ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20151228192623
Preliminary communication

Steganographic Integration of the Data Collected on the Traffic Road

Adam STANČIĆ, Ivan GRGUREVIĆ, Zvonko KAVRAN

Abstract: The surveillance system video structure represents a suitable medium for steganographic integration of the collected data about the condition of the road and its environment. The surveillance video retains the function of visual presentation of the condition on the road, and the integrated textual data are a component of the video recording structure. The analysis of the steganographically processed video frames indicates the impact on the integrated textual data, the video quality and the impact of manipulation of data on the integrated data. The work uses steganographic algorithm F5 for integration of various amounts of compressed textual files into image recordings recorded under various conditions. In order to prove that integrated and extracted data have identical content, cryptographic and polynomial functions have been used. For the calculations of statistical properties of the values of red, green, blue and intensity component the model was used formed in the MATLAB / *Simulink* applications.

Keywords: data analysis; data integration; statistical properties of images; steganography; surveillance video; traffic system

1 INTRODUCTION

Steganography is a combination of the Greek words *steganos* (στεγανός) – meaning "covered, concealed, or hidden" and *graphē* (γραφή) – meaning "drawing or writing". Literally translated, steganography means "secret writing" [1]. Steganography is a procedure of inserting a secret message within a "false" message which transfers information exploiting the characteristics of the human senses, in this case the sense of sight [2]. At the destination of the information follows the procedure of extracting the inserted message from the transferred file. The inserted message can be compressed, encrypted and protected by a password in order to make additionally difficult any unauthorized access and to eliminate repeating patterns in the data structure [3]. The aim of steganographic data processing is their protection against unauthorized access. The cryptographic protection is based on the complexity of the secret code used to protect the information, whereas steganography hides the protected information within the content that is used as a transportation medium.

A component of a modern road is the surveillance video system and the measurement devices, sensors and equipment used to collect data about the road condition. The basic idea of the carried out research is the formation of a combined source of information about the road condition by using the mechanism of steganographic integration and cryptographic data protection. The idea is to steganographically integrate the compressed and cryptographically protected data about road condition within the structure of the surveillance video. A healthy human eye should not notice that changes had been made to the contents of the video recording, and an unauthorised user could not access the integrated data. The traffic experts receive available authentic and credible source of information about the road condition in the form of visual and analytic information. The use of steganographic methods of integration of the collected data within the structure of the image recording allows:

- video recording of the surveillance camera to retain its basic function. The user who has no knowledge about the integrated data inspects a "usual" surveillance video recording;
- access to integrated data is possible only with adequate software support and ownership of the proper user rights;
- usage of steganographic integration of data for the integration of control data within a video recording as a measure of detection of manipulation with the contents of the surveillance video.

1.1 Subject and Aim of Research

The subject of research is the presentation of the procedures of steganographic integration of the traffic-relevant data into a combined, authentic and credible source of information about the traffic system condition. The steganographic integration means formation of a steganogram, i.e. information entity that will integrate within its structure data, i.e. another information entity. The primary subject of research is the influence of steganographic processing on the structure, content and memory occupancy of integrated data within a steganogram. The secondary subject of research is the influence of the steganographic processing on the statistical properties and visual quality of the steganogram. The application of appropriate mathematical and statistical methods in combination with the visual inspection should provide a clear answer to what extent the steganographically processed data are applicable and usable by the traffic experts. The main hypothesis of the presented paper can be summarised in the question whether it is possible to use the mechanisms of steganographic data processing. The primary objective is the formation of a combined, reliable and credible source of data that would, apart from visual representation of the situation, contain also information on the condition on the road and its environment. To achieve the aim of research it is necessary to carry out a series of experiments, and by using the mathematical and statistical model to study the influence on the integrated and transfer data, i.e. image recording (steganogram). In the first phase of research the study deals with how the procedure of steganographic processing and steganogram content manipulation affect the integrated data. The integrated data must not be altered in any way, not in the least. Detection of a difference in the data contents before integration and after

extraction is unacceptable. In that case the steganographic method of integrating traffic-relevant data is not applicable since it is not possible to form a reliable source of information about the road condition.

The second phase of research analyses the influence of the steganographic processing on the transfer data, i.e. steganogram. The preservation of the quality of transfer data is the secondary aim of this paper. In this case the steganogram is not a means of distracting the observer from the integrated data but rather it also contains the visual representation of the condition on the road. If the steganographic processing should result in the occurrence of patterns, artefacts or if it should disturb the visual presentation (static image or surveillance video) then the method of steganographic processing would be unacceptable. Both phases of research and objectives are presented in Fig. 1.

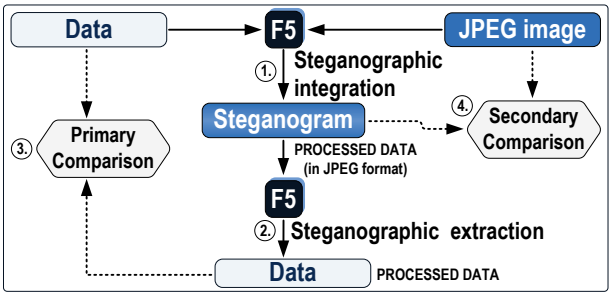

Figure 1 Primary and secondary aim of the analysis

Through a number of performed experiments and analyses of the results, the attempt was made to prove the hypothesis that steganographic integration of the collected traffic-relevant data changes the content of a steganogram (image recording) to such an extent which does not disturb its quality and usability while the content of integrated (textual) data remains completely unchanged.

1.2 Previous Research

The analysis of the available relevant scientific and research literature shows that the topics related to steganography deal with the following issues:

- still image steganographic processing, [4, 5, 6];
- stegoanalysis, [4, 5, 6];
- analyses of the characteristics and development of newer steganographic algorithms, [3];
- copyright and protection of intellectual rights for digitally saved data (very often the topic is the use of digital watermark), [1];
- generating of concealed communication and control sub-channels within TCP/IP protocol-based computer networks, [7];
- use of steganographic processing of data during VoIP communication, [8] and
- videosteganographic processing, [9, 10].

It should be emphasised that steganographic processing is regularly treated as a method of data protection. The scientific papers dealing with the topic of steganography can be divided into two categories according to the procedures – methods of encrypting and methods of detecting the steganographically processed files. Not a single one of the available scientific and research works deals with the topic of using steganography as a suitable method of integration. The transfer medium, i.e. the steganogram has the role of distracting the observer using banal (irrelevant) content.

In this paper, the primary property of steganographic processing is data integration, and concealing the data from the observer is not the focus of research. Special attention has been paid to the property of the steganographic algorithms concealing the data so that they are invisible to the human eye. In its content the data transmitter does not transfer banal or uninteresting information, but rather a visual representation of the condition on the road which is of high value for the traffic experts. Combining visual representation within which the data about the condition on the road have been steganographically integrated, forms a combined source of traffic-relevant data for the traffic experts, forensic investigations or analysis of the observed situation.

2 FORMATION OF COMBINED SOURCE OF INFORMATION

The data from different data sources collected at the same time on the same place (i.e. in appropriate spatial and time context) can be observed as common set of data that describe the condition of the observed section of ITS (*Intelligent Transportation System*), i.e. modern road. The sense of forming a combined source of data is easier viewing and analysis of the condition of a section of the traffic system.

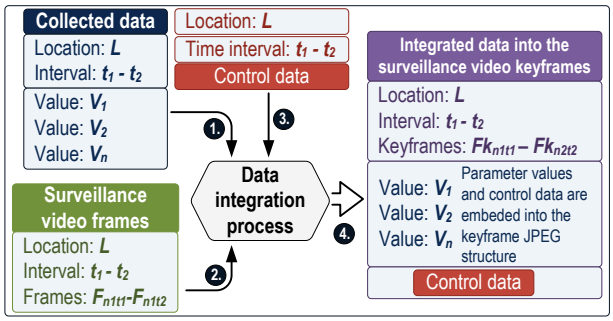

Figure 2 Combining of the collected traffic-relevant data

All the traffic-relevant data are integrated into a unique and authentic source of data which liberates the traffic experts from collecting and harmonizing the information collected from several different sources of traffic-relevant data.

Fig. 2 shows the procedure of integrating the collected data within the surveillance video frame structure. Fig. 2 mentions additionally the control data that help in preserving the integrity, authenticity and credibility of the combined source of traffic-relevant data. Regardless of the technical means and technology that were used to collect the data, all the collected information has to possess certain characteristics: common space and time of collecting traffic-relevant data and surveillance video recordings, defined technical means and technologies used to collect data, defined traffic parameters and data that are collected and are to be integrated into a whole, and defined structure of the recordings of collected data.

2.1 Selection and Collection of Data

By using the installed or mobile measuring instruments, sensors and measuring equipment, it is possible to collect a multitude of data about the condition of the observed section of the traffic system. The proposed combined source of traffic information which will be used in this work is presented in Fig. 3.

Survillance Video	Date of rec.: 23.05.2015 Time of rec.: 06:55:21 PM Camera ID : CAM:FPZ-KA	Clip No.: 089 Frame No.: 22774 ID: 552D5AA85793001CAD1
Traffic Radar	Radar ID : 511:FPZ-KA Location: Karlovac, HR Time: 23.05.2015/06:55:21 Street : Trg K.P. Svacica 1 Capture Zone : Entire street Radar Heading: 216 Speed Limit: 50 km/h Types of Vehicles : All	Direction(s) : Approaching Min rec. speed: 30 km/h Max rec. speed: 81 km/h Avg rec. speed: 40,9 km/h Last rec. speed: 37.2 km/h No. of Vehicles: 1085 (100%) No. of Veh. in limit: 1002 (92%) No.of Veh. over lim.: 87 (08%)
Meteorolog. data	Station ID: MET:FPZ-KA Location: Karlovac, HR Date/Time: 23.05.2015 Time: 06:55:21 PM Visibility: Good	Air temperature: 12 C / 53.6 F Pressure: 100.6 kPa Wind speed: 1.2 m/s Wind direction: W Humidity: 63%
Camera properties	Camera ID : CAM:FPZ-KA Location: Karlovac, HR Time: 23.05.2015/06:55:21 Camera Heading: 219 Field of View: 35 mm	Zoom: 1,0x Resolution: 1024x768 Frame rate: 12 FPS Mode: Day Output format: MJPEG

Figure 3 Proposed source of the collected traffic data

The textual data will be formatted, archived and steganographically integrated with the carrier image. The text and image date are spatiotemporally synchronized and form a combined source of traffic data. The text file will be copied *n* times in order to simulate higher amount of steganographically processed data in experiments.

2.2 Advantages and Limitations of SteganographicProcessing

Advantages of steganographic integration of traffic-relevant data within the steganogram structure:

- all relevant data are contained within the surveillance video recording, which facilitates and accelerates the situation analysis;
- memory occupancy of the combined set of data is not a mathematical sum of all the memory usage of transfer and integrated data;
- possibility of integration of the digital recording of data regardless of their type and content;
- use of cryptographic mechanism in order to increase authenticity and credibility of data;
- transfer of security sensitive information by forming of "concealed" communication sub-channels by using parts of the headers of TCP/IP (Transmission Control Protocol/Internet Protocol) datagram;
- the steganographic integration of data can be performed within specialised components within the surveillance video camera, reducing the possibility of unauthorised access and data manipulation;
- the system can be designed by using FPGA (Field Programmable Gate Array) – programmable architecture set, which enables fast operation with subsequent upgrade of the system, and
- their authenticity, integrity and credibility can be precisely defined.

Limitations of steganographic integration of traffic-relevant data within steganogram structure:

- sensitivity to manipulation by the content of transfer file, which can lead to destruction of integrated data;
- a large number of different algorithms that differently treat transfer and integrated data;
- it is not possible to steganographically integrate large quantities of data without effects on the quality of presentation or the size of the transfer file;
- implementation of the system of steganographic integration requires installation and configuration of additional equipment at the location;
- sensitivity of steganographically processed data to manipulation of the steganogram content;
- during work on some devices or equipment for data collection there may come to problems that can be manifested as difficult work or outage. Then the required data fail to be integrated within the recording, and
- by studying the available literature, publications and on-line sources of data, relatively few papers can be found that combine the topics of steganographic integration, use of surveillance video and traffic sciences.

2.3 Selection of Steganographic Algorithm

Out of a multitude of available steganographic tools, the paper uses F5 steganographic algorithm developed by the author *Andreas Westfeld*, [9]. Steganographic algorithm F5 was developed within the academic community based on the previous versions F3 and F4, [3] by implementation of the significant improvements. F5 algorithm can use the so-called steganographic key, but its use in the steganographic processing is not obligatory. The key is entered in the command line as password. In case it is indicated, it has to be indicated for steganographic extraction of data. Without knowing it, it is impossible to extract data. F5 algorithm has shown high resistance to statistical attacks and procedures of steganoanalysis [3]. The selected algorithm tends to change the minimal number of bits by using matrix encoding as a measure of efficiency the value of the number of inserted bits per change is used. The proposed algorithm takes into consideration the uniform dispersion of integrated data within the steganogram by using the method of permutation straddling. The source code of steganographic algorithm is written in Java, [12]. Once written, the source code will be a translated set of instructions, so-called Java bytecode which will be realised within VM - Java Virtual Machine. This ensures successful performance of application on every platform on which the Java Virtual Machine has been developed.

It should be emphasised that steganographic algorithm F5 is applicable on static, independent image recordings. Video recording can be observed as a series of independent image recordings that are sequentially connected by software tools (coders), optimised and connected into a series of recordings that a human eye, due to its inertia, perceives as a video recording. The work uses independent image recordings that can be observed as frames of the surveillance video.

3 STATISTICAL PROPERTIES OF PROCESSED DATA

Based on the analysis of available scientific and technical literature it can be concluded that the authors of papers have been focused on the issues of detection of the used steganographic algorithm and detection of the integrated message, [3, 4]. In the presented paper the emphasis is on the preservation of the quality of image recording because it is known that the data are integrated and there is no need for proof.

Table 1 Frame statistical properties (JPEG, RGBI components) [13]

1st group of the array statistical properties	
Absolute Difference	Root Mean Square
Histogram	Stand. Deviation
Mod	Variance
Min / Max	Median
Mean	Entropy
2nd group of the array statistical properties	
Arrays comparison	Mean Abs. Error (MAE)
Correlation and Cross-Correl.	Sum Absolute Error (SAE)
Maximum Abs. Diff. (MAD)	Sum Squared Error (SSE)
Mean Square Error (MSE)	Peak Signal Noise Ratio

For every matrix representing the values of RGB (R:*Red*, G:*Green*, B:*Blue*) components and image intensity, it is necessary, by using the applications MATLAB and *Simulink*, [13] to calculate the statistical properties. In Tab. 1 there are three groups of observed statistical properties of RGBI components: statistical properties of matrix recording, relation of the values of matrix recordings of original and steganographically processed image and the values of mutual deviations. The model, according to which the statistical properties in applications MATLAB and *Simulink* are calculated, is presented in Fig. 4.

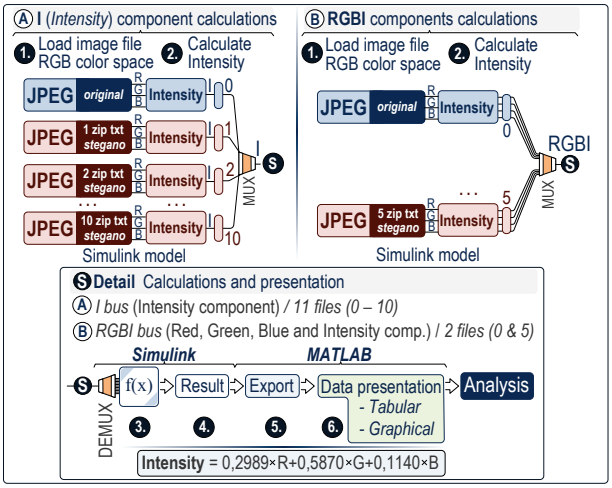

Figure 4 MATLAB / Simulink model for testing statistical properties

The calculation of the statistical properties is performed through experiments that can be divided into three main phases: selection and preparation of data, steganographic processing (integration and extraction) and calculation of statistical properties and comparison of integrated data before and after processing [14, 15].

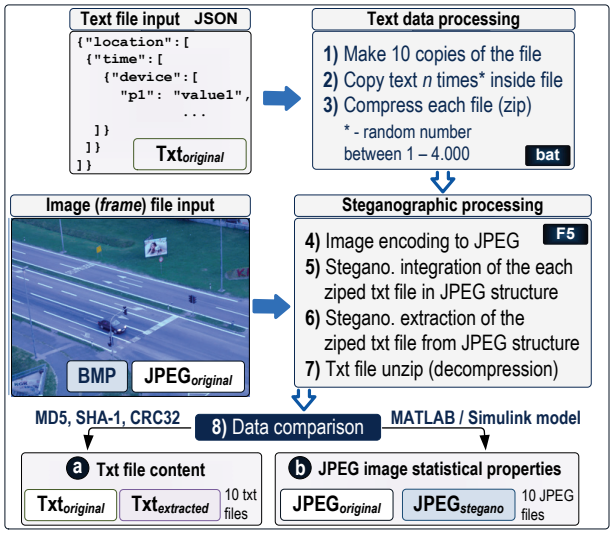

Figure 5 Preparation of texts and video frames for experiments

The phases of preparing the text and steganogram are presented in Fig. 5. Experimental procedures should prove the hypotheses that steganographical processing:

- does not degrade the quality of transfer data (or steganograms) in the measure that can be perceived by a healthy human sense of vision;
- transfer files retain the function of visual representation of the condition on the road before and after the procedure of steganographic integration and extraction of data;
- change of statistical properties of transfer data depends on the quantity of integrated data. It is necessary to study the change of statistical properties as indicator of change in visual quality over steganographically the video frames processed with minimal and maximal quantity of integrated data;
- steganographic integration, storage, transfer of transfer data and extraction of collected data does not change their contents in the least. The data before integration and after extraction have to be completely identical in content, structure and memory usage, and
- the possibility of detecting the manipulation of content over steganographically processed data. It is necessary to examine the influence of content manipulation of transfer file to integrated data.

Table 2 Data size (kB), resolution and number of colours

Text and archived file size (kB)					
File	Txt	Zip	File	Txt	Zip
Zip1	6,94	1,03	Zip6	4 594,56	29,83
Zip2	229,03	2,46	Zip7	4 890,68	31,67
Zip3	1 131,29	8,11	Zip8	5 809,14	37,43
Zip4	1 172,93	8,38	Zip9	7 590,51	48,60
Zip5	3 703,87	24,25	Zip10	9 249,27	59,00
JPEG image properties: resolution: 1024 × 768 (786 432 px)					
File Name	Morning	Noon	Evening	Night	
Size [kB]	490,32	633,19	532,23	465,03	
No. of col.	91 179	97 841	47 193	81 113	

The data that are used in the experiments are JPEG compressed (or original recording) and steganographically processed JPEG recording (both recordings have identical content). The recordings

recorded on identical locations at different periods of day (morning, noon, evening and night) are used.

The collected data are stored in the textual file. In order to simulate a larger amount of data the data are copied from 2 to 4,000 times by random selection of ten values. The data are compressed in ZIP format, [16] before the steganographic integration procedure. The amount of textual and image data is presented in Tab. 2. During the experiment the influence of steganographic processing on uncompressed and compressed textual data has been analysed.

3.1 Influence of SteganographicProcessing on Integrated Data

As proof that after the steganographic integration and extraction procedure the content of textual data has not been changed the following has been used:

- cryptographic function MD5, [17] (*Message-Digest Algorithm* 5) in the length of 128 bits;
- cryptographic function SHA – 1, [18] (*Secure Hash Algorithm*) in the length of 160 bits, and
- polynomial function CRC-32, [19] (*Cyclic Redundancy Check*) in the length of 32 bits.

Apart from the content the memory usage of uncompressed and compressed textual recordings has been studied. The analysis of results proves without doubt that the textual data during the steganographic processing have not been changed regarding content or memory usage. In the following experiment, presented in Fig.6, the influence of content manipulation of transfer JPEG file on the steganographically integrated text has been studied.

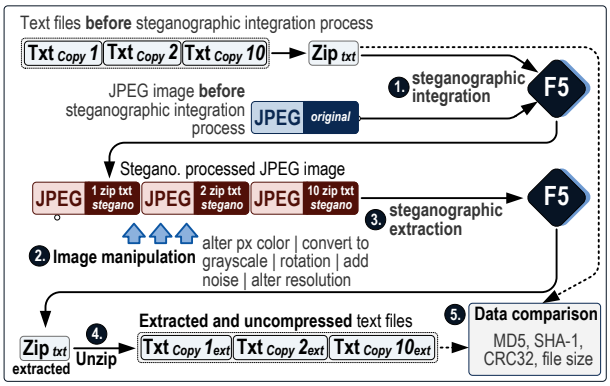

Figure 6 Testing of influence of change of content of image recording on steganographically integrated data

Regardless of the method or scope of JPEG processing, the integrated data were destroyed. The steganographic processing is very sensitive to content manipulation and may represent an additional indicator that there has been manipulation over the content.

3.2 Statistical Properties of Pixel Intensity

The lighting intensity of the road pixel (presented in Fig. 8) is connected with the time of recording. With the analysis of the values of statistical characteristics a very "mild" change of the values can be noted between different video frames.

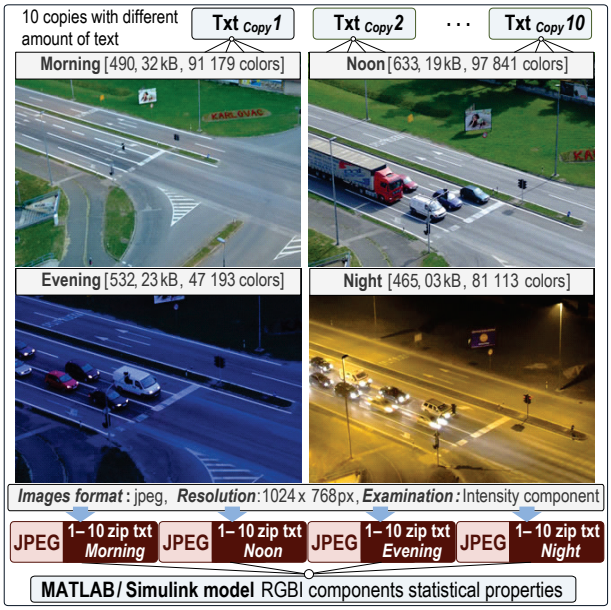

Figure 7 Preparation of image recordings and text data for analysis [14]

Regardless of the time of recording (different intensity and colours) the difference between the statistical values is very small regardless of whether it concerns the frames with minimal and maximal amount of integrated data. Fig. 7 presents the procedure of preparing textual and image recordings for the experiment of testing the change in lighting intensity.

Table 3 Original and steganograpically processed JPEG array statistical properties comparison (1st group)

Value	Morning		Noon	
	JPEG	Steg_avg	JPEG	Steg_avg
Mod	135,000	135,000	158,000	157,900
Min	8,000	8,100	5,000	5,000
Max	252,000	252,000	255,000	255,000
Avg	116,000	116,000	105,813	105,813
RMS	121,408	121,403	117,713	117,708
StdDev	35,802	35,788	51,490	51,478
Var	3 817,000	3 815,600	2 933,000	2 932,100
Med	122,000	122,000	101,000	101,000
Ent	6,982	6,981	7,451	7,450
Value	Evening		Night	
	JPEG	Steg_avg	JPEG	Steg_avg
Mod	19,000	19,300	4,000	4,000
Min	1,000	1,000	0,000	0,000
Max	255,000	255,000	255,000	255,000
Avg	45,313	45,313	86,688	86,688
RMS	53,454	53,446	104,636	104,630
StdDev	28,300	28,286	58,533	58,525
Var	2 857,000	2 856,000	25,000	24,200
Med	44,000	44,000	95,000	95,000
Ent	6,364	6,361	7,491	7,488

JPEG: Original image (*keyframe*), *Steg_avg*: Average value of the stegano. processed images (iteration 1×-10×), *Min*: 2-D Minimum, *Max*: 2-D Maximum, *Avg*: 2-D Mean, *RMS*: Root Mean Square, *StdDev*: 2-D Standard Deviation, *Var*: 2-D Variance, *Med*: Median, *Ent*: Entropy

Tabs. 3 and 4 show the relation of statistical properties of lighting intensity of the original JPEG recording and the amount of average value of the lighting intensity of all steganographically processed files (*Stegano*_1×-10×) for both groups of statistical properties.

Table 4 Original and steganograpically processed JPEG array statistical properties comparison (2nd group)

Value	Morning	Noon	Evening	Night
	JPG/Stg	JPG/Stg	JPG/Stg	JPG/Stg
PSNR	51,536	51,867	51,599	51,411
Corr2	0,999	0,999	0,999	0,999
Xcorr2	0,999	0,999	0,999	0,999
MAD	4,000	4,000	4,000	4,000
MAE	0,001	0,001	0,001	0,001
MSE	0,000	0,000	0,000	0,000
SAE	1291,168	1188,701	1272,513	1317,219
SSE	5,520	5,116	5,441	5,681

JPG: Original image (*keyframe*), *Stg*: Value of the stegano. processed image (10th iteration), *PSNR*: Peak Signal-to-Noise Ratio, *Corr2*: 2-D Correlation, *Xcorr2*: 2-D Cross-Correlation, *MAD*: Maximum Absolute Difference, *MAE*: Mean Absolute Error, *MSE*: Mean Square Error, *SAE*: Sum Absolute Error, *SSE*: Sum Squared Error

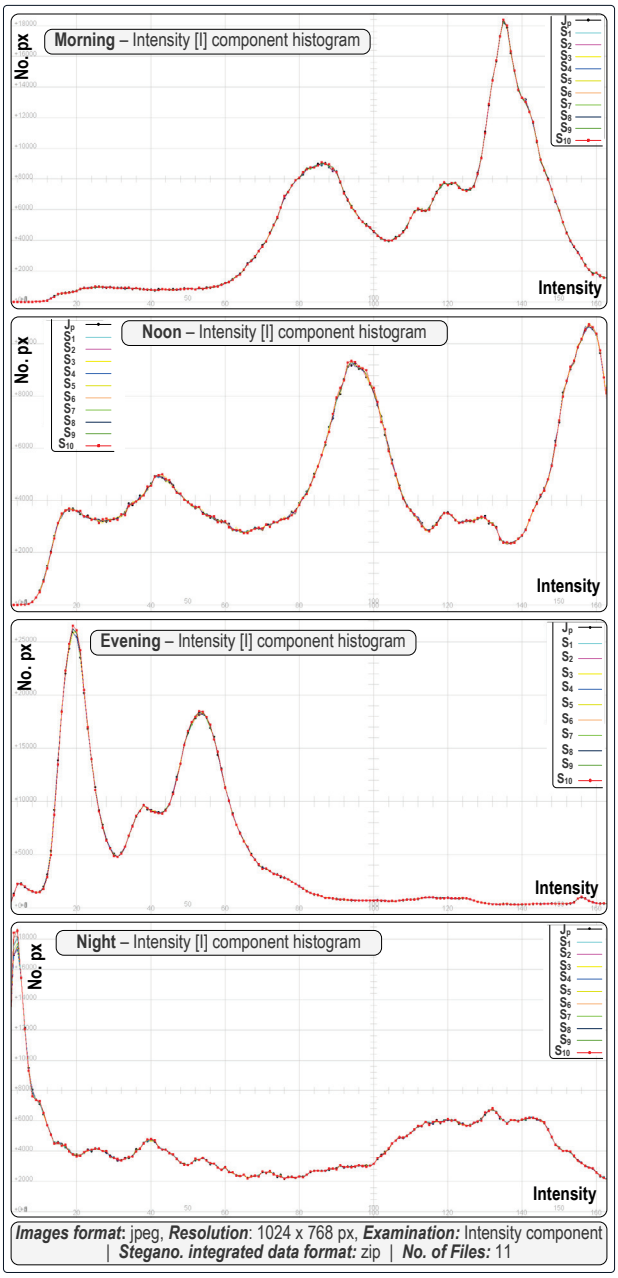

Figure 8 Histograms of intensity component for various amounts of steganographic integrated data

Both tables show very small difference of the values of original and steganographically processed recordings. Based on the presented results it may be concluded that the steganographic processing changes the statistical properties, i.e. content of the image recording to a very small extent. Visual inspection only confirms the mentioned conclusion since the changes are invisible to the human eye.

It is obvious that the histograms of lighting intensity (*I*), presented in Fig. 8, for various amounts of integrated data ($S_{1\text{-}10}$) differ to a very small measure which confirms the thesis that the quality of steganogram is preserved and that the changes are invisible to the human eye.

3.3 Statistical Properties of RGB Components

The analysis of statistical characteristics of RGBI components of JPEG compressed and steganographically processed image recording which have been recorded in different lighting conditions confirms the results of previous analyses – values of statistical characteristics are very close, and in some cases identical (Tabs. 5 and 6). During testing the recording with medium amount of integrated data (*Stegano_5×*) was used. Tab. 5 shows the absolute difference of statistical properties of the values of RGBI components of original JPEG recording and steganographically processed files (*Stegano_5×*) for the first group of statistical properties. As in the previous case, one can conclude that steganographic processing changes the statistical properties, i.e. the content of the image recording to a very small extent and is capable of maintaining the statistical properties for every single component.

Visual inspection of the steganographically processed image (pixel intensity and image texture quality) additionally supports the mentioned conclusion since it is not possible to observe any visual changes in the content of the steganographically processed image recording.

3.4 Visual Quality of the Processed Data

Absolute difference of the change in the pixel lighting intensity between JPEG and steganographically processed JPEG image recording shows how the steganographic integrated message is distributed within the data carrier [14, 15]. By increasing the amount of integrated data the object contours can be more obvious. Fig. 9 shows the graphical presentation of the absolute difference in the frame lighting intensity.

By achieving the limit of steganographic capacity of 13.00 % of the frame memory usage, the graphical image shows a very large number of pixels which detect the change in intensity. The quantity of pixels with changed lighting intensity for recording recorded during night amounts to 19.27 %, and for the recording recorded during afternoon it is 17.56 %. For ease of reference the road contours have been drawn. Steganographic processing inevitably leads to a change in the quality of the image recording presentation. The basic question is to what extent there has come to a change and whether the observer can notice it. In case the change in quality is visible, then the visual information is worthless and the concept of steganographic processing is not applicable.

Table 5 Original and steganographically processed JPEG - absolute difference between arrays for RGBI components(1st group statistical properties)

Value	ΔMod	ΔMin	ΔMax	ΔAvg	ΔRMS	ΔStdDev	ΔVar	ΔMed	ΔEnt
Mo-$R_{jpg-steg}$	1,000	0,000	0,000	0,000	0,012	0,004	1,000	0,000	0,001
Mo-$G_{jpg-steg}$	0,000	1,000	0,000	0,000	0,016	0,004	1,000	0,000	0,001
Mo-$B_{jpg-steg}$	0,000	0,000	0,000	0,018	0,004	1,000	0,000	0,001	0,000
Mo-$I_{jpg-steg}$	0,000	0,000	1,000	0,000	0,012	0,003	1,000	0,000	0,001
No-$R_{jpg-steg}$	0,000	0,000	0,000	0,000	0,013	0,003	0,000	0,000	0,000
No-$G_{jpg-steg}$	0,000	0,000	0,000	0,000	0,011	0,006	1,000	0,000	0,000
No-$B_{jpg-steg}$	1,000	0,000	0,000	0,000	0,010	0,003	0,000	0,000	0,001
No-$I_{jpg-steg}$	0,000	0,000	0,000	0,000	0,009	0,004	1,000	0,000	0,001
Ev-$R_{jpg-steg}$	0,000	0,000	0,000	0,000	0,003	0,001	0,000	0,000	0,004
Ev-$G_{jpg-steg}$	0,000	0,000	0,000	0,000	0,019	0,011	1,000	0,000	0,003
Ev-$B_{jpg-steg}$	0,000	0,000	0,000	0,000	0,021	0,008	1,000	0,000	0,004
Ev-$I_{jpg-steg}$	0,000	0,000	0,000	0,000	0,012	0,006	1,000	0,000	0,003
Ni-$R_{jpg-steg}$	0,000	0,000	0,000	0,000	0,011	0,005	1,000	0,000	0,001
Ni-$G_{jpg-steg}$	0,000	0,000	0,000	0,000	0,007	0,004	0,000	0,000	0,001
Ni-$B_{jpg-steg}$	0,000	0,000	0,000	0,000	0,010	0,007	0,000	1,000	0,001
Ni-$I_{jpg-steg}$	0,000	0,000	0,000	0,000	0,007	0,004	0,000	0,000	0,002

Mo-$R_{jpg-steg}$: Absolute difference between JPEG ($RGBI_{jpg}$) and steganographically processed image ($RGBI_{steg}$) values (*R*: Red, *G*: Green, *B*: Blue, *I*: Intensity components). Image taken in *Mo*: Morning, *No*: Noon, *Ev*: Evening and *Ni*: Night. Values: *Min*: 2-D Minimum, *Max*: 2-D Maximum, *Avg*: 2-D Mean, *RMS*: Root Mean Square, *StdDev*: 2-D Standard Deviation, *Var*: 2-D Variance, *Med*: Median, *Ent*: Entropy

Table 6 Original and steganographicallyprocessed JPEG - absolute difference between arrays for RGBI components

Value	PSNR	Corr2	Xcorr2	MAD	MAE	MSE	SAE	SSE
Mo-$R_{jpg/steg}$	50,403	0,999822	0,999974	4,000	0,002	0,000	1279,196	7,167
Mo-$G_{jpg/setg}$	52,238	0,999813	0,999988	4,000	0,001	0,000	1064,188	4,698
Mo-$B_{jpg/steg}$	49,344	0,999844	0,999978	5,000	0,002	0,000	1432,000	9,146
Mo-$I_{jpg/steg}$	54,753	0,999915	0,999993	2,000	0,001	0,000	668,251	2,633
No-$R_{jpg/steg}$	51,168	0,999917	0,999979	4,000	0,001	0,000	1095,004	6,010
No-$G_{jpg/steg}$	52,833	0,999932	0,999989	3,000	0,001	0,000	936,620	4,096
No-$B_{jpg/setg}$	49,893	0,999908	0,999977	5,000	0,002	0,000	1268,239	8,061
No-$I_{jpg/steg}$	55,281	0,999964	0,999993	2,000	0,001	0,000	592,337	2,331
Ev-$R_{jpg/steg}$	50,610	0,999522	0,999782	4,000	0,002	0,000	1238,043	6,834
Ev-$G_{jpg/steg}$	52,316	0,999742	0,999930	3,000	0,001	0,000	1048,075	4,613
Ev-$B_{jpg/steg}$	49,152	0,999853	0,999969	5,000	0,002	0,000	1474,898	9,560
Ev-$I_{jpg/steg}$	54,763	0,999864	0,999962	2,000	0,001	0,000	666,576	2,627
Ni-$R_{jpg/steg}$	51,131	0,999949	0,999986	4,000	0,001	0,000	1135,129	6,061
Ni-$G_{jpg/steg}$	52,467	0,999947	0,999982	3,000	0,001	0,000	1019,141	4,456
Ni-$B_{jpg/steg}$	49,720	0,999782	0,999856	5,000	0,002	0,000	1332,627	8,388
Ni-$I_{jpg/steg}$	54,648	0,999967	0,999990	3,000	0,001	0,000	682,243	2,697

Mo-$R_{jpg/steg}$: Relationship between JPEG ($RGBI_{jpg}$) and steganographically processed image ($RGBI_{steg}$) values (*R*: Red, *G*: Green, *B*: Blue, *I*: Intensity components). Image taken in *Mo*: Morning, *No*: Noon, *Ev*: Evening and *Ni*: Night. Values: *PSNR*: Peak Signal-to-Noise Ratio, *Corr2*: 2-D Correlation, *Xcorr2*: 2-D Cross-Correlation, *MAD*: Maximum Absolute Difference, *MAE*: Mean Absolute Error, *MSE*: Mean Square Error, *SAE*: Sum Absolute Error, *SSE*: Sum Squared Error

Visual detection of the change or presence of information is not desirable because:

- steganographic processing is primarily a method of data security and protection. The observer who has no right of access or is not interested in additional information, perceives the steganographically processed recording as a "usual" surveillance video;
- the occurrence of processed parts of the image (as result of steganographic processing) can suggest to the observer that the image shows a part or contour of a facility or it may eliminate details that are necessary for better understanding of the traffic situation;
- the observer's eye finds obvious the phenomenon of content manipulation or loss of detail in visual presentation which reduces the credibility of the surveillance video since it is impossible to conclude whether a certain detail is a result of actual condition or a product of steganographic processing, and
- computer detection and forensic investigations of tiny details, lines, textures or contours of facilities in the image cannot provide precise answers whether it is an actual situation or patterns of steganographic processing.

By magnifying certain parts of steganographically processed image and original JPEG image and by comparison of RGB values one can acquire insight into the intensity of change (Fig. 10).

In the experiment the detail of the magnified part with the licence plate on a car is used, before and after the steganographic processing. Fig. 11 shows how the differences between the values of RGB components are very small and difficult to notice (by human eye).

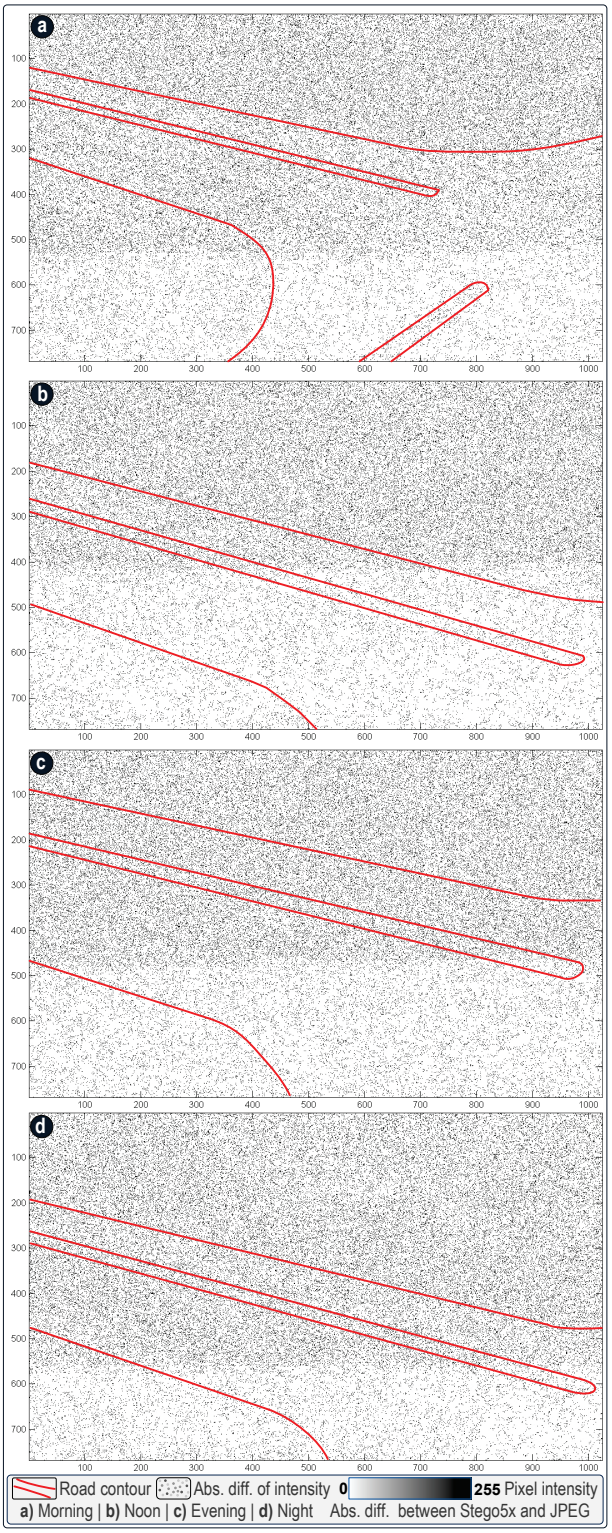

Figure 9 Graphical presentation of absolute value of frame lighting intensity difference

The example clearly shows that steganographical integration of data affects the visual quality of the video frames to an extent which cannot be noticed by human eye. In the example in Fig. 11 even with a high magnification, the differences, if they exist, are difficult to notice. Performing the experiment in all images (recorded at different parts of the day) provides the final answer that steganographic integration is capable of steganographically integrating the data without any visible deformation of the content of the image recording, and the integrated data do not change in the least.

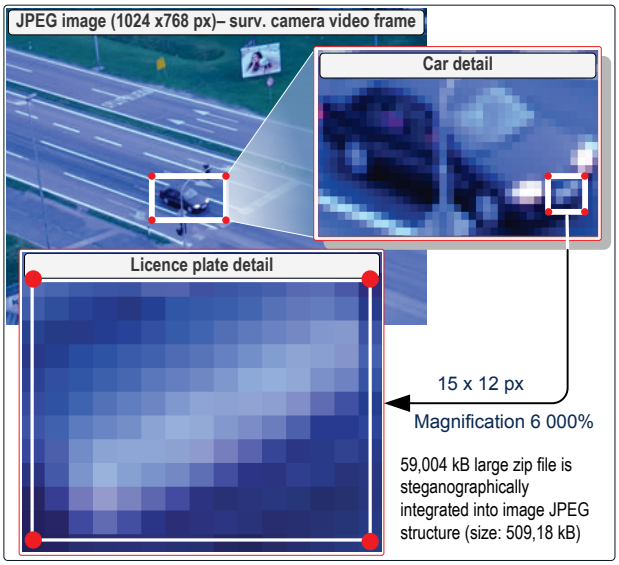

Figure 10 Magnification of details of steganographicallyprocessed JPEG recording

4 CONCLUSION

The paper has presented the procedure of steganographic integration of the traffic-relevant data within the surveillance video frame structure. The procedure has to satisfy two basic criteria: primary condition is that the data before and after steganographic integration have to be completely identical. The secondary condition is that the change in the surveillance video frame structure is invisible to the human eye. An additional condition is that the integrated data have to have a structure which can be easily and fast presented or saved in the database.

As proof of fulfilling the two given basic criteria, the experiments were carried out on integrated text and steganographically processed image recording (in the role of a frame of the surveillance video). The steganographical algorithm F5 has been used to integrate different quantity of compressed textual files into image recordings recorded in different conditions. The application of hash function over textual data before and after the steganographic processing has proven the primary condition – the content, structure and memory usage of data are completely identical. The experiments studied the influence of the change of content of the transfer image recording on integrated data. It has been proven that steganographically integrated data would be destroyed regardless of the method or scope of the image recording change.

With the formation of the model, the calculations and analysis (two groups) of statistical characteristics of the image recording, very small deviations have been determined which prove the secondary condition – intensity of lighting and textures of transfer data have been changed to such an extent that it is invisible for the human eye. A proportional relation has been detected between the amount of integrated data and the change in statistical characteristics, but if the integrated amount of data is below the steganographic capacity of the transfer

image recording, the change of statistical characteristics is very low. Visual inspection of image recordings has confirmed the previous hypothesis and no changes in details, texture or lighting have been noticed in image recordings.

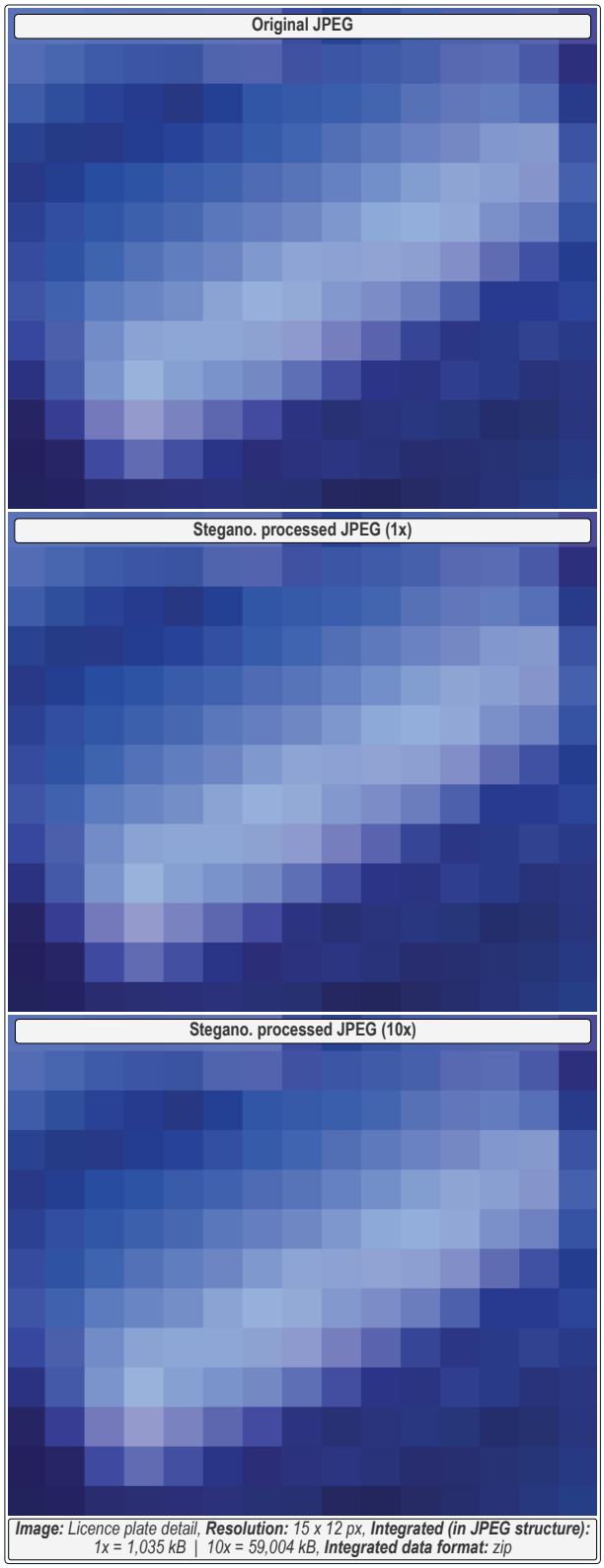

Figure 11 Comparison of visual quality of original and steganographically processed JPEG recording

The main hypothesis of the paper has been confirmed; the steganographic processing of data represents a suitable method with the aim of forming an independent and combined source of traffic-relevant information on the road condition. The use of mechanisms of cryptographic protection and infrastructure of the public key the data are ensured integrity, authenticity and credibility.

The topic of future research will be the usage of steganographic processing within the structure of the compressed video recording. The gathered and steganographically processed data would be within an independent data flow or within the intra-frame. It is necessary to examine the influence of the steganographic processing on the structure, quality and memory usage of the compressed video recording.

5 REFERENCES

[1] Katzenbeisser, S. & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*, Artech House, Boston, USA.

[2] Judaš, M. & Kostović, I. (1997). *Temelji neuroznanosti - slušni i vestibularni sustav, Temelji neuroznanosti - fiziologija oka i fototransdukcije*, 1. izdanje, MD, Zagreb, (Croatian language).

[3] Westfeld, A. (2001). F5 - A steganographic algorithm: High capacity despite better steganalysis, *Ira S. Moskowitz (Hrsg.): Information Hiding. 4th International Workshop, IH'01*, Pittsburgh, USA, 289-302. https://doi.org/10.1007/3-540-45496-9_21

[4] Kharrazi, M., Sencar, H. T. & Memon, N. (2004). *Image steganography: Concepts and practice*, WSPC / Lecture Notes, Polytechnic University, Brooklyn, New York.

[5] Curran, K. & Bailey, K. (2003). An evaluation of image based steganography methods. *International Journal of Digital Evidence, 2*(2).

[6] Cole, E. (2003). *Hiding in plain sight: Steganography and the art of covert communication*, Wiley Publishing, Inc., Indianapolis, Indiana.

[7] Murdoch, S. J. & Lewis, S. (2005). Embedding covert channels into TCP/IP. *Information hiding international workshop, no. 7, vol. 3727*, Barcelona, Spain. https://doi.org/10.1007/11558859_19

[8] Mazurczyk, W. & Kotulski, Z. (2006). New security and control protocol for VoIP based on steganography and digital watermarking. *Annales UMCS Informatica*, Lublin-Polonia, Sectio AI, 417-426.

[9] Carvalho, D. F., Chies, R. & Rudinei G. (2008). MP4Stego: esteganografiaemvídeos MPEG-4. *Proceedings of the 14th Brazilian Symposium on Multimedia and the Web*, Vila Velha, Brazil, October 26-29. https://doi.org/10.1145/1666091.1666118

[10] Sherly, A. P. & Amritha, P. P. (2010). A Compressed Video Steganography using TPVD. *International Journal of Database Management Systems (IJDMS), 2*(3).

[11] Andreas Westfeld, http://www2.htw-dresden.de/~westfeld/ (20.12.2015)

[12] Java Help Center, http://www.java.com/en/download/help/index.xml (20.12.2015)

[13] Math Works Inc. MATLAB and Simulink user documentation, http://www.mathworks.com/help/index.html (20.12.2015)

[14] Stančić, A. (2013). Steganographic Integration of the Collected Data within Transportation System, *Ph.D. thesis*, University of Zagreb, Faculty of Transport and Traffic Sciences, Zagreb, Croatia.

[15] Gonzalez, R. C., Woods, R. E. & Eddins, S. L. (2003). *Digital image processing using MATLAB*, Prentice-Hall, Inc.

[16] ZIP archive, http://web.archive.org/web/20030702014023/http://pkware.com/products/enterprise/white_papers/appnote.html (20.12.2015)
[17] The MD5 Message-Digest Algorithm, Network Working Group, Request for Comments 1321, April 1992, https://www.ietf.org/rfc/rfc1321.txt (19.11.2015)
[18] Paar, A. & Petzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer-Verlag, Berlin Heidelberg, Germany. https://doi.org/10.1007/978-3-642-04101-3
[19] Williams, R. N. (1993). *A Painless Guide to CRC Error Detection Algorithms*, Rocksoft Pty Ltd., Adelaide, Australia. http://www.ross.net/crc/download/crc_v3.txt (20.12.2015)

Contact information:

Adam STANČIĆ, PhD
Karlovac University of Applied Sciences
Department of Mechanical Engineering
Ivana Meštrovića 10, 47000 Karlovac, Croatia
E-mail: adam.stancic@vuka.hr

Ivan GRGUREVIĆ, PhD
University of Zagreb
Faculty of Transport and Traffic Sciences
Department of Information and Communications Traffic
Vukelićeva 4, 10000 Zagreb, Croatia
E-mail: ivan.grgurevic@fpz.hr

Zvonko KAVRAN, PhD
University of Zagreb
Faculty of Transport and Traffic Sciences
Vukelićeva 4, 10000 Zagreb, Croatia
E-mail: zvonko.kavran@fpz.hr