УДК 004.056.5

I. Bobok, A. Kobozeva, M. Maksymov, O. Maksymova

Odessa National Polytechnic University, Odessa, Ukraine

Checking the integrity of CCTV footage in real time at nuclear facilities

Video surveillance has become an important constituent part of the integrated security system of nuclear power plants. Due to this, the integrity and authenticity of the video transmitted by the surveillance camera are extremely important, and so is the possibility to identify violations of these categories of information in real time.

The authors propose a new method to detect one way of violating the integrity of the video sequence — "camera loop" hijacking. The proposed method based on identifying the perturbation in matrix of the current frame of the original video sequence in transition to the next frame ensures the efficiency of the method that is not dependent on the specifics and characteristics of the analyzed video sequence. The high efficiency of the method is confirmed by results of a computational experiment, under which type I and type II errors were not found. The practical value of the proposed method is the possibility of its work in real time because it is a polynomial of degree 1, as well as the simplicity and multiplatform implementation.

Keywords: integrated security system, video surveillance, video sequence, camera loop.

І. І. Бобок, А. А. Кобозєва, М. В. Максимов, О. Б. Максимова

Перевірка цілісності записів камер відеоспостереження в режимі реального часу на об'єктах атомної енергетики

За останні роки відеоспостереження стало невід'ємною складовою частиною комплексної системи безпеки атомних електростанцій. Тому надзвичайно важливими є цілісність і автентичність відеоінформації, переданої камерою відеоспостереження, а також можливість встановлення порушень згаданих категорій інформації в режимі реального часу.

У роботі пропонується метод виявлення одного з порушень цілісності відеопослідовності — заставки. Принцип, покладений в основу методу (виявлення збурень матриці поточного кадру оригінальної відеопослідовності під час переходу до подальшого кадру), дає змогу забезпечити незалежність ефективності методу від специфіки отримання та характеристик аналізованої відеопослідовності. Висока ефективність методу підтверджена результатами обчислювального експерименту, в умовах якого помилки першого і другого роду не виявлено. Практична цінність методу полягає в можливості організації його роботи в режимі реального часу, оскільки він є поліноміальним ступеня 1, а також у простоті й мультіплатформенності реалізації.

Ключові слова: комплексна система безпеки, відеоспостереження, відеопослідовність, порушення цілісності, заставка.

Modern digital technologies, which are applied in the development of automated control systems of technological processes, computer networks, security systems, etc., play an important role in the operation of nuclear power plants. These technologies transmit information from the station level to the power grid management level and back, implement the operational management of the current regime by operators, track changes in the state of an object in real time, etc. It should be noted that the use of the above-mentioned technologies, many of which are vulnerable to cyber attacks, at installations with limited access requires special attention to the issue of integrated security [1, 2].

This paper considers one element of the integrated security system — CCTV system.

Early Basic Research Efforts and Publications. Today, CCTV has become an essential part of the integrated security system at limited access facilities (banks, administrative institutions, scientific laboratories, nuclear power plants), because the modern equipment allows not only monitoring and control of various components of the object in real time and video recording, but also program response from the entire security system upon alarm signals. In view of this, camera-generated video sequence may be the subject of falsification by the attackers, whose aim is the unauthorized entry to a secure object.

The falsifications of the video sequences from surveillance cameras can occur in various ways [3]. First of all, it depends on where the camera (indoor/outdoor) is placed and where its stationary position is. So, if the location of a stationary camera is indoors, access to which is limited, an attacker can involve hijacking video streams and seamlessly replace them with static image which repeats over and over again; it is called "camera loop" [4].

The Aim of Research is to develop a method for detection of the "camera loop" hijacking in video sequences from surveillance cameras in real time.

Description of Research. In view of the fact that the use of the "camera loop" hijacking is limited in time (often small) interval t, it is extremely difficult to visually notice the result because the dynamics of scene changes in the premises where movement is very small. However, in a real room this dynamics should take place, which is associated with (albeit minor) heat and mass transfer, brightness, humidity, etc., which leads to movement of air masses. Modern video cameras are very sensitive to the most minor changes of scene, invisible to the human eye. These changes can be registered as perturbation of brightness matrix elements of consecutive frames of video sequences.

To confirm the hypothesis, numerical experiments were conducted. During the experiments, various cameras were installed in the inaccessible premises and made 24th-shooting of all scenes. Moreover, the presence of natural and artificial light sources in the room changed with different (stationary) position of the camera geometrically and toward the light source. The arbitrary video sequence is a sequence of frames, each of which can be seen as a stationary digital image. The formal representation of such images is one, three, four two-dimensional matrices depending on color or monochrome image, storage schema, etc. [3]. The changes of scene in terms of developments can be seen as changes of element values of matrices, corresponding to successive frames.

During the experiment, the first 100 frames from each analyzed video sequence were thrown out, and then sequence of 200 frames was processed. For each pair of consecutive frames, $n \times m$-matrices of which are denoted as $\mathbf{F}$ and $\overline{\mathbf{F}}$ with

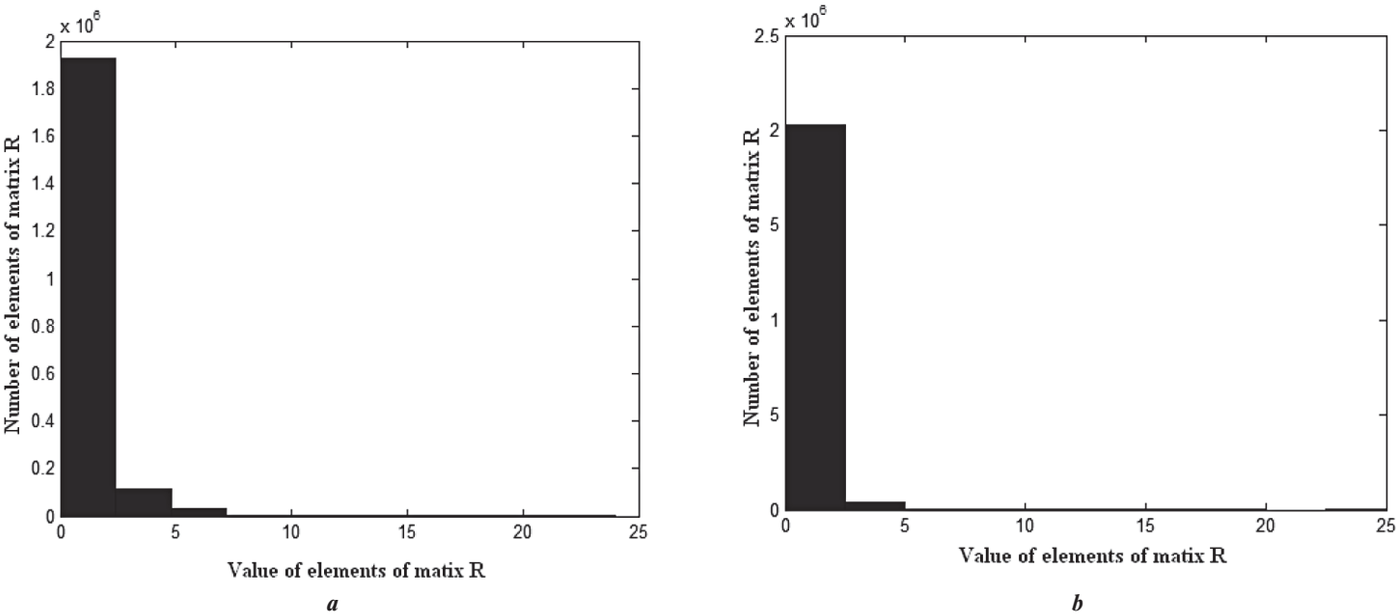


Fig. 1. The typical form of histogram of the values of the elements of matrix **R** for two consecutive frames of the original video sequence: *a* — without natural light source; *b* — with natural light source

elements $f_{ij}, \overline{f}_{ij}$, $i = \overline{1,n}, j = \overline{1,m}$, respectively, we determine the $n \times m$-matrix of absolute difference $\mathbf{R} = \text{abs}\left(\mathbf{F} - \overline{\mathbf{F}}\right)$ with elements

$$r_{ij} = \left| f_{ij} - \overline{f}_{ij} \right|, \; i = \overline{1,n}, \; j = \overline{1,m} \; .$$

We founded that for each pair of consecutive frames from each of the original video sequences, there are elements of the matrix **R** different from 0, i.e. for each pair of consecutive frames:

$$\mathbf{F} \neq \overline{\mathbf{F}} \; .$$

Moreover, such elements constitute from 8 to 21 % of the total. Detailed experimental results for some of the examined video sequences are presented in Table 1. The results are given for the red color component of the matrix representation of the frame (RGB system); those for the other two color components are comparable to the presented results.

On average, for each pair of consecutive frames, brightness of nine percent pixels is changed by more than one scale. A typical pattern is shown in Fig. 1.

The chart corresponds to the original video sequence that fully confirms the proposed hypothesis. For the "camera loop", there are no changes from frame to frame, which would allow distinguishing it from the original video and identifying unauthorized actions of the attacker.

Taking into account the potential large size of analyzed frames and the need for fundamental possibility of analyzing in real-time, it is possible to analyze not entire frame, but only part of it. To do this, we must set the allowable size of the part of the frame, the analysis of which would be informative in terms of detecting "camera loop" hijacking, i.e. the portion sizes, which will obligatory contain disturbed pixels (for the frame sequence number of such pixels may be less than 5 % (Table 1) and their arrangement within a frame in the general case is unknown).

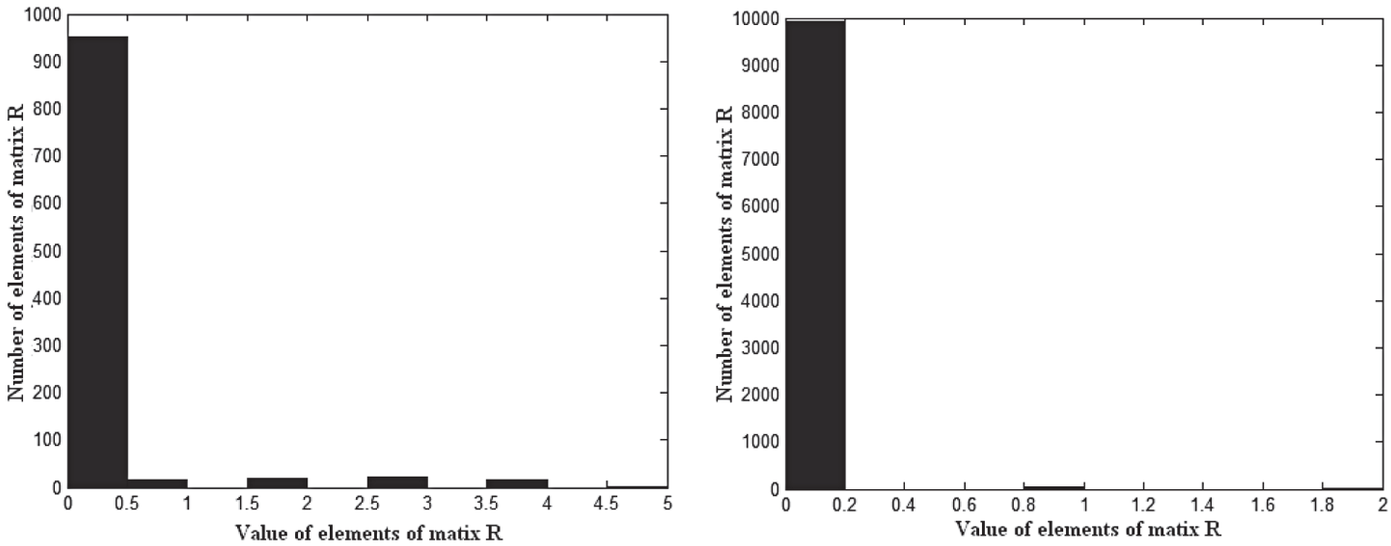
Table 1. Results of the computational experiment for original video sequences made by stationary camera

VS	Arithmetical mean of the number of non-zero elements of matrix R by frames of video sequence, %	Arithmetical mean for maximal value of elements of matrix R by frames of video sequence	Arithmetical mean of the number of non-zero elements of matrix R greater than one, %
V_1	81	31	10
V_2	82	33	11
V_3	81	27	10
V_4	84	27	9
V_5	90	33	5
V_6	90	24	5
V_7	90	25	4
V_8	89	32	5
V_9	87	36	8
V_{10}	83	37	10

As a result of computing experiment, it was determined that for video sequence corresponding to scene with natural light source it is sufficient to consider the frame's sub-domains of size 100×100 pixels (such sub-domains necessarily contain (single) disturbed pixels) (Fig. 2, *b*), and without natural light source — 32×32 pixels (Fig. 2, *a*).

To reduce the analysis time of the video sequence (to allow the execution in real time) we propose to conduct a comparison of pairs of the non-consecutive frames, but frames taken with certain time period *T*. It is necessary that

$$T < t. \qquad (1)$$



a *b*

Fig. 2. The typical form of histogram of the values of the elements of matrix **R** for subdomains of two consecutive frames of the original video sequence: *a* — without natural light source size of subdomain is 32×32 pixels; *b* — with natural light source (size of subdomain is 100×100 pixels)

Using the non-consecutive frames will reduce analysis time due to:

- the reduction in the number of analyzed pairs of frames;
- the fact that differences in non-consecutive frames of the original video sequences will be in more pixels than in consecutive frames; it will also reduce the sizes of the analyzed subdomains of frames.

In view of the presented results, algorithm of detecting the presence of the "camera loop" in the video sequence from surveillance camera in real time is as follows.

Let's V is analyzed video sequence, where $V^{(1)}$, $V^{(2)}$, ..., $V^{(k)}$ are frames; r is frame rate; T is a period between two analyzed frames and is measured in seconds.

Step 1 (Initialization). $p = p_0$ (p_0 — number of first analyzed frame from V).

Step 2. For $V^{(p)}$ and $V^{(p+rT)}$ we extract the analyzed subdomains of size $l \times l$: $\mathbf{F}^{(l)}$ and $\overline{\mathbf{F}}^{(l)}$ in an arbitrary color component (RGB system) (or brightness matrix (YUV [5])).

Step 3. Forming the $l \times l$-matrix $\mathbf{R} = \mathrm{abs}\left(\mathbf{F}^{(l)} - \overline{\mathbf{F}}^{(l)}\right)$.

Step 4. For matrix **R** elements:

If $r_{ij} = 0$ for $\forall i, j = \overline{1, l}$,
then "Camera Loop" detected, EXIT;
else
if $p + 2rT \le k$
then $p = p + rT$, go to Step 2
else EXIT.

Remark. For processing the pair of frames of the video sequence, the number of operations does not depend on the size of the frame's matrix, the total number of frames, i.e. it is a constant. In view of this, the maximum computational complexity of the algorithm in the processing of frames $V^{(1)}$, $V^{(2)}$, ..., $V^{(k)}$ (in the case of processing two successive frames, i.e. $rT = 1$) would be defined as

$$\underline{O}(k), \tag{2}$$

which makes it possible to use it in real time.

Discussion. Underlying the principle of the proposed method based on identifying the perturbation of matrix of the frame of the original video sequence in the transition to the next frame, ensures the independence of the efficiency of the method on the specifics of obtaining and characteristics of the analyzed video sequence.

To test the effectiveness of the developed method and algorithmic implementations for different values of the parameters numerical experiments were conducted in MATLAB 7.4.0.287 (License number: 21808. Platform: All. License option: Group Term: Perpetual. Use: Classroom) on a 2.7 GHz Intel Core i5 processor. There were 300 original video sequences (MPEG-4 codec, MOV container), each of which was from 90 to 900 seconds recorded by multiple cameras, namely Olympus SP-820 — 1/2,3" CMOS, 14MP; Nikon COOLPIX P100 — 1/2,3" CMOS, 10,3MP; Canon PowerShot A520 — 1/2,5" CCD, 4MP. It should also be pointed out that characteristics of cameras used in experiments similar to cameras used in production facilities including at nuclear facilities, for example, Rolls-Royce CDS 5000 [6], or ECA Group DTR 65 HRC [7]. Shooting was made at different times of the day, in presence/absence of natural/artificial light sources (Table 2 — here, the last column shows the designation of the video sequence belonging to this category, which is used below); herewith frames obtained by cameras are represented as images with different resolution (from 320×240 to 1920×1080), contrast, brightness, with/without fine details.

The proposed method is actually a binary classifier therefore the effectiveness of the algorithmic implementation of the method was evaluated using the Type I ("camera loop" is not detected) and Type II ("camera loop" is false detected) errors.

Type I and Type II errors were defined by a standard way [8], namely, the frequency of occurrence of the relevant events in the experiments, taking into account that with an increase in number of trials (in our case — the number of analyzed video sequences) the frequency of the event loses its random nature, tends to stabilize, and approach to some average

constant value (in accordance with Bernoulli's theorem), which is the probability of the event. It is only necessary to note that this "approach" has a feature: with increasing number of trials n the frequency of event u_n converges to its probability p, i.e. for any $\varepsilon > 0$ with increasing n the probability of the following inequality

$$|u_n - p| < \varepsilon$$

tends to 1 [9]. Thus, with increasing number of trials n the frequency approaches to the probability without absolute certainty, but with the probability that with large number of trials can be considered as the practical certainty [9]; that was used for estimating of Type I and Type II errors.

Table 2. The distribution of 300 original video sequences used during the numerical experiment into different categories

Number of video sequences that made in the presence of natural light (without artificial light source)	Time 6^{00} — 12^{00}	25	V_{11}
	Time 12^{00} — 17^{00}	25	V_{12}
	Time 17^{00} — 24^{00}	25	V_{13}
Number of video sequences that made in the presence of natural light (with artificial light source)	Time 6^{00} — 12^{00}	25	V_{21}
	Time 12^{00} — 17^{00}	25	V_{22}
	Time 17^{00} — 24^{00}	25	V_{23}
Number of video sequences that made without natural light source (with artificial light source)	150		V_{31}

The theoretical possibility of Type I errors can be only in one case — if the condition (1) is false; in any other case Type I errors are impossible. If the preliminary assessment of the time t of the attacker's possible actions is not available, the best in order to avoid a possible "camera loop" hijacking skip during the video sequence analysis is to consider the pairs of consecutive frames, i.e. $T = \frac{1}{r}$ guarantees the absence of errors of Type I errors.

Type II errors [8] are fundamentally possible in the case where the sizes $l \times l$ of the analyzed subdomain of the frame would be insufficient to contain guaranteed perturbed (relative to the previous frame pixels) of the subsequent analyzed frame of the original video sequence. Results of computational experiment where $T = \frac{1}{r}$, are given in Table 3; the conclusion of the "camera loop" in video sequences was made as soon as was found at least one pair of frames for which $l \times l$-matrix $\mathbf{R} = 0$.

The presented results in practice confirm the above theoretical conclusion that the effectiveness of this method does not depend on the specific conditions in which the received video sequence, the specifics of frames (resolution, contrast, brightness, presence/absence and size of the background areas, presence/absence of fine details) — the results for all categories are congruent. In the algorithmic implementation of the method, it makes sense to consider $l \times l$-subdomains for $l \geq 100$.

Table 3. Type II errors in the analysis of video sequences using the developed method, %

VS \ l	8	16	32	100	120
V_{11}	100	87	14	2	0
V_{12}	97	87	17	0	0
V_{13}	98	86	12	0	0
V_{21}	100	84	15	0	0
V_{22}	99	72	21	2	0
V_{23}	99	88	11	1	0
V_{31}	98	90	2	0	0

Conclusions. Securing objects with limited access, which are the modern nuclear power plants, remained unresolved task until now and requiring solutions for the integrated systems approach. Certainly, the special attention is given to the important issues relating to nuclear security and preventing interference from the outside, cooling the reactor and prevent the escape of radioactive substances outside the pressurized zone [10], while the cause of such worst-case situations may be the unauthorized actions of attackers who had access to the limited access premises and networks. Due to this, the integrity and authenticity of the video transmitted by the CCTV cameras are extremely important, as well as the possibility of establishing violations of these categories of information in real time.

In this article the authors presented a new method for detection of the "camera loop" hijacking in video sequences from surveillance cameras in real time. The high efficiency of the developed method is confirmed by the results of computational experiments — during the analysis of video sequences by comparing the $l \times l$-subdomains of the pairs of consecutive frames with $l > 100$, Type I and Type II errors were not found.

The practical value of the proposed method is as follows:

- the possibility of organizing its work in real time, as in accordance with (2) it is a polynomial of degree 1, even when processing successive frames of a video sequence;
- simplicity and multiplatform implementation.

The signal from the CCTV cameras considered by the way of attacks on the integrity is one of the most easily implemented variations of this violation. This method is not used by the attackers if camera's installation is not stationary, or the camera is outside the premise with limited access. In this case, it will be used "insert"-method [11], when the original signal V from the camera at the time t will be replaced by another video signal $\overline{V}_t$, and then the broadcast of original signal will be resumed. There are several options for generating $\overline{V}_t$, but the most interesting, difficult to recognize and most likely (given to the interest in challenging the process of establishing the real signal substitution) is a choice when $\overline{V}_t$ video sequence showing the scene similar to V and made by the same camera for which substitution is performed. Here, the problem of detecting the substitution is reduced to determine of "place of insert", because all the technical parameters of the video sequence $\overline{V}_t$ are similar to the parameters of the original video V. The results of this task solution in real-time are currently being prepared for publication by the authors.

References

1. *Song, J.-G., Lee, J.-W., Lee, C.-K.* (2012), "A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants", Nuclear Engineering and Technology, Vol. 44, No. 8, pp. 919–928.

2. *Park, J., Suh, Y.* (2014), "A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities", Nuclear Engineering and Technology, Vol. 46, No. 1, pp. 47–54.

3. *Herling, J.* (2014), "Advanced Real-Time Manipulation of Video Streams", Berlin, Springer, 244 p.

4. *Finkle, J.* (2013), "U.S. Security Expert Says Surveillance Cameras can be Hacked", Reuters, available at: http://www.reuters.com/article/2013/06/17/us-surveilance-hackers-idUSBRE95G10520130617

5. *Gonzalez, R., Woods, R., Chochia, P.A.* (2005), "Digital Image Processing", translated from Eng., Moscow, Tekhnosfera, 1072 p.

6. CDS-5000 Mini IP Camera Dome System. Nuclear Services, available at: http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/nuclear/po-cds-5000-tcm92-49937.pdf

7. DTR 65 HRC, available at: http://www.ecagroup.com/en/solutions/dtr-65-hrc

8. *Fainzilberg, L.S., Zhuk, T.N.* (2009), "Guaranteed Assessment of Efficiency of Diagnostic Tests Based on Advanced ROC-Analysis" [Garantirovannaia otsenka effektivnosti diagnosticheskikh testov na osnove usilennogo ROC-analiza], Control Systems and Machines, No. 5, pp. 3—13. (Rus)

9. *Venttsel, Ye.S.* (1999), "The Theory of Probability" [Teoriia veroiatnostei], Moscow, Vysshaia Shkola, 6th edition, 575 p. (Rus)

10. *Bautin, A.V.* (2012), "Safety of NPP: from Chernobyl to Fukushima-1" [Bezopasnost' atomnykh elektrostantsii: ot Chernobylia do Fukusimy-1], available at: http://www.agps-2006.narod.ru/konf/2012/sb-2012/sec-1–12/13–01-12.pdf (Rus)

11. *Kobozeva, A.A.* (2009), "Basis of a General Approach to a Problem of Signal Forgery Detection" [Osnovy obshchego podkhoda k resheniiu problem obnaruzheniia falsifikatsii tsifrovogo signala], Electrical Machine-Building and Electrical Equipment, No. 72, pp. 35–41. (Rus)

Received 09.11.2015.