extension, when the ordered chain of bits prepared for embedding is refined by randomly generated pulses, and then embedded in a whole series of frame-defining frequencies. The use of this solution guarantees increased resistance of even a relatively small information chain. In this case, discontinuous cosine transforms are used, since they are quite common in high-performance hardware implementations.

It is important to note that the majority of existing techniques that provide the proper degree of video data security are aimed at solving highly specialized problems, usually determined by a specific study [31, 32]. But when considering trends in improving techniques that provide the necessary level of video data protection, attention should be paid to "soft", that is, non-cryptographic techniques.

Several methods based on "soft" assessments deserve attention. This category includes a number of shorthand methods, or those based on key features; however, they only consider empirical thresholds rather than offer a probabilistic assessment of the video data integrity. The use of probabilistic assessment opens up the prospect of a deep theoretical analysis of the probability of attacks by intruders, which is necessary mainly for building a protective system against professional attackers.

3. RESEARCH METHODS AND RESULTS

The use of a general methodology for creating a model that ensures the video data protection is shown in Figure 1. Based on the general methodology for creating the structure of a model that ensures the protection of video data, and on the results of studies performed, during which each component was estimated, we proposed a more effective model that provides the necessary level of video data protection and covers several components:

1. Providing protection for senders, and including:
- The operation of creating noise-resistant convolution functions (F)
- The operation of creating an identifier (Q)
- The operation of creating a digital watermark W_{emd}
2. Basic information about generated messages v_T
3. Broadcasting channels. This is a simulation of the encoder (C), and a simulation of the decoder (D) of video data.
4. Basic data of recipients v_D

Protective component of recipients, including:

- Noise-resistant convolution functions (*F*)
- Identifier verification (*A*)
- The operation of obtaining DWM (W_{ext})

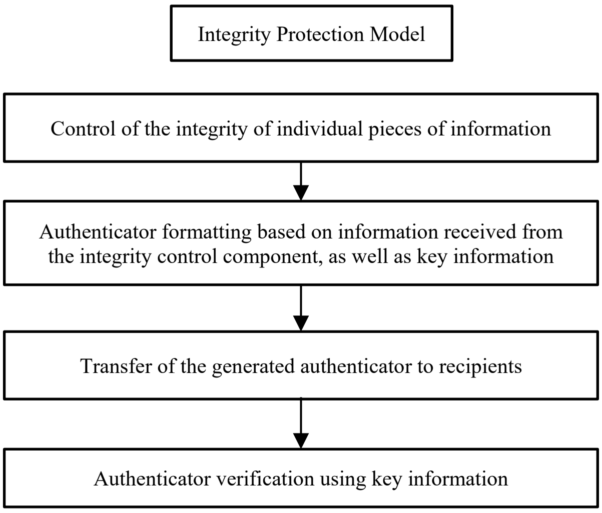
Integrity Protection Model
Control of the integrity of individual pieces of information
Authenticator formatting based on information received from the integrity control component, as well as key information
Transfer of the generated authenticator to recipients
Authenticator verification using key information

Figure 1. Appearance of the main components of the model that provides video data protection

The proposed simulation is characterized by the fact that any segment of video data *I* will pass through one of the components of the protection system. This component is calculated by noise-resistant convolution functions based on the protected segment of video data. Next, the existing hash code and the basic data of the senders are applied. At the next stage a "semi-fragile" identifier is created. This identifier of the DWM creation component will be embedded in the segment that is under protection. From a mathematical viewpoint, this operation can be described by the relation:

$$I'_w = W_{emd}(I, Q(F(I,q), h, v_T), w) \quad (1)$$

where, I'_w is a segment of video data on which a DWM record is superimposed, W_{emd} is a simulation of the process of DMW creation, *Q* is a model for creating an identifier for each single identifier, *F* is noise-resistant convolution functions, *h* is the working lengths of "semi-fragile" identifiers in individual identifiers, *q* is a vector of characteristics of noise-resistant convolution functions. This vector of characteristics also covers all values *h*, at the same time *w* is the vector of characteristics of the simulated DWM. In addition, this vector of characteristics covers all values *h*, and v_T displays basic data of senders.

Upon completion of the identifier embedding, the segment is compressed:

$$I'_{cw} = C(I'_w) \quad (2)$$

where, I'_{cw} is a compressed video segment directed into the stream. After this, the protected video segment is transmitted to the broadcast channel. The receiving side performs reverse decompression:

$$I'_{pw} = D(I'_{cw}) \quad (3)$$

where, I'_{pw} is a "decompressed" simulation of a video data decoder, marked *D*, which data define the protected video segment. Then verification of the video segment of the recipient's protective component is used. Next, the received identifier is verified using the basic data of the recipient and the calculated hash code. Then comes the decision-making phase regarding whether the sent chain has passed verification, guided by the threshold rule. Here, the possibilities of not detecting a targeted negative effect, and a certain probabilistic threshold are compared. The current operation can be expressed by the relation:

$$U(A(W_{ext}(I'_{pw}, w, h), F(q, I'_{pw}), v_R), h) \le P_{\max} \quad (4)$$

where, *U* represents a combinatorial relationship for assessing the possibility of not detecting a targeted negative impact, *A* is a model for verifying the identifier of each single identifier using the received DWM identifier, due to the use of the delivered W_{ext} and the basic data of the recipient v_R.

To create and verify the identifiers, a technique was used based on the scheme proposed by Johanson, which is adapted to protect video data. At this stage, the creation of a "semi-fragile" identifier begins. This version of the identifier is long to ensure guaranteed non-detection of interference relative to "fragile" identifiers, but having a high degree of resistance. Its structure involves a list of single identifiers, and the possibility of not detecting a "semi-fragile" identifier can be calculated by the relation:

$$P > U(k,n) = (\sum_{v=0}^{k} C_n^v) / ((\sum_{v=0}^{k} C_n^v) + (\sum_{v=0}^{k} C_n^v)) \quad (5)$$

where, *n* is the total number of single identifiers, *k* represents the number of single identifiers that failed verification.

To create and verify one "fragile" identifier, the following relations can be applied [33]:

$$v_{T3i} = v_{R1i} \otimes v_{T1i} \times v_{R2i} \quad (6)$$

$$v_{T4i} = v_{R3i} \otimes v_{T2i} \times v_{R2i} \quad (7)$$

where, $v_{Ti} = (v_{T1i}, v_{T2i}, v_{T3i}, v_{T4i})$ are the basic data bits for creating *i*-th single "fragile" identifiers; $v_{Ri} = (v_{R1i}, v_{R2i}, v_{R3i})$ represent bits of the recipient's basic data for verifying the *i*-th "fragile" identifiers. In total, considering the combinations of basic data of senders and recipients, it is possible to create 16 lists for which the given ratios will be correct. Therefore, this formula of lists of basic data bits does not allow recipients to realize the optimal identifier, and senders not to receive the created identifier; therefore, this technique is able to provide a protection system against all types of adverse impacts.

By conducting several transformations and taking x_i, *i* is bit of noise-resistant hash code created by the convolution functions, two-bit *i–e* identifiers can be expressed as [30]:

$$\alpha = V_{T1} \otimes X \times V_{T2} \quad (8)$$

$$\beta = V_{T3} \otimes X \times V_{T4} \quad (9)$$

Each video data segment will be created by single *h* "fragile" identifiers.

For verification purposes, the recipient of the received *i–x* "fragile" identifiers will perform the following transformation [30]:

$$\overline{\beta} = V_{R1} \otimes \alpha \times V_{R2} = \otimes X' \times V_{R3} \quad (10)$$

It is that Integrity is obviously preserved, and the probability of this is determined by 0.5 when $\beta = \overline{\beta}$. Using the combinatorial Equation (10) to verify the "semi-fragile" identifier, and relying on this technique, we obtain an estimation of the non-detection of negative impacts generalized for a segment of video data.

It turns out that by using noise-resistant convolution functions, and the technique of creating "semi-fragile" identifiers and considering the scheme proposed by Johanson, it is possible to create an identifier for each video data segment. A segment will be considered verified when the possibility of undetectability is below a certain threshold value $P_{\max}$.

A visual representation of the proposed model is shown in Figure 2.

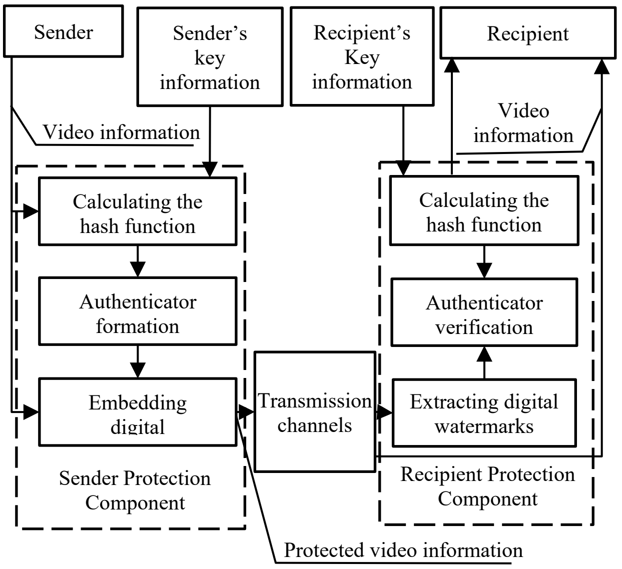
Sender
Sender's key information
Recipient's Key information
Recipient
Video information
Video information
Calculating the hash function
Authenticator formation
Embedding digital
Sender Protection Component
Transmission channels
Calculating the hash function
Authenticator verification
Extracting digital watermarks
Recipient Protection Component
Protected video information

Figure 2. External view of a simulation providing video data protection.

The advantages of the proposed model are flexibility, easy adaptation of components to solve the specific task of protecting the integrity of video information, ease of use and small size of the video information protection unit. Unlike existing ones, the proposed model combines "semi-fragile" identifiers, and a number of the identified data insuperabilities from the protected information chain through the use of DWM algorithms.

4. DISCUSSION

Summarizing the research results, it is worth mentioning that we proposed a novel model that ensures the video data protection. In this work, identifier inside messages was used, with the built-in DWM. The advantages of this structure are:

1. The presence of protection is "transparent" to the user, that is, the usual way of using video information is not disrupted.
2. Since authenticators are built directly into the message, there is no additional load on the transmission channel.
3. If the frame is significantly distorted or replaced, distortions can be detected without resorting to the use of a hash function.

But the use of this structure has some limitations:

1. Strict restrictions on the permissible amount of embedded information.
2. Difficult to embed.
3. Some bits may be destroyed due to compression that is lossy beyond acceptable limits.

Differing from existing methods, where authentication for protection is built on the EDS basis [27], the capabilities of the proposed model make it possible to successfully combine a number of DWM technologies, noise-resistant hashing of video data and techniques for creating Johanson's scheme-based "semi-fragile" identifiers. This solution provides the possibility to create full-fledged video data protection, characterized by high resistance, even when the main indicators of video data change, and to ensure protection from various threats.

Figure 3 shows, that the proposed protection model has much greater stability according to the given criterion.

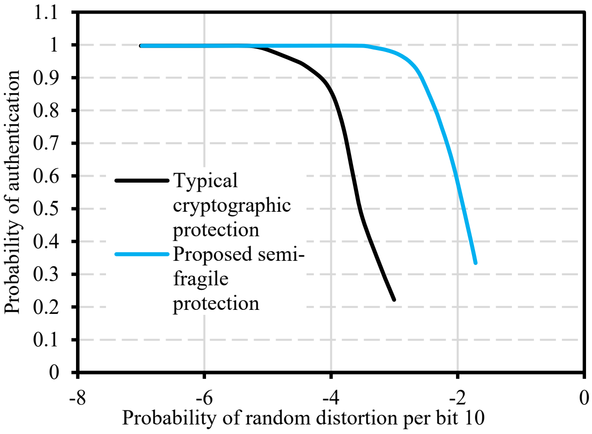

Figure 3. Results of a study assessing the likelihood of identifying a negative impact

5. CONCLUSION

Video data are characterized by high redundancy, and easy change of real display. The use of all available techniques that provide complete protection of information data from a possible attack often does not guarantee the degree of flexibility required by users, and high security from possible attacks by intruders. The result of this research is the development of a new solution to a number of complex scientific and technical tasks aimed at increasing the stability of the system that protects video data by developing a novel model of video information integrity.

The research results include:

1. Analysis of threats from video information attackers. To confirm the adequacy of the threat model, some of the existing forensic integrity verification methods were reviewed.
2. An analysis of the EDS noise immunity revealed that this class of protection is not applicable for use in steganographic systems.
3. The study of the main existing approaches to protecting video information from integrity threats identified the main directions and trends.

4. The study of the existing DWM algorithms for video information enabled to select one of the possible algorithms for embedding DWM into video information.
5. A model for protecting the video information integrity using steganography was proposed. This model is modular in nature and can be configured depending on the specific task and real constraints and requirements.

The model has the following advantages compared to analogues:
1. Independence to the codec used, since protection is installed on video fragments before compression, and the embedding algorithm can be selected depending on the codec.
2. Resistance to re-coding both into the same format and into another.
3. The key information of security formation and verification are different, which broadens the scope of application.
4. Using a Johanson's scheme-based method to generate an authenticator made it possible to increase noise immunity to equally probable errors by almost two orders of magnitude.
5. Since steganography technologies were used, the problem of additional load on the communication channel was solved.

The practical use of the proposed model opens up the prospect of increasing the protection resistance against random targeted and negative impacts. As a recommendation, we propose using the developed model to generate key information for senders and recipients of video information.

ACKNOWLEDGEMENTS

The work was carried out at the Federal State Autonomous Scientific Institution Institute for Design-Technological Informatics RAS with the financial support under project No. 075-11-2022-029 dated 04/08/2022 between STREAM LABS LLC and the Ministry of Science and Higher Education of the Russian.

REFERENCES

[1] D. Gura, I. Markovskii, N. Khusht, I. Rak, S. Pshidatok, "A Complex for Monitoring Transport Infrastructure Facilities Based on Video Surveillance Cameras and Laser Scanners", Transportation Research Procedia, Vol. 54, pp. 775-782, 2021.

[2] R. Hasan, R. Hasan, "Threat Model and Security Analysis of Video Conferencing Systems as a Communication Paradigm During the COVID-19 Pandemic", Novel AI and Data Science Advancements for Sustainability in the Era of COVID-19, pp. 181-199, 2022.

[3] N. John, M. Wellmann, "Data Security Management and Data Protection for Video Conferencing Software", International Cybersecurity Law Review, Vol. 1, No. 1-2, pp. 39-50, 2020.

[4] F.H.M Sediq Al Kadei, "Robust Video Data Security Using Hybrid Cryptography-Steganography Technique", Periodicals of Engineering and Natural Sciences (PEN), Vol. 8, pp. 1741-1751, 2020.

[5] Y. Liu, L. Wang, A. Qouneh, X. Fu, "Enabling PIM-Based AES Encryption for Online Video Streaming", Journal of Systems Architecture, Vol. 132, p. 102734, 2022.

[6] J.Y. Yu, Y. Kim, Y.G. Kim, "Intelligent Video Data Security: A Survey and Open Challenges", IEEE Access, Vol. 9, pp. 26948-26967, 2021.

[7] B. Umapathy, G. Kalpana, "A Novel Symmetric Cryptographic Method to Design Block Complexity for Data Security", Computers and Electrical Engineering, Vol. 104, p. 108467, 2022.

[8] A. Fatnassi, H. Gharsellaoui, S. Bouamama, "Towards Novel Video Steganography Approach for Information Security", Procedia Computer Science, Vol. 159, pp. 953-962, 2019.

[9] M. Yousefi Valandar, P. Ayubi, M. Jafari Barani, B. Yosefnezhad Irani, "A Chaotic Video Steganography Technique for Carrying Different Types of Secret Messages", Journal of Information Security and Applications, Vol. 66, p. 103160, 2022.

[10] S. Kumar, M. Kumar, R. Budhiraja, M.K. Das, S. Singh, "A Cryptographic Model for Better Information Security", Journal of Information Security and Applications, Vol. 43, pp. 123-138, 2018.

[11] S. Gadde, J. Amutharaj, S. Usha, "A Security Model to Protect the Isolation of Medical Data in the Cloud Using Hybrid Cryptography", Journal of Information Security and Applications, Vol. 73, p. 103412, 2023.

[12] Z. Chkirbene, R. Hamila, A. Erbad, S. Kiranyaz, N. Al Emadi, "D2DLive: Iterative Live Video Streaming Algorithm for D2D Networks", Computer Networks, Vol. 229, p. 109734, 2023.

[13] D. Ghosh, M. Pandey, C. Gautam, A. Vidyarthi, R. Sharma, D. Draheim, "Utilizing Continuous Time Markov Chain for Analyzing Video-on-Demand Streaming in Multimedia Systems", Expert Systems with Applications, Vol. 223, p. 119857, 2023.

[14] X. Li, M. Darwich, M.A. Salehi, M. Bayoumi, "A Survey on Cloud-Based Video Streaming Services", Advances in Computers, Vol. 123, pp 193-244, 2021.

[15] W.N. Lie, S.T. Chiu, Y.K. Chen, J.C. Chiang, "Semi-Automatic 2D-to-3D Video Conversion Based on Background Sprite Generation", Journal of Visual Communication and Image Representation, Vol. 70, p. 102801, 2020.

[16] X. Cheng, J. Zhou, X. Zhao, H. Wang, Y. Li, "A Presentation Attack Detection Network Based on Dynamic Convolution and Multi-Level Feature Fusion with Security and Reliability", Future Generation Computer Systems, Vol. 146, pp. 114-121, 2023.

[17] L. Velazquez Garcia, A. Cedillo Hernandez, M. Cedillo Hernandez, M. Nakano Miyatake, H. Perez Meana, "Imperceptible Visible Watermarking for Copyright Protection of Digital Videos Based on Temporal Codes", Signal Processing: Image Communication, Vol. 102, p. 116593, 2022.

[18] A. Zotin, M. Favorskaya, A. Proskurin, A. Pakhirka, "Study of Digital Textual Watermarking Distortions under Internet Attacks in High Resolution Videos", Procedia Computer Science, Vol. 176, pp. 1633-1642, 2020.

[19] H. Agarwal, F. Husain, "Development of Payload Capacity Enhanced Robust Video Watermarking Scheme Based on Symmetry of Circle Using Lifting Wavelet Transform and SURF", Journal of Information Security and Applications, Vol. 59, p. 102846, 2021.
[20] S.D. Mali, L. Agilandeeswari, "Non-Redundant Shift-Invariant Complex Wavelet Transform and Fractional Gorilla Troops Optimization-Based Deep Convolutional Neural Network for Video Watermarking", Journal of King Saud University, Computer and Information Sciences, Vol. 35, No. 8, p. 101688, 2023.
[21] C. Barajas Solano, J.M. Ramirez, J.I.M. Torre, H. Arguello, "Compressive Spectral Video Sensing using the Convolutional Sparse Coding framework CSC4D", Journal of Visual Communication and Image Representation, Vol. 92, p. 103782, 2023.
[22] A. Sasithradevi, S.M.M. Roomi, "Video Classification and Retrieval Through Spatio-Temporal Radon Features", Pattern Recognition, Vol. 99, p. 107099, 2020.
[23] H. Pan, L. Xie, Z. Wang, "C3DBed: Facial Micro-Expression Recognition with Three-Dimensional Convolutional Neural Network Embedding in Transformer Model", Engineering Applications of Artificial Intelligence, Vol. 123, p. 106258, 2023.
[24] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, M. Yousaf, "Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey", Computer Science Review, Vol. 47, p. 100530, 2023.
[25] N. Sahu, A. Sur, "SIFT Based Video Watermarking Resistant to Temporal Scaling", Journal of Visual Communication and Image Representation, Vol. 45, pp. 77-86, 2017.
[26] J.R. Padilla Lopez, A.A. Chaaraoui, F. Florez Revuelta, "Visual Privacy Protection Methods: A Survey", Expert Systems with Applications, Vol. 42, No. 9, pp. 4177-4195, 2015.
[27] A. Kuznetsov, A. Pushkar'ov, N. Kiyan, T. Kuznetsova, "Code-Based Electronic Digital Signature", The IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 331-336, Kiev, Ukraine, 24-27 May 2018.
[28] K.A. Saadi, A. Bouridane, A. Guessoum, "Combined Fragile Watermark and Digital Signature for H. 264/AVC Video Authentication", The 17th European Signal Processing Conference, pp. 1799-1803, Glasgow, Scotland, 24-28 August 2009.
[29] M. Hefeeda, K. Mokhtarian, "Authentication Schemes for Multimedia Streams", ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 6, No. 1, pp. 1-24, 2010.
[30] G. Oligeri, S. Chessa, R.D. Pietro, G. Giunta, "Robust and Efficient Authentication of Video Stream Broadcasting", ACM Transactions on Information and System Security, Vol. 14, No. 1, pp. 1-25, 2011.
[31] V. Kuklin, I. Alexandrov, D. Polezhaev, A. Tatarkanov, "Prospects for Developing Digital Telecommunication Complexes for Storing and Analyzing Media Data", Bulletin of Electrical Engineering and Informatics, Vol. 12, No. 3, pp. 1536-1549, 2023.
[32] G.S. Lebedev, E.Y. Linskaya, V.Y. Terekhov, A.A. Tatarkanov, "Monitoring and Quality Control of Telemedical Services via the Identification of Artifacts in Video Footage", International Journal of Intelligent Systems and Applications in Engineering, Vol. 11, No. 2, pp. 82-92, 2023.
[33] T. Johansson, "On the Construction of Perfect Authentication Codes that Permit Arbitration", In Advances in Cryptology, CRYPTO' 93, Lecture Notes in Computer Science, Springer, Vol. 773, pp. 343-354, Heidelberg, Berlin, Germany, 1993.

BIOGRAPHIES

Name: **Abas**
Middle Name: **Khasanovich**
Surname: **Lampezhev**
Birthday: 07.07.1997
Birthplace: Murmansk, Russia
Bachelor: Navigation and Ballistic Support for Use of Space Technology, Department of Dynamics and Flight Control of Rockets and Spacecraft, Faculty of Special Mechanical Engineering, Bauman Moscow State Technical University, Moscow, Russia, 2016
Master: Navigation and Ballistic Support for Use of Space Technology, Department of Dynamics and Flight Control of Rockets and Spacecraft, Faculty of Special Mechanical Engineering, Bauman Moscow State Technical University, Moscow, Russia, 2020
The Last Scientific Position: Researcher, Institute of Design and Technology Informatics, Russian Academy of Sciences, Moscow, Russia, Since 2020
Research Interests: Multi-Parameter Optimization and Mathematical Modeling, Multi-Parameter Optimization and Mathematical Modeling
Scientific Publications: 14 Papers, 2 Patents, 2 Theses

Name: **Viktor**
Middle Name: **Romanovich**
Surname: **Lysenko**
Birthday: 16.12.1989
Birthplace: Nalchik, Russia
Master: Engineering FIeld, Design, Production and Operation of Rockets and Rocket-Space Complexes, Department of Spacecraft and Launch Vehicles, Faculty of Special Mechanical Engineering, Bauman Moscow State Technical University, Moscow, Russia, Since 2015
The Last Scientific Position: Junior Researcher, Institute of Design and Technology Informatics, Russian Academy of Sciences, Moscow, Russia, Since 2022
Research Interests: Simulation Modeling, Chess Analysis, Process Optimization and Automation
Scientific Publications: 1 Paper, 2 Theses

Name: **Alexander**
Middle Name: **Alexandrovich**
Surname: **Umyskov**
Birthday: 25.10.1982
Birthplace: Saransk, Russia
Master: Engineering Field, Fundamental Computer Science and Information Technology, Department of Fundamental Informatics, Faculty of Mathematics and Information Technologies, Mordovian State University, Saransk, Russia, 2005
The Last Scientific Position: Junior Researcher, Institute of Design and Technology Informatics, Russian Academy of Sciences, Moscow, Russia, Since 2021
Research Interests: System Programming, Data Analysis, Statistics, Neural Networks
Scientific Publications: 2 Papers, 1 Thesis