Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 123 (2018) 161–164

Procedia Computer Science

www.elsevier.com/locate/procedia

8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017

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*

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

pdgusev@gmail.com, borzunov_g@mail.ru

Abstract

This paper 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 paper 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.

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures

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 (A. Epishkina, Searching for Random Data in File System During Forensic Expertise, 2015). Herewith the need for video authentication by the scientific approaches is greatly growing. In paper (Gusev, 2015) 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 (A. Epishkina, Visual representation of the file content during forensic analysis to detect files with pseudorandom data, 2015). In (Saurabh Upahyay) 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 (Gusev, 2015) that uses motion direction vectors can be used as an authentication data generation algorithm. Each frame or the vide is divided into $N = N_x \times N_y$

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures

10.1016/j.procs.2018.01.026

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

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

is used to find motion direction feature

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

After that the graph of the angle θ from frame number in scene can be plotted for each block. In (Gusev, 2015) 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 (Gusev, 2015) 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).

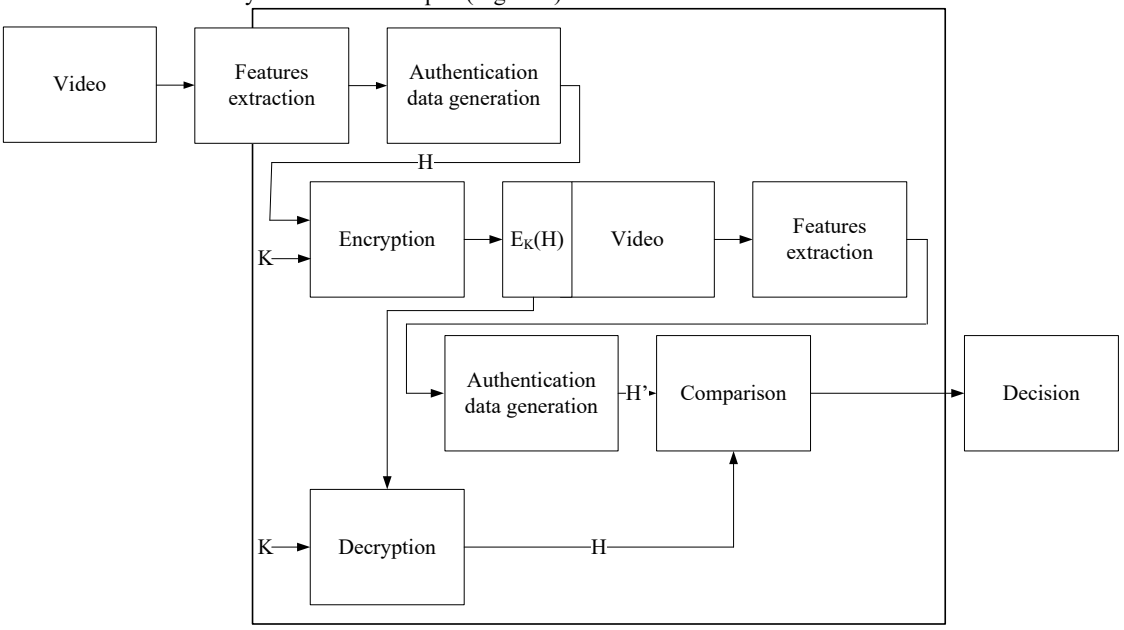

Figure 1 — Typical video authentication system.

According to established practice optimal video authentication system must:

- be sensible to malicious video tampering;
- localize and recover tampering regions;