IVAN GRGUREVIĆ, B.Eng.
E-mail: ivan.grgurevic@fpz.hr
ADAM STANČIĆ, B.Eng.
E-mail: adam.stancic@gmail.com
Ultra d. o. o.
M. Laginje 1, HR-47000 Karlovac, Republic of Croatia
PERO ŠKORPUT, B.Eng.
E-mail: pero.skorput@fpz.hr
University of Zagreb,
Faculty of Transport and Traffic Sciences
Vukelićeva 4, HR-10000 Zagreb, Republic of Croatia

Information and Communication Technology
Review
Accepted: Feb. 27, 2008
Approved: Nov. 6, 2008

CREDIBILITY AND AUTHENTICITY OF DIGITALLY SIGNED VIDEOS IN TRAFFIC

ABSTRACT

The paper presents the possibilities of insuring the credibility and authenticity of the surveillance camera video by digital signing, using the public key infrastructure as part of interoperable traffic and information system in the future intelligent transport systems. The surveillance camera video is a sequence of individual frames and a unique digital print, i. e. hash value is calculated for each of these. By encryption of the hash values of the frames using private encryption key of the surveillance centre, digital signatures are created and they are stored in the database. The surveillance centre can issue a copy of the video to all the interested subjects for scientific and research work and investigation. Regardless of the scope, each subsequent manipulation of the video copy contents will certainly change the hash value of all the frames. The procedure of determining the authenticity and credibility of videos is reduced to the comparison of the hash values of the frames stored in the database of the surveillance centre with the values obtained from the interested subjects such as the traffic experts and investigators, surveillance-security services etc.

KEY WORDS

digital signature, video recording, intelligent transport systems

1. INTRODUCTION

The digital video surveillance as part of the information-communication system of the future intelligent road i. e. part of the interoperable traffic-information system represents an upgrade of the classical road and should be considered as part of the information system of the intelligent transport systems (ITS). The possibilities of implementing the digitally signed video within the ITS and a whole series of additional possibilities provided by its implementation have not been considered in more detail either in the world or in the national scientific and professional circles.

According to the analyzed and available literature the scientific public and the papers published in a wider area of implementing videos focus as a rule on the issues of implementing the specialized applications of autonomous detection of disturbances in traffic, transport or logistic system. The issue of cryptographic protection of data has focused on the problems of preventing unauthorized access to data during their transfer. This paper is primarily focused on the possibility of redesigning the existing systems of video surveillance and implementing the digital system of video surveillance that provide authentic, credible and digitally signed video recording as output. Unlike classical video recording, the digitally signed video contents cannot be manipulated, without being detected. Apart from the basic functions offered, such systems create preconditions of interoperability at inter-organizational, organizational, functional, and technical level with other systems and provide the possibility of confirming the authenticity of a video and its legal credibility. Further in the text the basic notions of cryptographic protection of data and digital signature will be presented as well as the methods of preparation, processing and verification of surveillance camera videos, and the guidelines towards achieving interoperability from the aspect of ITS. In order to be able to sign digitally the video recording of a surveillance camera, the following conditions have to be fulfilled: video recording format has to allow digital signature of each frame, digital signatures have to be saved in the database for faster control and search, surveillance centre has to have an approved certificate of the digital signature and a pair of cryptographic keys and computer and software support of professional and qualified personnel.

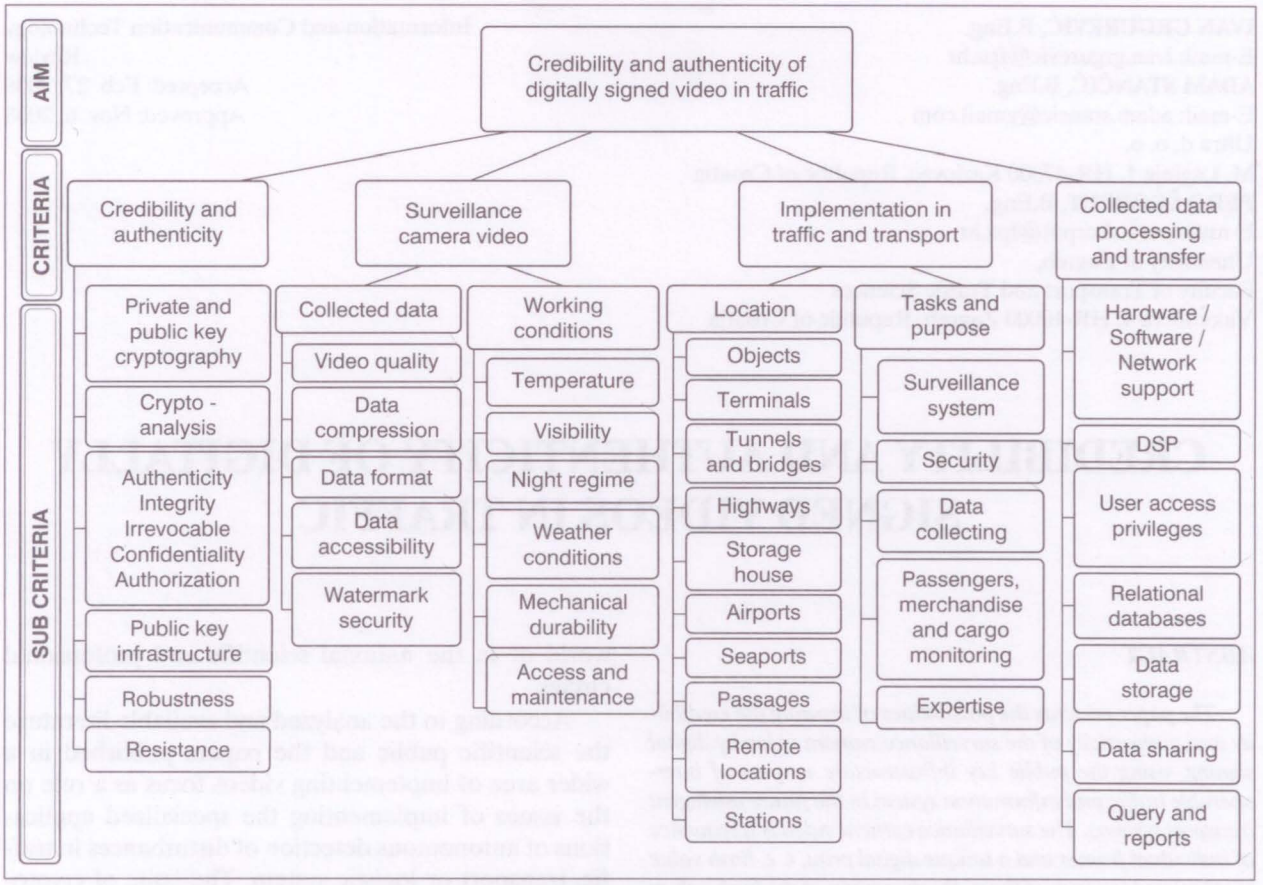

Figure 1 – Objective and criteria of credible and authentic digitally signed video

2. RESEARCH OBJECTIVE

The presented model defines the objective and sets the criteria in applying the digitally signed video in traffic. Each of the criteria, i. e. sub-criteria (which closely describes the process itself) can be studied independently, and using multi-criteria analysis possible alternatives may be defined.

Four basic questions have to be highlighted:

1. how to make the digital video credible and authentic?
2. how to check the credibility of digital videos?
3. who can and how one can use the advantages of a credible and authentic video recording?
4. which are the advantages, and which are the restrictions of the mentioned procedure?

As part of the answers to the first two questions, the scheme of collecting, processing, digital signing and verification of digital surveillance camera video is presented.

The paper will explain in more detail the systems of cryptographic protection and digital signing of electronic documents, the system of video surveillance and the format of recording of the collected data and finally the procedure of digital signing and verification. In the end the interoperability of implementing a credible and authentic video will be discussed, from the aspect of ITS and what are the advantages and limitations of the proposed system of ensuring credibility and authenticity of the video recording.

3. DIGITAL SIGNATURE

The key is a (secret) parameter used by the algorithms for encryption and decryption of data (encryption, i. e. data transformation into a coded form, and decryption, data transformation from the coded into the original form). The key has to be continuously changed in a strictly defined way so as to provide successful cryptographic protection. The procedure of digital signing includes the use of asymmetric encryption and *hash* function. It is characteristic for asymmetric encryption that pairs of private and public keys are used for coding and decoding. Everyone interested has a public key, and the private key is owned by the owner only. It should be explained where the value of the signature lies – the signatories confirm by their own signatures that they shall comply with, agree to the conditions, approve of the procedures and/or have been informed about the contents of the document. Apart from the committing effect, personal signature provides authenticity and legal power to the signed

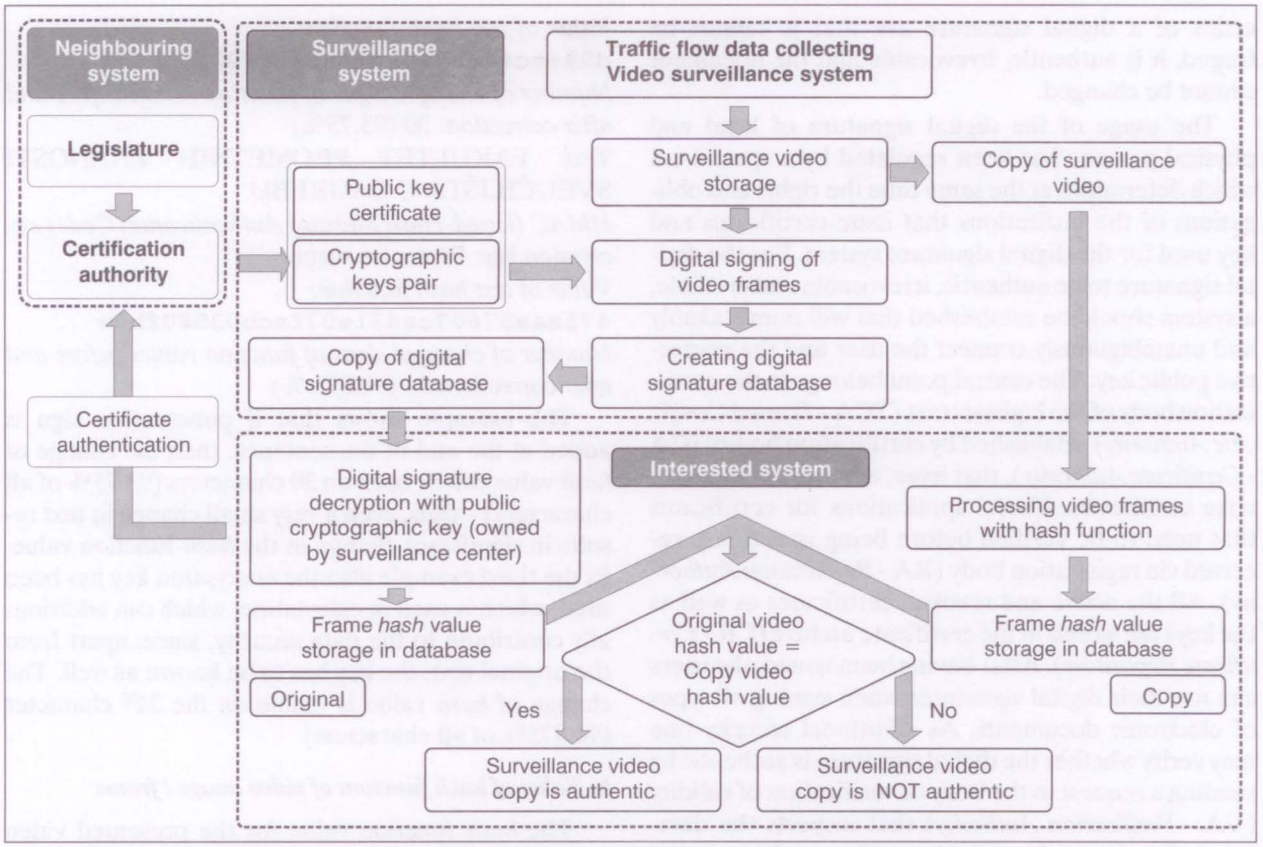

Figure 2 – System of digital signing and verification of video recording by surveillance camera

document. Every electronic document cannot be signed personally, and it is necessary to know who signed, what was signed and to what has the signer made the commitment. Primarily, the digital signature has to have support in legal provisions of the legislative bodies of the state or in international agreements to which the state has committed itself in order to be legally valid, credible and acceptable. The basic prop-

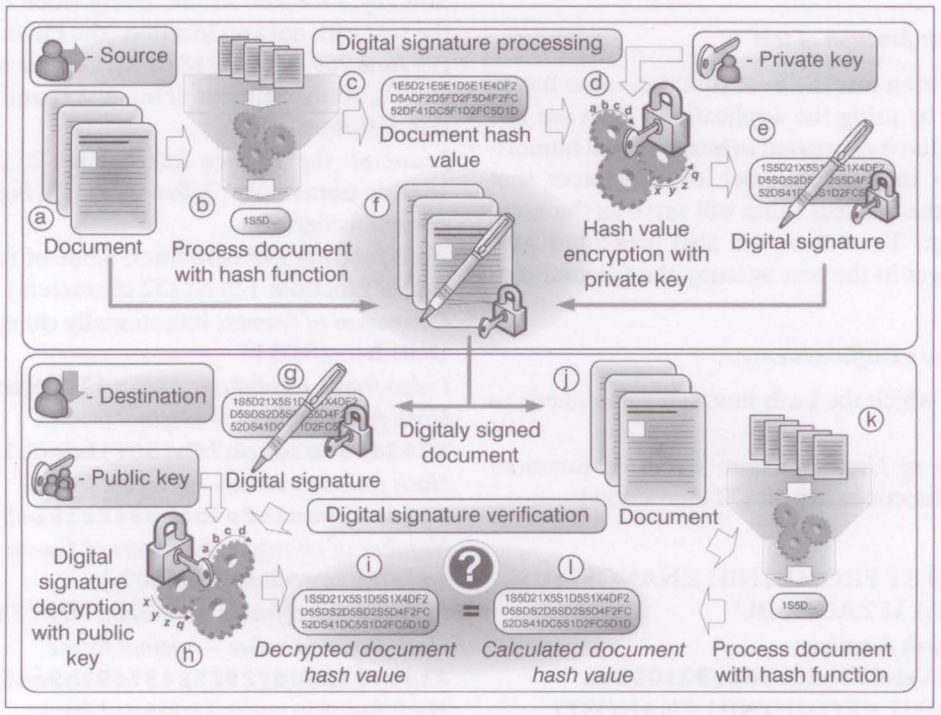

Figure 3 – Signing and verification of digital signature of the electronic document

erties of a digital signature are that it cannot be forged, it is authentic, irrevocable and the document cannot be changed.

The usage of the digital signature of legal and physical persons has been regulated by a special act which determines at the same time the rights and obligations of the institutions that issue certificates and key used for the digital signature system. For the digital signature to be authentic, irrevocable and credible, a system should be established that will unmistakably and unambiguously connect the user and the respective public key. The central point belongs to the certification body of the highest trust (TCA - *Trusted Certificate Authority*) established by certification bodies (CA - *Certificate Authority*), that issue, administrate and revoke certificates. Users' applications for certificates that need to be verified before being issued, are received via registration body (RA - *Registration Authority*). All the active and revoked certificates as well as the keys are stored in the certificate archive (CR - *Certificate Repository*). After having been issued, the users can use their digital signatures when signing all types of electronic documents. As additional security one may verify whether the digital signature is authentic by sending a request to the body of verification of validity (VA - *Verification Authority*) that inspects the database of active and revoked certificates through the certification body.

4. EXAMPLES OF *HASH* FUNCTION EVALUATION OF VIDEO FRAME

a) Value of hash function of text

For the written text the *hash* function value has to be calculated by using the application *HashCalc ver. 2.02*[1]. *Hash* value is expressed in hexadecimal numerical system so that the number of characters that changed and the decimal value will serve as the measure of change. The values are also presented with minimal changes in the text by using the (textual) encryption key:

Prometni sustav (Traffic system):

Text: Text for which the hash function value needs to be calculated.
Characteristics of Hash function: name of function: MD5, size of function: 128 bit (32 characters)

Examples:

Text: FAKULTET PROMETNIH ZNANOSTI SVEUČILIŠTA U ZAGREBU
Value of text hash function:
`80e3b942a61eb653cdfe062c921012ea`
Text: FAKULTET PROMETNIH ZNANOSTI SVEUČILIŠTA U ZAGREBU. (dot)
Value of text hash function:
`d994cc4aeb9a45c763fdcff00603b7f1`
Number of changed signs of function values before and after correction: 30 (93.75%)
Text: FAKULTET PROMETNIH ZNANOSTI SVEUČILIŠTA U ZAGREBU
HMAC (keyed-Hash Message Authentication Code) encryption key: Prometni sustav
Value of text hash function:
`475aae87607ca431e07facb03580fb5e`
Number of changed signs of function values before and after correction: 31 (96.875 %)

The example shows that if punctuation sign is added at the end of the sentence, then the change of *hash* value can be seen on 30 characters (93.75% of all characters) – thus, even a very small change in text results in significant change in the *hash* function value. In the third example also the encryption key has been used, which is used in calculation, which can additionally contribute to the data security, since, apart from the original text, the key has to be known as well. The change of *hash* value is visible on the 31st character (96.875% of all characters).

b) Value of hash function of video image / frame

The *hash* function value for the presented video frame has to be calculated by using software *HashCalc ver. 2.02.* In order to study the level of change in the *hash* function value before and after correction, it is necessary to change the resolution of the original frame, as well as the presentation of time (in the upper left corner of the frame) and by using (textual) encryption key: *Prometni sustav*. Every video frame contains the text with data on location (the Plitvice Lakes) date (*25 June 2007*), time (*18:01 h*), camera number (*Camera: 2*), frame number (*Frame: 23*) and video resolution (*Hi-Res*).
Location: the Plitvice Lakes, *date*: 25.06.2007., *time*: 18:01 h, *camera No.*: 2, *frame No.*: 23, *high resolution of camera recording*.
Hash function characteristics: name of function: MD5, size of function: 128 bit (32 characters)
Correction of frames: intentionally changed time from 18:01 h to 18:03 h!
Video frame resolution: 2288 x 1712 pixels
Hash function value – original frame
`7743d997b3eaeb7fbf50f1bdacb15c86`
Hash function value – corrected frame
`F99da404eefe2a4acbe842c182e5fece`
Number of changed characters of function value before and after correction: 32 (100%)
Reduced video frame resolution: 709 x 530 pixels
Hash function value – original frame
`F184403380df29252437f93b9e462c26`
Hash function value – corrected frame
`4bd06ee365ddafbc86bf7b129a06d3c6`

Figure 4 – Original frame

Figure 5 – Corrected frame

Number of changed characters of function value before and after correction: 28 (87,5 %)
Frame res.: 2288 x 1712 pixels + text. *HMAC encryption key:* Prometni sustav RH
Hash function value – original frame
83d8451e8223cd87d7b82a022264640c
Hash function value – corrected frame
A345132315574543f7cd1376bb2490af
Number of changed characters of function value before and after correction: 29 (90,625 %)
Frame res.: 709 x 530 pixels + text. *HMAC encryption key:* Traffic system of RH
Hash function value – original frame
F3af310dbbfc9d93dc2d2af2620bdd82
Hash function value – corrected frame
A5c813898b916f902cd1ff4adb860c8d
Number of changed characters of function value before and after correction: 28 (87.5%)

From the example in which the resolution and the content of the video frame (regarded as a static image) were changed, one can see that the change of resolution, change of content (last digit in the time display) and usage of the textual encryption key (*Prometni sustav RH*) change significantly the *hash* function value of the video frame.

Both examples show how a very small change in the content of the text or image will result in significant change of the *hash* function value. In order to prove manipulation, it would be sufficient to find the minimal change (in just one value sign), and in the mentioned examples the minimal change is as much as 87.5% of characters, which very clearly and unambiguously indicates that the text or image have been manipulated.

5. VIDEO SURVEILLANCE SYSTEM IN TRAFFIC

The existing video surveillance systems have been developed over the last twenty years and they have found wide application in various segments of human activities. Their application in traffic dates back to their very creation, reduced mainly to the transfer of mobile or fixed images to the traffic surveillance centres. Today, *Wide Area Vehicle Detection System* or VIDS systems (*Video Image Detection System*) are common.

The video surveillance systems basically consist of video cameras and central control unit in which, apart from collecting, processing and saving of video recordings, the detection of relevant values of the observed traffic flow can be carried out, and in systems of the latest generation also the digital signing of the video. The obtained analogue or digital video recording and the traffic flow parameters can be sent directly to the traffic surveillance centre or can send feedback to the control device at the intersection.

The analysis of the existing video surveillance systems in traffic and the synthesis of the acquired knowledge in the field of cryptography, video recording and ITS have resulted in the knowledge that insufficient attention has been paid to authenticity, integrity and credibility of the data collected by the video surveillance.

5.1 Digital systems of video surveillance in traffic

Advanced digital video surveillance cameras store the data in digital form in the desired format. It is easy to process the digital video and to obtain any desired effect with amazing precision and reality of the presentation which makes it suitable for the art of film, but its drawback is a very low level of authenticity. How can one know that nobody has manipulated the digital video and that what is displayed is precisely what the author of the recording wanted to display. The conversion of the analogue signal into the digital

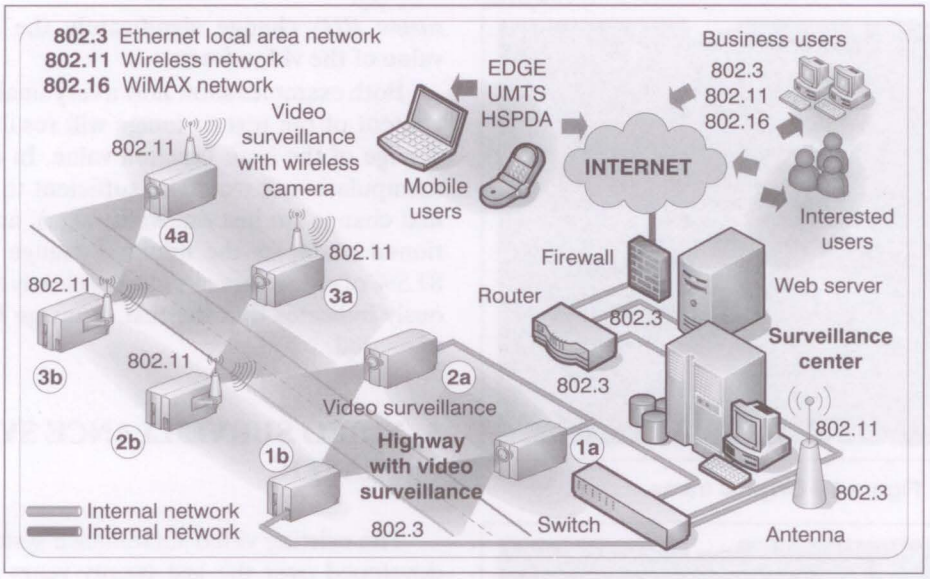

Figure 6 – Scheme of video surveillance system of the road

form and its processing so as to get the video in the desired format is done by the digital surveillance camera itself using electronic units found in its housing. The surveillance camera recording contains a large number of data and the video recording has to be processed, and it has to be stored, transferred (by limited) transfer capacities or additionally processed (e. g. digitally signed). The existing analogue video surveillance systems can be used and adapted to the requirements of interoperability, authenticity, integrity and credibility since they can be subsequently digitalized and cryptographically processed.

Basically, the processing of a "plain" video means compression of the video that can be:

- compression with losses;
- compression without losses.

The algorithm of compression with losses of video data "expels" redundant data keeping in mind that the quality of the video remains sufficiently good for the control. The algorithm for compression of the video takes advantage of the effect of the human eye inertia (human eye notices well the change in lighting, but has very poor recognition of small changes in colour nuances). The video compressed in this way occupies less memory and is more suitable for the transfer and emitting, but the compression procedure is not reversible – the video cannot be returned to its original condition. Compression without losses allows the original video to remain exactly the same as when it was recorded by the surveillance camera, but the compression does not significantly reduce the memory size of the video which makes it unsuitable for transfer or emitting.

5.2 Preparation of video recording

Since surveillance camera videos are located at separate locations, the video needs to be transferred by telecommunication-information infrastructure to the surveillance centre, user or other subject. Because of the limited transfer capacities the video needs to be compressed (with loss) and saved in such a format which treats the video as a series of separate images i. e. frames. This is the necessary condition since it is necessary to digitally sign each single frame in order to make the video credible. When encoding the video two encoding techniques are used, the inter-frame and intra-frame one.

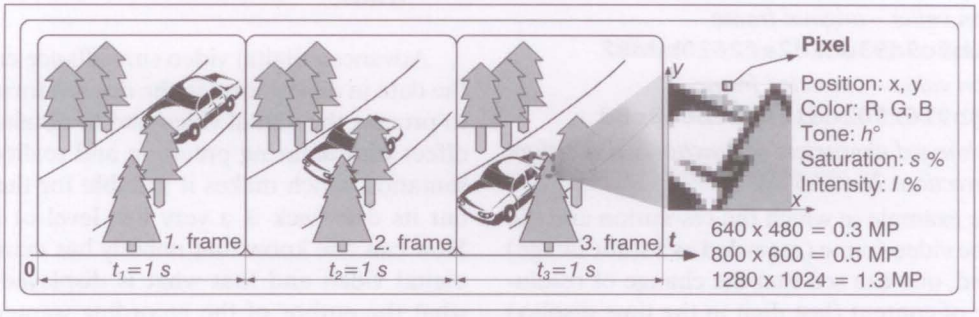

Figure 7 – Video frame parameters

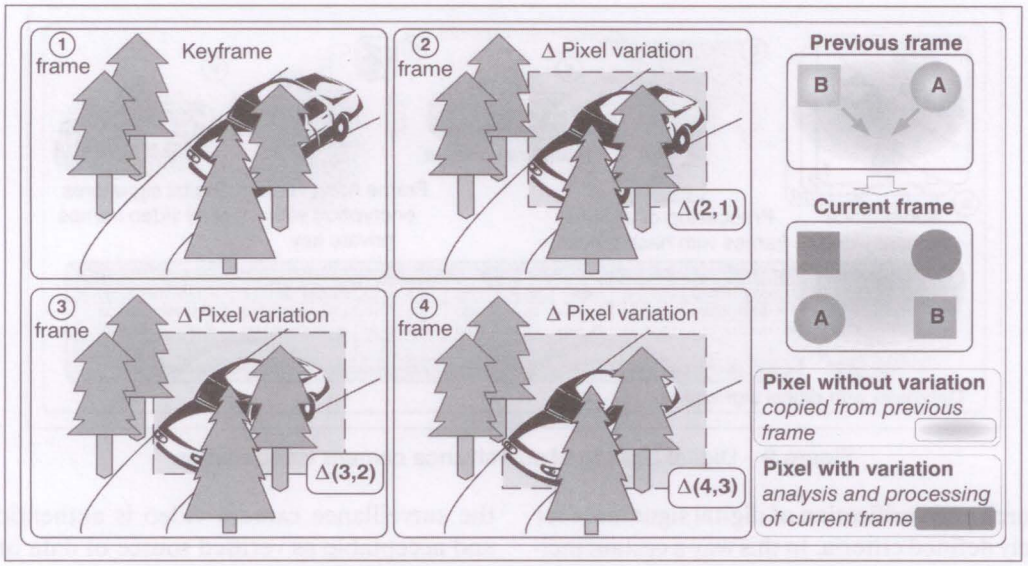

Figure 8 – Processing of MJPEG format of video recording

The inter-frame encoding technology compares each video frame with one or more previous frames. If nothing changed in the frame compared to the previous frame then the pixels of the previous frame are copied to the frame being studied, and if there has been change in the pixels (e. g. because of the shift of the object) then the algorithm of the image processing will change colour, intensity or saturation of the copied pixels in the frame. If one frame is deformed (e. g. in processing or transfer of data) then all the subsequent frames will be deformed and the recording will not be properly displayed. The so-called key frames can be used as the solution to the problem, and these would be entirely taken over from the video, and the remaining sequence of frames (to the following key frame) would be compared with the previous one. Such processing of data is fast and results in a video recording which occupies significantly less memory and is suitable for transfer and emitting.

The intra-frame encoding technology considers every video frame independently and compresses it as a static image. The video recording is of high quality, and occupies a large amount of memory and is not suitable for transfer and emitting but rather for storage and archiving. The format of the surveillance camera video recording which fulfils two essential conditions: processing of each single frame and high level of compression with satisfying quality of the video recording is the MJPEG format. MJPEG (*Motion JPEG*) is a digital video format in which every frame is processed and compressed as special JPEG (*Joint Photographic Experts Group*) recording, and the inter-frame encoding technique is used, which renders a high level of compression and becomes the unofficial standard of the video recording of digital surveillance cameras.

JPEG format of the recording of the static image has not been patented which allows wide usage, and the processing, creation and reproduction of MJPEG video is not demanding regarding processor, which additionally stimulates further development and implementation of this video format. The standard for the transmission of MJPEG videos via Internet has been defined by the working group for the transfer of visual and audio data (*Audio-Video Transport working group*) as part of IETF (*Internet Engineering Task Force*) with the document RFC (*Request for Comments*) 2435 which defines the transfer of MJPEG video recordings in real time (*Real-Time Transport Protocol Payload Format for JPEG-compressed Video*). The drawbacks of MJPEG format are that there is (currently) no unique standard system which precisely determines the format. If the video recording is of high quality, then the memory occupancy is somewhat greater than in other widespread formats of the video recording. Furthermore, a more advanced format of the JPEG static images which are not used by MJPEG (currently).

5.3 Procedure of digital signature of video recording

The digital signal of the surveillance camera is transferred to the surveillance centre and saved in MJPEG format. Since the video recording is saved as a sequence of static images, i. e. frames, then it is possible to sign digitally each of them. In order to make a saving on resources, it is possible to sign every *n*-th video frame. All the digital signatures are saved in SQL (*Structured Query Language*) compatible database which can be easily maintained and searched later. The database of digital signatures has to be organized according to the criteria of time, location and surveillance camera identification label of the surveillance camera in order to be able to perform the proce-

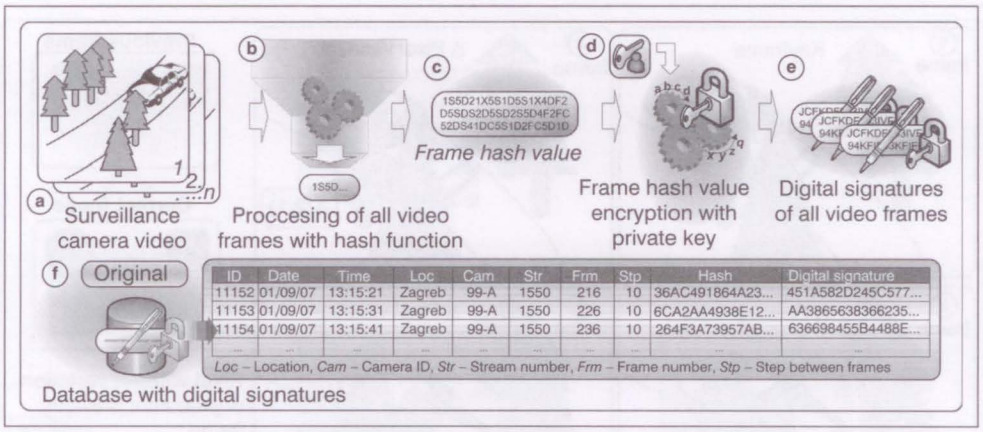

Figure 9 – Digital signing of surveillance camera video frames

dure of search and verification of digital signatures for the precisely defined criteria. In this way a certain incident situation between two key frames can be isolated from the video, and the digital signatures of a series of selected frames can be verified.

5.4 Procedure of verifying digital signature of video recording

If the surveillance camera video is the source of data for the traffic expert or interested subject, then the video recording is copied from the surveillance centre to the desired location and the procedure of digital signing of each frame is repeated. All the digital signatures of the video copies are stored in a special database that is compared with the original database. If all the recordings in both bases are identical, then the surveillance camera video is authentic, credible and acceptable as verified source of data or evidence material. Verification can be done in two ways as presented in Figures 10 and 11.

5.5 Interoperability of applying digital video recording from the aspect of intelligent transport systems

According to Prof. Bošnjak, D. Sc., to achieve solution interoperability *in principle four main aspects of ITS interoperability may be identified.* [1]

- *technical interoperability;*
- *functional interoperability;*
- *institutional interoperability;*
- *legislative measures for interoperability.*

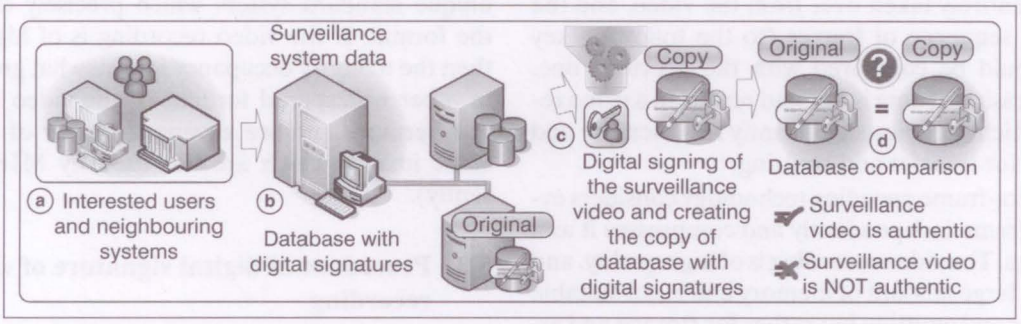

Figure 10 – Verification of digital signature of frame by comparing frame database

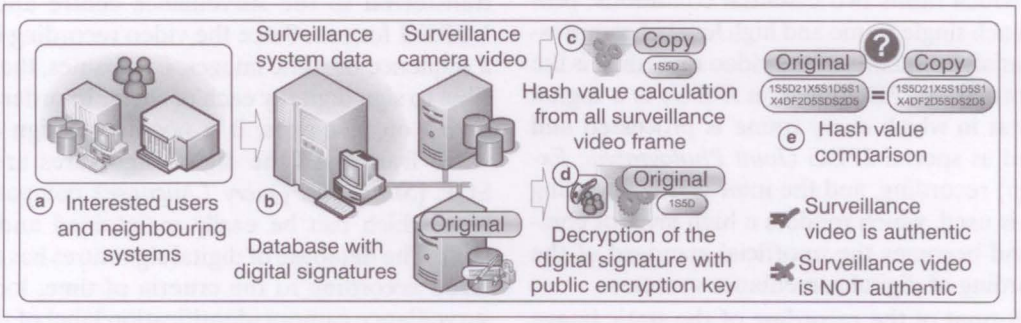

Figure 11 – Verification of digital signature of frame by comparing hash value of frames

The introduction of digitally signed video should not be considered as separate telematic solution but rather as upgrade and re-engineering of the traffic, transport and logistic system. The application of this type of system of digital video does not require development of new and expensive technologies, methodologies and knowledge since the current level of development of computer, software, video and information-telecommunication technology allows effective procedure of digital signing of the video.

6. CONCLUSION

There is no strictly defined methodology of ensuring the credibility and authenticity of video recordings with the aim of usage as verified and reliable source of data on the condition of the supervised part of the traffic system. Digital recording can be easily manipulated and until now it has not been considered a serious and credible source of data or proof of recorded condition. In order to carry out the entire procedure of implementing and verifying the credibility of the video recording, it is possible to use the existing technical and technological means and systems. The systems of older generations of surveillance cameras, computer-software support and information-telecommunication infrastructure need to be upgraded because of substantially greater amount of data that need to be collected, processed, saved and delivered.

The 4th chapter provides an example of calculating the value of hash function of text and image, i. e. video frames. The results show that a very small change of the contents significantly changes the hash function value. For example, it is sufficient to add in the original text only a punctuation sign, which changes the hash value of the changed text in 30 characters (93.75% of all characters). When this refers to the image, then the hash value of the manipulated image changes in the range from 28 characters (87.5%) to 32 characters (100%) depending on the level of manipulation and processing (performed on the image, i. e. video frame). This significant change guarantees that every manipulation of video contents will be simply and easily detected.

Through analysis and synthesis of the existing knowledge on cryptographic protection of electronic documents, video surveillance and ITS, the paper presents the method of digital signing of video recordings of surveillance centre camera and verification of its credibility. Credibility and authenticity of digitally signed video recording in traffic have been considered from several aspects of ITS interoperability (technical, functional, institutional and legislative) and can be considered as the main guidelines in developing the system. Every part of the video digital signature system has shown individually in practice as reliable and functional, but for the moment there is no practical implementation of the system that would unify the digital signature and video surveillance. The legislation mentions explicitly the digital signing of electronic documents, not mentioning the video recording or frames of which it is composed.

The presented system of ensuring credibility and authenticity offers the following advantages: insurance of high level of credibility and integrity, the video becomes a reliable source of data in scientific and research work of traffic experts and many other systems (national safety, police, insurance companies, etc.), impossibility of ill-intentioned manipulation of video. In the implementation of the presented system of insuring the credibility and authenticity of the video the following restrictions are possible: increased costs due to upgrading of the technical and technological means of the older generation, organizational and financial burdens due to the training of professional staff, and (for the moment) understated legislation.

IVAN GRGUREVIĆ, dipl. ing.
E-mail: ivan.grgurevic@fpz.hr
ADAM STANČIĆ, dipl. ing.
E-mail: adam.stancic@gmail.com
Ultra d. o. o.
M. Laginje 1, 47000 Karlovac, Republika Hrvatska
PERO ŠKORPUT, dipl. ing.
E-mail: pero.skorput@fpz.hr
Sveučilište u Zagrebu, Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb, Republika Hrvatska

SAŽETAK

VJERODOSTOJNOST I AUTENTIČNOST DIGITALNO POTPISANOG VIDEO ZAPISA U PROMETU

U radu su prikazane mogućnosti osiguranja vjerodostojnosti i autentičnosti video zapisa nadzorne kamere postupkom digitalnog potpisivanja korištenjem infrastrukture javnog ključa kao dijela interoperabilnog prometno-informacijskog sustava u budućim inteligentnim transportnim sustavima. Video zapis nadzorne kamere je slijed pojedinačnih okvira i za svaki od njih se izračunava jedinstveni digitalni otisak, odnosno hash vrijednost. Kriptiranjem hash vrijednosti okvira privatnim kriptografskim ključem nadzornog centra kreiraju se digitalni potpisi koje je pohranjuju u bazu podataka. Nadzorni centar može izdavati kopiju video zapisa svim zainteresiranim subjektima u svrhu znanstveno-istraživačkog rada i vještačenja. Bez obzira ne opseg, svaka naknadna manipulacija sadržajem kopije video zapisa sigurno će promijenit hash vrijednost svih okvira. Postupak utvrđivanja autentičnosti i vjerodostojnosti video zapisa svodi se na usporedbu hash vrijednosti okvira pohranjenih u bazi podataka nadzornog centra sa vrijednostima dobivenih na strani zainteresiranih subjekata kao što su prometni stručnjaci i vještaci, nadzorno-sigurnosne službe i sl.

KLJUČNE RIJEČI

digitalni potpis, video zapis, inteligentni transportni sustavi.

REFERENCES

1. http://www.slavasoft.com/hashcalc/index.htm, version for MS Windows operation system

LITERATURE

[1] **Bošnjak, I.**: *Inteligentni transportni sustavi 1*, University of Zagreb, Faculty of Transport and Traffic Sciences, Zagreb, 2006

[2] **Boillot F., Midenet S., Pierrelée J. C.**: *The real-time urban traffic control system CRONOS: Algorithm and experiments*, Transportation Research Part C, Volume 14, Issue 1, Pages 18-38, 2006

[3] **Boillot F., Midenet S., Pierrelée J. C.**: *The real-time urban traffic control system CRONOS: Algorithm and experiments*, Transportation Research Part C, Volume 14, Issue 1, Pages 18-38, 2006

[4] **Barker E., Barker W., Burr W., Polk W., Smid M.**: *Recommendation for Key Management – Part 1: General* (Revised), National Institute of Standards and Technology, NIST Special Publication, 2006

[5] **Hartung F., Girod B.**: *Fast public-key watermarking of compressed video*, Proc. ICIP'97, Vol. I, pp 528-531, 1997.

[6] **Saaty, T. L.**, *Decision Making for leaders - The Analytic Hierarchy process for Decisions in a Complex World*, RWS Publications, USA, 2001

[7] **Zhang X., Forshaw M. R. B.**: *A parallel algorithm to extract information about the motion of road traffic using image analysis*, Transportation Research Part C, Volume 5, Issue 2, Pages 141-152, 1997

[8] *Hash Calculator*, http://www.slavasoft.com/hashcalc/index.htm (02 Feb. 2008)

[9] Narodne Novine službeni list RH (Official Gazette), No. 10/2002, *Zakon o elektroničkom potpisu*, http://www.nn.hr/ (02 Feb. 2008)