The Analysis of Modern Methods for Video Authentication

Pavel D. Gusev[1] and Georgii I. Borzunov[1,2]

[1] National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Moscow, Russia

pdgusev@gmail.com

[2] Russian state university of A. N. Kosygin (Technology. Design. Art), Moscow, Russia

borzunov_g@mail.ru

Abstract

This report is dedicated to the review of existing methods for video authentication. The study includes analysis and classification of existing methods by using algorithms and by problems which are solved by video authentication. The report presents the definition of video authentication, the typical authentication scheme is described and known algorithms are classified. The existing methods are analyzed in which the most promising directions are revealed and recommendations for further evolution of this subject.

Keywords: video authentication, authentication, video sequence, authentication algorithms, non-malicious modifications.

1 Introduction

Video-sequences as evidence play an important role in crime investigation because they allow to get precise and particular information [1]. Herewith the need for video authentication by the scientific approaches is greatly growing. In paper [2] the author has suggested algorithm for digital fingerprinting which can be used for fast task solution. Meanwhile although the problem topicality is growing constantly, techniques used in real video inspections often don't have scientific substantiation underneath. That is why the research and generalization of existing methods for camera identification and video authentication seems very relevant. This paper represents the results of such study.

2 Video authentication problem

It is necessary to consider that nowadays there is a wide range of powerful tools for different manipulations over video-sequences with various purposes [3]. In [4] video authentication is defined as process which considers that video content is authentic and is exactly the same as content of the video captured by camera. Solving this problem requires systematic approach that includes inner- and outer-frame montage detection, date, time and location identification, camera identification, video copying detection. Video can be considered as matrix function $V_0(t)$ with real values dependent on time t observed in rectangular window W during

some time interval T. If $B(t)$ is a modification matrix the modified video $M_0(t)$ is also real valued matrix function:

$$M_0(t) = V_0(t) + B(t). \quad (1)$$

For given video the video authentication process starts with features extraction. Features are some information from the video that identifies it uniquely. It can be some sample of brightness and color of pixels in some regions of different frames, motion direction vectors, etc. On the basis of features f authentication data H is generated. The generation algorithm is a function with features f with variable length as input and some sort of summarizing value H, generally with variable length either.

For example the method for digital fingerprinting developed in [2] that uses motion direction vectors can be used as an authentication data generation algorithm. Each frame or the vide is divided into $N = N_x \times N_y$ blocks. Let f_t and f_{t+1} be current and subsequent frames of the video. A small pattern *P* with the size (p_x, p_y) is chosen around the central pixel of block *B* in frame f_t with coordinates (x_t, y_t). Around the central pixel of the same block *B* but in subsequent frame f_{t+1} with coordinates (x_{t+1}, y_{t+1}) the search area with size (S_x, S_y) is chosen. Then pattern *P* is located to all possible positions inside the search area and sum of absolute differences of the corresponding pixels brightness components. This sum is used as areas matching measure. Such place inside the searching area where this sum is minimal is considered to be the matching area. Let (Mx_{t+1}, My_{t+1}) be the coordinates of this area central pixel. The displacement vector

$$d = (d_x, d_y) = (x_t - Mx_{t+1}, y_t - My_{t+1}) \quad (2)$$

is used to find motion direction feature

$$\theta = \arctan\left(\frac{d_y}{d_x}\right). \quad (3)$$

After that the graph of the angle θ from frame number in scene can be plotted for each block. In [2] vector consisting of these graphs local extremums is considered to be the authentication data. This analogue to hash function is added to simplify the authentication process as usually the number of features is massive. In the example above features are angles of motion direction. For each frame in depending of chosen settings there can be very few and it can be thousands of features. That lead to the amount of information from ten Kb to hundreds Mb (few Mb on average) for a 5 minute video if we use double variables to keep the angles. The result of the generation algorithm is relatively compact authentication data H. Depending on the algorithm collision probability can be various. In [2] there was no collision in 1000 videos. Then

authentication data are encrypted and packed with video as digital signature or inserted into the video content itself as a digital watermark. Video integrity is checked by generating new authentication data H’ and comparing with decrypted original authentication data H. If they match the video is considered to be authentic otherwise it was modified.

3 Requirements for video authentication system

Based on the analysis of modern video authentication algorithms the typical scheme determining requirements for video authentication systems was developed (Figure 1).

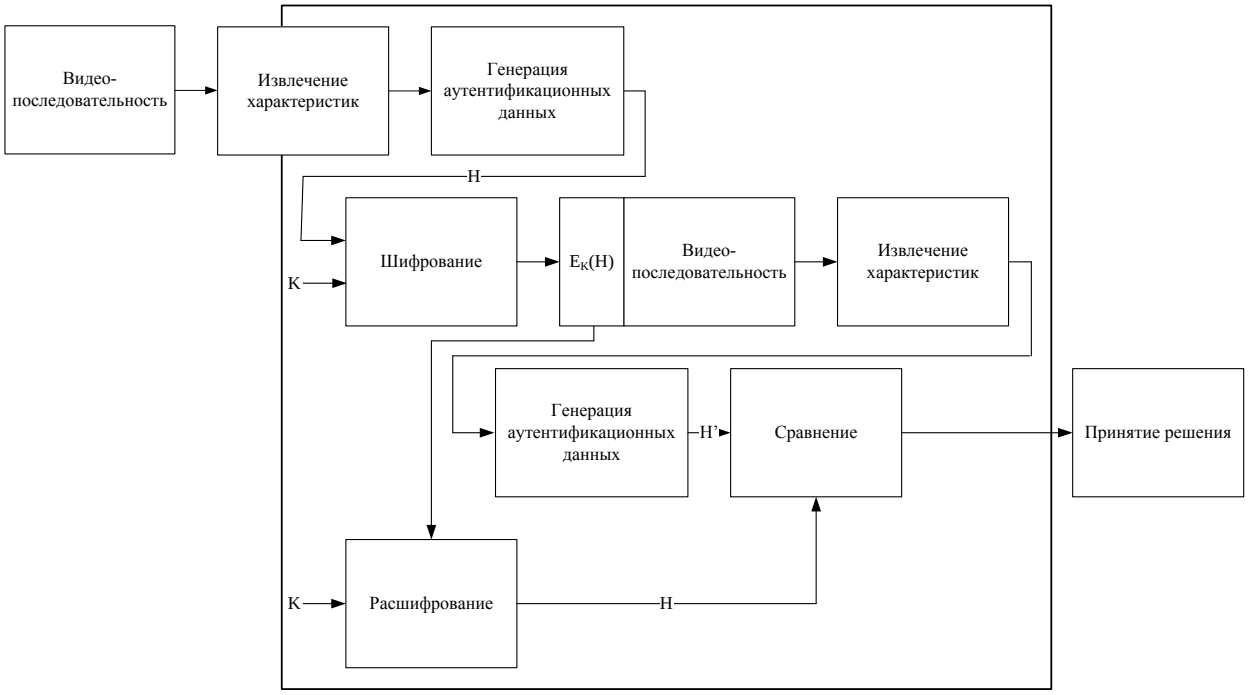

Figure 1 — Typical video authentication system.

According to established practice optimal video authentication system must:

- be sensible to malicious video tampering;
- localize and recover tampering regions;
- be sustainable to ordinary non-malicious video processing operations;
- consider possible insignificant information loss;
- have compact authentication data;
- be sensible to false features;
- be computing feasible.

Such video authentication system makes video resistant to non-malicious operations and allows to detect malicious tampering. In this paper non-malicious operations are considered to be video processing operations that do not modify video content semantically such as geometrical transformations, quality improvement and compression. During the analysis three classes of algorithms were examined: watermarking algorithms, digital signature algorithms and intelligence techniques (machine learning algorithms). 15 video authentication algorithms were

analyzed. In digital signature algorithms the signature depends on video data itself and some secret information (secret key) which is known only to verifying person. Actually digital signature only verifies video integrity. Digital signatures are used mostly in video surveillance systems. Watermarking algorithms use the multimedia data specificity for security mechanism integration. Although watermarking can be used for protection of any multimedia data most studies are dedicated to static digital images. Except multimedia data integrity check and malicious tampering detection watermarking algorithms are used to confirm the authorship of content. Predominant property of these methods is the ability to insert watermark without significant quality loss. As watermark is inserted strictly to video content any manipulation with video will change watermark itself. Such methods are usually applied for copyrighting, in video surveillance and other systems that have an access to the original video or/and original camera. Intelligence techniques (machine learning algorithms) are supposed to authentication of the video that wasn't protected anyway. In other words these algorithms intended for inner- and outer-frame montage and do not set a goal to confirm video integrity. Like every other machine learning system it needs to be educated on sufficiently big test sample before the use. Although general digital signature algorithms continue the development and have a bright future nowadays there is a trend of changing general algorithms to special ones that use features of the digital objects that need protection. That is why the main development of video authentication methods is observed in watermarking algorithms area and intelligence techniques. Nowadays great experience is accumulated in static images watermarking and the trend of much wider usage watermarking in video protection systems is observed. Soon there are new watermarking algorithms expected from static images protection and brand new resistant, half-resistant, non-resistant, visible, invisible, etc. Nowadays it is the biggest group of video authentication methods that are used with the condition that there is an access to the original video-sequence. However the most evolving methods nowadays are machine learning techniques. They allow to authenticate video when nothing is known about it. This area nowadays is not studied properly. The existing methods use as machine learning technique the Support Vector Machine (SVM). These algorithms show incredible results. For example one of the suggested algorithms was checked on the base of 795 modified and not modified video-sequences. The accuracy of classification was about 99,92%. Further implementation in this area is expected. Nowadays it can be assessed as the most promising. The complexity of education process must be pointed. To show high accuracy results education process time complexity must exceed authentication process complexity by several orders. As itself the educated algorithm must have time complexity equal to digital signatures algorithms on average.

4 Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Professional Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

5 Conclusion

Modern video authentication system must ignore random distortions ore modifications due to ordinary video processing, i.e. compression, resolution change and geometrical transformations. At the same time this system must detect distortions as a result of malicious attack. The selection of video authentication methods class depends on tasks that must be solved and available resources. Digital signature algorithms are the fastest and the strongest. They are used in surveillance systems for video integrity check. Watermarking algorithms are widely used in video authentication nowadays. Intelligence techniques solves the problem without any information about the original video-sequence. The usage of these methods needs long period of self-education. Nevertheless this research direction is the most prospective for video authentication improvement.

References

1 A.Epishkina, V.Matveeva Searching for Random Data in File System During Forensic Expertise // Biosciences Biotechnology Research Asia. – 2015. – Vol. 12, Issue 1. – Pp. 745 – 752.

2 P. Gusev, Development of Video Fingerprinting Algorithm // Bezopasnost informacionnyh tehnology. — 2015. - № 1. — P. 72-73.

3 A.Epishkina, V.Matveeva Visual representation of file content during forensic analysis to detect files with pseudorandom data // Scientific Visualization. - 2015. - Vol. 7, No. 4. — Pp. 109 – 120.

4 Saurabh Upadhyay, Sanjay Kumar Singh, Video Authentication – An Overview http://airccse.org/journal/ijcses/papers/1111ijcses06.pdf