ADAM STANČIĆ, Ph.D.[1]
E-mail: adam.stancic@vuka.hr
IVAN GRGUREVIĆ, Ph.D.[2]
E-mail: ivan.grgurevic@fpz.hr
(Corresponding author)
ZVONKO KAVRAN, Ph.D.[2]
E-mail: zvonko.kavran@fpz.hr
[1] Karlovac University of Applied Sciences
Meštrovićeva 10, 47000 Karlovac, Croatia
[2] University of Zagreb,
Faculty of Transport and Traffic Sciences
Vukelićeva 4, 10000 Zagreb, Croatia

Intelligent Transport Systems (ITS)
Preliminary Communication
Submitted: Mar. 29, 2016
Accepted: Sep. 21, 2016

INTEGRATION OF TRANSPORT-RELEVANT DATA WITHIN IMAGE RECORD OF THE SURVEILLANCE SYSTEM

ABSTRACT

Integration of the collected information on the road within the image recorded by the surveillance system forms a unified source of transport-relevant data about the supervised situation. The basic assumption is that the procedure of integration changes the image to the extent that is invisible to the human eye, and the integrated data keep identical content. This assumption has been proven by studying the statistical properties of the image and integrated data using mathematical model modelled in the programming language Python using the combinations of the functions of additional libraries (OpenCV, NumPy, SciPy and Matplotlib). The model has been used to compare the input methods of meta-data and methods of steganographic integration by correcting the coefficients of Discrete Cosine Transform JPEG compressed image. For the procedures of steganographic data processing the steganographic algorithm F5 was used. The review paper analyses the advantages and drawbacks of the integration methods and present the examples of situations in traffic in which the formed unified sources of transport-relevant information could be used.

KEY WORDS

integration; intelligent transport system; meta-data; surveillance system; steganography;

1. INTRODUCTION

Modern technical means enable fast and reliable collection, processing and integration of data into the unified source of all the collected information about the supervised situation. Regarding the format, the collected transport-relevant data can be divided into two groups: the first group are analytic data recorded in the form of structured textual recording and the second group of visual data, which is represented by image (or video) recordings. The procedure of integration of the analytic data within the structure of visual data and the usage of cryptographic security measures represent suitable methods in the process of forming a unified source of transport-relevant data. Integration of data can be observed as encapsulation of the collected data within one, for this purpose suitable set of data. The review paper will present the possibilities of integrating textual data into the image.

All transport-relevant data are merged into a unique authentic source of information and facilitate the analysis of the condition of a part of the transport system. Regardless of the technical means which are used to perform the integration and extraction of data, there must be absolutely no change in the content of integrated (analytical) data, not in the least. Depending on the method of integration, the transfer image can be partly changed either in content or in the memory usage. The change has to be performed to such an extent that the human eye cannot notice it and that it keeps its primary property – visual presentation of the condition on the supervised location.

The input methods of meta-data and steganographic processing in the available scientific and research literature were not observed in the context of information integration that apart from information about image would contain information about immediate environment in which the record has been recorded (excluding the information on location). The input methods of meta-data in the image are primarily intended for the description of characteristics and partly the description of the image content [1, 2, 3, 4]. The primary purpose of the steganographic methods is hiding of data within the image whose banal content has the task to “distract” the observer from the integrated data [5, 6, 7, 8, 9]. The presented review paper differs from other available scientific-research papers (dealing with the topic of steganography) because additional attention has been paid to the images. Their visual content contains valuable information for transport experts during analysis of the observed situation on the road and it is not limited to the role of transfer of integrated information. Through the discussion on the title topic of the research review paper in the following sections the methods will be presented, their influence on the data, advantages and drawbacks and examples how transport experts can use them while analysing the transport situations particularly in case of the law enforcement activities. It should be emphasized that the steganographic processing is not strictly applicable to transportation and traffic technology only nor to image files as the embedded content carrier. Steganography techniques can be applied to any kind of digitally stored data. Due to the fact that image, audio, text and video files possess redundant structure and content they represent suitable medium for steganographic processing [5, 7].

2. RESEARCH OBJECTIVE

The primary objective of data integration is the formation of unified, authentic and credible source of transport-relevant information about the situation on the road and its environment. The transport experts would have available the visual presentation of the situation (image) within which there are measured and collected data from the measuring devices and sensors on the road. Through research work it is necessary to answer the following questions: to which extent can the integration procedure affect the structure of the image, which format and which quantity of data can be integrated and finally, how does the procedure affect the structure of integrated data. Only after having answered these questions adequate method of integration needs to be proposed.

The integration procedure must respect certain limitations: integrated data are not visible and the human eye cannot detect the change of the image content in the form of lighter and darker areas, deformations of contours or texture, ghost-samples in the image (French: moiré effect). Before integration and after extraction the integrated data have to be completely identical since these are collected analytical data whose value cannot and must not be changed, not in the least. During research one should consider also the security aspect so that the procedure ensures integrated data against unauthorized access and modification. The research work used adequate software support in order to study the characteristics of the image and integrated data. Ratnakirti and Suvamoy [10] propose the quality evaluation system of the steganographic algorithm based on the following parameters: security, capacity, imperceptibility and runtime performance. Evaluation method takes into account several steganographic algorithms divided into two groups: spatial domain and transform domain. According to the article, F5 [6] showed best performance among all the researched algorithms. F5 has high resistance to visual and statistical attacks, high embedding efficiency, high capacity and processing procedure is not complex and computational resources consuming. For the procedures of steganographic processing the steganographic algorithm F5 (f5r11) was used. Using the programming language Python (ver. 2.7.10) [11] and with combination of the functions of additional libraries OpenCV (ver. 3.1.0) [12], NumPy (ver. 1.10.4) [13], SciPy (ver. 0.17.0) [14] and Matplotlib (ver. 1.5.1) [15] the mathematical model was formed in order to use the analysis of results to answer the previously defined questions respecting the defined restrictions. F5 algorithm has been developed in three programming languages: primarily Java - this version was used in the presented research, Python [16] and C# [17]. It is also worth mentioning that F5 algorithm has been developed by A. Westfeld [18] within an academic community. Enhancements and algorithm code improvements did not stop so that in the last few years some authors have made modifications in order to increase the steganographic capacity [19], use algorithm in audio/video files [20] or use it in encoded video recordings [21].

3. TRANSFER AND INTEGRATED DATA

Data of different data sources collected at the same time, at the same place represent a joint set of data that describes the condition of the supervised part of intelligent transport system (ITS). In the concrete case, the collected data were divided into two groups: analytical (or measured) data in textual format and visual (or recorded) image data. Regardless of the source, form, group and structure, all the collected data share the identical space-time context, i.e. location and time interval in which they have been collected. Regardless of the space-time context, the used technical means and applied technologies of data collection and processing, the procedures of exchange, integration and processing of information have been standardized, the integration of supervised and identification data performed, the cryptographic protection implemented in order to ensure the integrity of data and the system of collecting, processing, storage, analysis and presentation of transport-relevant data has been organized.

Regarding the group of collected data (analytical or image) it is necessary to define the structure of data. The analytical data are recorded in the form of alpha-numerical characters stored in a textual file. The problem may be the heterogeneity of the system for data collection with the aspect of applied technical-technological solutions. The measurement instruments and sensors of different producers can have different characteristics and additional functionalities (although of identical purpose). Equally, the quality, structure and accuracy of the collected data of a certain instrument do not have to be identical with other instruments. In case of integration it is necessary to structure the collected data so as to ensure the possibility of extraction, import in the database, analysis or presentation. Although not necessary, the textual files can be compressed due to lower memory space usage and cryptographically processed because of data protection.

The image structure is defined primarily by applied compression mechanisms with or without loss of data. Higher degree of compression reduces the necessary memory resources, but affects directly the image quality. In case of using the compression without losses it is necessary to ensure significant computer resources that can process a large amount of images in a short period. The type of image is fundamentally determined by implemented surveillance system and computer support that can isolate a single image within the surveillance video. *Figure 1* shows the procedure of forming the unified source of information.

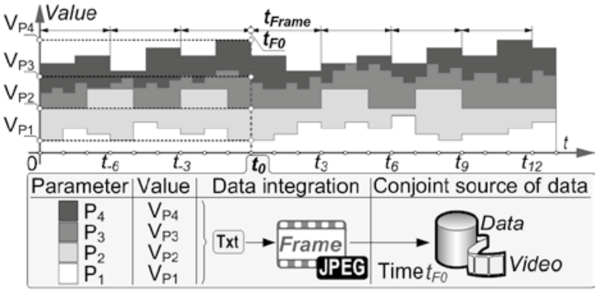


Figure 1 – Integration of collected data in the image

The integration procedure is performed by inputting the collected data on the condition of the supervised part of traffic infrastructure in the image file. Thus, the image data become transferable, and the collected (analytical) ones become integrated data. It should be emphasised that the integrated data should not be visible or degrade the image texture, or transfer data to the extent which is visible for the human eye. Integrated data have to be integrated in such a way that their content, structure and memory usage are not to be changed, not even in the slightest degree. In case of change it would not be possible to determine whether the integrated data have been really measured or an error occurred during the integration procedure. The integration procedure has to be performed in a manner that allows the extraction of integrated data in the appropriate format for subsequent analysis or presentation of data.

With the proposed procedure the traffic experts would have at their disposal a unified source of transport-relevant data which refer to a certain location in a certain time. The image data display visual situation whereas integrated collected data provide additional information about the measured transport-relevant parameters as presented in *Figure 2*.

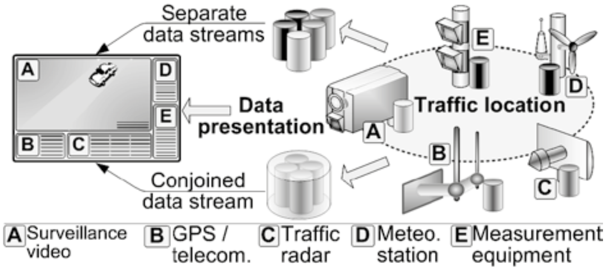


Figure 2 – Presentation of measured and visual data

In this way the need to collect, process and present each single source of information about the road condition would be avoided. The software support can enable the display of collected visual and analytical data in the desired format.

3.1 Procedure of data integration within image

Until today several standards for the integration of different descriptive, technical or administrative data within the image have been developed. The data are input as part of the meta-data or within the image structure. The input of meta-data is a well-known and often applied method which is used in different types of files, and it is best known for the use of image (and multimedia) records. The second method is the steganographic processing of files, and it proved most efficient precisely in case of image processing. With regard to the topic of research work the methods of inputting the collected data within JPEG image format [22] will be defined. According to JPEG standard, the image in its structure contains the so-called application segments each of which has been characterised by markers APPn (APP – Application) in which n represents numeric designation of the segment. Maximal memory usage of each segment amounts to 64 kb. JEITA (Japan Electronics and Information Technology Industries Association) developed in 1996 EXIF (Exchangeable Image File Format), [1]. EXIF is entered within APP1 segment in the form of textual data, i.e. meta-data which describe the image (author, time, and location of recording, camera parameters, etc.) and store a thumbnail image (Thumbnail). Information can be additionally stored in APP2 segment if additional multi-resolution images are used (FlashPix extensions). In 2001 the Adobe Company presented an extensible platform for meta-data XMP (Extensible Metadata Platform), [2] which became ISO standard in 2012, [3]. XMP record can be much richer with information about the image (records modifications and used tools on the original image). If integrated in JPEG the image format is stored in the APP1 segment without the possibility of extension. If SMP record is stored separately from the image then the memory usage has no limitations. Within the APP13 segment meta-data can be stored according to IPTC - IIM standard

(International Press and Telecommunications Council), [4]. The JPEG structure of the compressed image and the record segments within which it is possible to integrate the transport-relevant data is shown in *Figure 3* [1]:

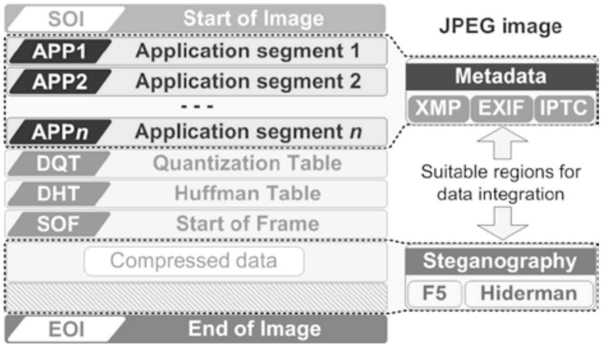


Figure 3 – JPEG image structure

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”, [5]. Steganography is a procedure of inserting a secret message within a “false” message which transfers information. 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 any unauthorized access additionally difficult and to eliminate repeating patterns in the data structure [6]. The previously mentioned false or transfer message has the function of transferring the inserted message to whom it has been intended and “distracts” the observer (from the inserted message) [7]. In the presented research work the steganographic processing is used as the integration procedure of analytic traffic relevant data within the structure of the transfer image file which in itself presents visual presentation of the situation on the road. In this case there are no “false” and “real” messages but rather integrated and transfer data have equal value as the source of transport-relevant information. Therefore, it is of utmost importance for the steganographic processing to change the image to such an extent which is invisible for the human eye, with the content of the integrated data remaining completely unchanged. As in the previous data integration method, the focus is on JPEG format of the image (or video) recording.

The methods of steganographic integration of data can be divided into: methods of Spatial Domain and methods of Transform Domain [10]. The method of Spatial Domain uses LSB (Least Significant Bit) in the recording of the image pixel colour. Methods of the Transform Domain modify 2-D DCT (2-Dimensional Discrete Cosine Transformation) coefficients of JPEG compressed recording. Both methods modify the very structure of the image recording and become its integral part. By modifying the DCT coefficients the position of integrated data in the image structure can be in the continuation of the basic JPEG structure or as its element. By adding integrated data after JPEG structure of the image has no influence on the image structure, but the memory usage of the processed image is the sum of the usage of image and integrated data. In case of integrating data within the JPEG structure there is impact on the image quality, but the influence on the memory usage is far lower and the message is better protected against unauthorized access.

Between the methods of spatial and transform domain there are essential differences [8, 9]. The methods of spatial domain are applied to non-compressed image contents such as BMP format (Bitmap). Visual changes are small with high capacity, statistical properties of the image are significantly changed, and the method is applicable only on some parts of the recording (because of the LSB value modification). The methods of transform domain are applied to the compressed image formats such as JPEG format. Modification of DCT coefficients affects the ratio of compression, they have lower capacity than the methods from spatial domain, but have significantly lower influence on the statistical characteristics of the image. *Figure 4* shows the procedure of the so-called Matrix Encoding which is used by F5 steganographic algorithm [6] in order to properly distribute the integrated data within the structure of the transfer image. Uniform distribution of integrated data inside the image structure is important for two reasons: avoidance of the visual distortion of image content and better security against attack from unauthorized user. Any kind of the visual distortion on the image may fool the viewer that the real object is recorded and disrupt conclusions related to the observed traffic situation.

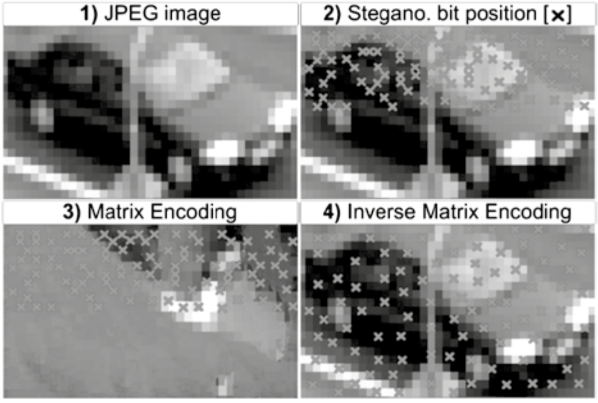
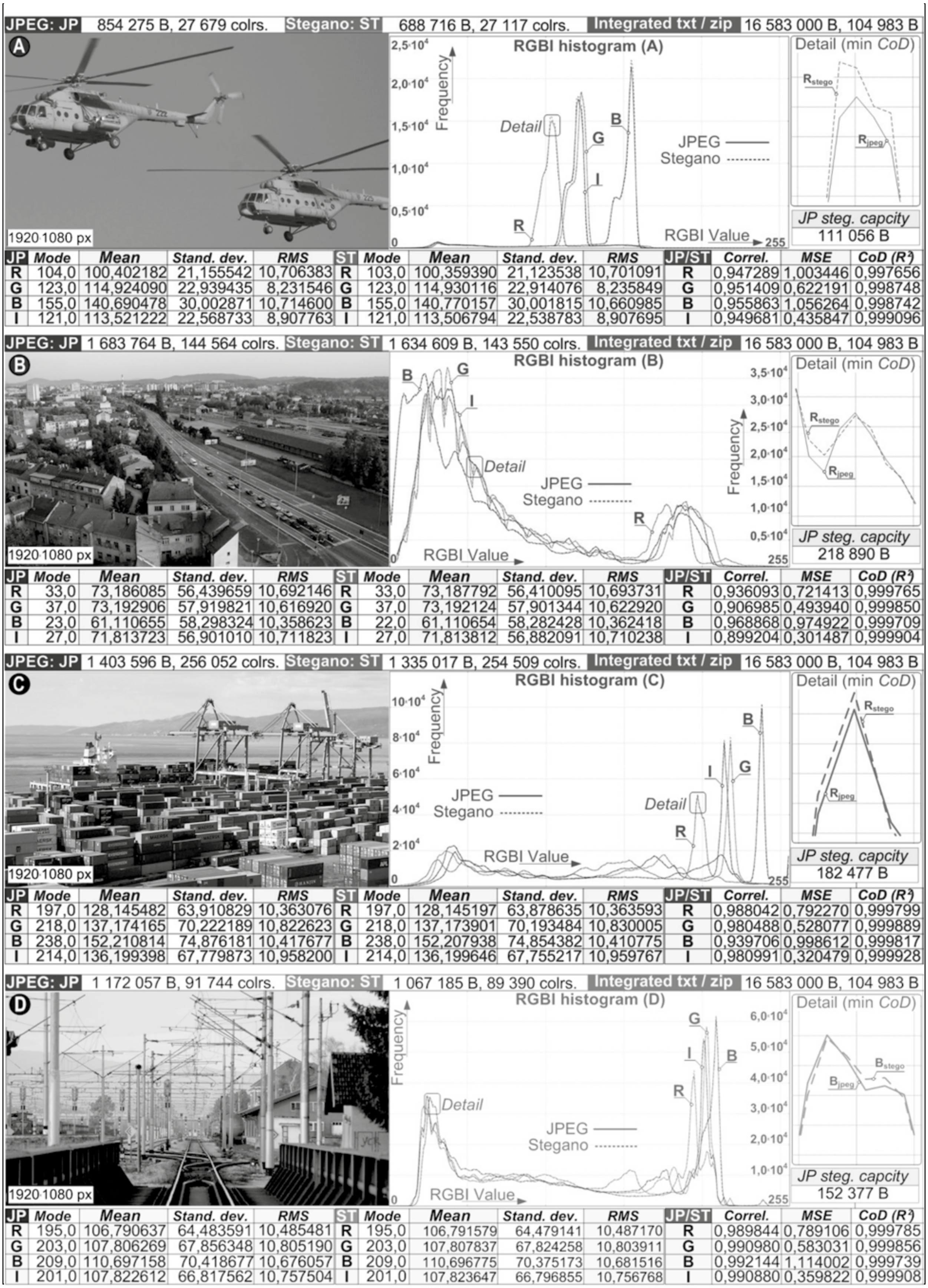


Figure 4 – Arrangement of integrated message within the image

How successful the procedure of steganographic integration (by method of transform domain), of the compressed textual file within the image is, is shown in *Figure 5*.



JPEG: JP 854 275 B, 27 679 colrs. Stegano: ST 688 716 B, 27 117 colrs. Integrated txt / zip 16 583 000 B, 104 983 B

JP steg. capcity 111 056 B

JP	Mode	Mean	Stand. dev.	RMS	ST	Mode	Mean	Stand. dev.	RMS	JP/ST	Correl.	MSE	CoD (R²)
R	104,0	100,402182	21,155542	10,706383	R	103,0	100,359390	21,123538	10,701091	R	0,947289	1,003446	0,997656
G	123,0	114,924090	22,939435	8,231546	G	123,0	114,930116	22,914076	8,235849	G	0,951409	0,622191	0,998748
B	155,0	140,690478	30,002871	10,714600	B	155,0	140,770157	30,001815	10,660985	B	0,955863	1,056264	0,998742
I	121,0	113,521222	22,568733	8,907763	I	121,0	113,506794	22,538783	8,907695	I	0,949681	0,435847	0,999096

JPEG: JP 1 683 764 B, 144 564 colrs. Stegano: ST 1 634 609 B, 143 550 colrs. Integrated txt / zip 16 583 000 B, 104 983 B

JP steg. capcity 218 890 B

JP	Mode	Mean	Stand. dev.	RMS	ST	Mode	Mean	Stand. dev.	RMS	JP/ST	Correl.	MSE	CoD (R²)
R	33,0	73,186085	56,439659	10,692146	R	33,0	73,187792	56,410095	10,693731	R	0,936093	0,721413	0,999765
G	37,0	73,192906	57,919821	10,616920	G	37,0	73,192124	57,901344	10,622920	G	0,906985	0,493940	0,999850
B	23,0	61,110655	58,298324	10,358623	B	22,0	61,110654	58,282428	10,362418	B	0,968868	0,974922	0,999709
I	27,0	71,813723	56,901010	10,711823	I	27,0	71,813812	56,882091	10,710238	I	0,899204	0,301487	0,999904

JPEG: JP 1 403 596 B, 256 052 colrs. Stegano: ST 1 335 017 B, 254 509 colrs. Integrated txt / zip 16 583 000 B, 104 983 B

JP steg. capcity 182 477 B

JP	Mode	Mean	Stand. dev.	RMS	ST	Mode	Mean	Stand. dev.	RMS	JP/ST	Correl.	MSE	CoD (R²)
R	197,0	128,145482	63,910829	10,363076	R	197,0	128,145197	63,878635	10,363593	R	0,988042	0,792270	0,999799
G	218,0	137,174165	70,222189	10,822623	G	218,0	137,173901	70,193484	10,830005	G	0,980488	0,528077	0,999889
B	238,0	152,210814	74,876181	10,417677	B	238,0	152,207938	74,854382	10,410775	B	0,939706	0,998612	0,999817
I	214,0	136,199398	67,779873	10,958200	I	214,0	136,199646	67,755217	10,959767	I	0,980991	0,320479	0,999928

JPEG: JP 1 172 057 B, 91 744 colrs. Stegano: ST 1 067 185 B, 89 390 colrs. Integrated txt / zip 16 583 000 B, 104 983 B

JP steg. capcity 152 377 B

JP	Mode	Mean	Stand. dev.	RMS	ST	Mode	Mean	Stand. dev.	RMS	JP/ST	Correl.	MSE	CoD (R²)
R	195,0	106,790637	64,483591	10,485481	R	195,0	106,791579	64,479141	10,487170	R	0,989844	0,789106	0,999785
G	203,0	107,806269	67,856348	10,805190	G	203,0	107,807837	67,824258	10,803911	G	0,990980	0,583031	0,999856
B	209,0	110,697158	70,418677	10,676057	B	209,0	110,696775	70,375173	10,681516	B	0,992144	1,114002	0,999739
I	201,0	107,822612	66,817562	10,757504	I	201,0	107,823647	66,796855	10,756768	I	0,990880	0,359822	0,999908

Figure 5 – Statistical characteristics of steganographically processed JPEG recording

A compressed textual file of size indicated under item integrated txt in tables has been integrated within every image (denoted by A, B, C, D) using steganographic algorithm F5. Under items JPEG(JP) and STEGO(ST) there is obvious change of the file size and of the number of colours after the steganographic integration thus proving that the procedure affects the ratio of the compression of the image recording. By using the mathematical model the statistical characteristics of RGBI (R=Red, G=Green, B=Blue, I=Intensity) of every image have been calculated. The calculation of mode, mean value, standard deviation and RMS (Root Mean Square) for JPEG have been presented and the image of each single channel has been steganographically processed. The results prove the hypothesis that steganographic integration affects the image to such extent which is invisible to the human eye, and the difference can be read as mild change of statistical characteristics of the image. Statistical characteristic of the correlation (Correl.), Mean Square Error and Coefficient of Determination between compressed and steganographically processed recording additionally confirm the thesis that the differences between recordings are very small. The presentation of the histogram of each single RGBI channel, shows an almost perfect overlapping of the lines of compressed and steganographically processed image. It should be noted that the textual data before integration and after extraction are fully identical regarding the content and memory usage. This has confirmed the hypothesis that steganographic processing does not change the integrated data, not in the least. The arrangement of integrated data within the image structure is presented in *Figure* 6.

It is obvious that the steganographic algorithm F5 tends to distribute the integrated message properly within the image structure. The black nuances in the graphic display refer to the size of the change in the pixel lighting intensity of the steganographically processed recording. The integration and change of the values of the image recording is not concentrated to a single area of the image thus reducing the possibility of changing the texture and deformation of image.

Preservation of statistical properties of the image is essential from the aspect of data security since some steganographic algorithms leave characteristic "trails" in the recording structure. By analysing the image, the potential attacker (or malicious user) could influence the content of integrated messages thus degrading the credibility and authenticity of the transport-relevant data. The characteristics of the mentioned methods of data integration within the image are mentioned in *Figure 7* [1, 2, 3, 4, 5, 6, 7, 9].

The advantages of the methods of meta-data input are the maximal capacity regardless of the image content, resistance to the change of content and standardized procedure. The drawbacks are that only textual data input is possible, and the undeveloped data security system against content change.

The essential advantage of steganographic processing is the possibility of integrating data regardless of their format, the procedure does not generate additional data; the procedure has very developed systems for data security against unauthorized access and subsequent manipulation. The drawbacks are reflected through the dependence of integration capacity on the image content; in case of manipulation with the content of the image the integrated data are destroyed and the fact that the procedure is non-standardized. Therefore, it may be concluded that steganographic processing enables integration of different types of data with high level of security against subsequent manipulation and represents high-quality method of data integration against the usage of meta-data. It should be emphasised that both integration methods are not mutually exclusive and it is possible to use both methods at the same time on a joint image.

3.2 Steganographic integration of transport-relevant data

The aim of steganographic processing is the integration of collected data in the image structure at the supervised location. The purpose, type and characteristics of the applied measuring equipment depend on the specifications and requirements of the supervisory bodies of ITS, transport experts and the subjects interested in these data. Apart from the collected data, the control data which can be additionally cryptographically protected are also steganographically integrated. Control data can transfer information about the origin and real owner of the collected and integrated information. It should be kept in mind that the amount of integrated data is limited due to steganographical algorithm constraints or their memory usage.

Regardless of the number of supervised locations it is essential that all the collected data and images

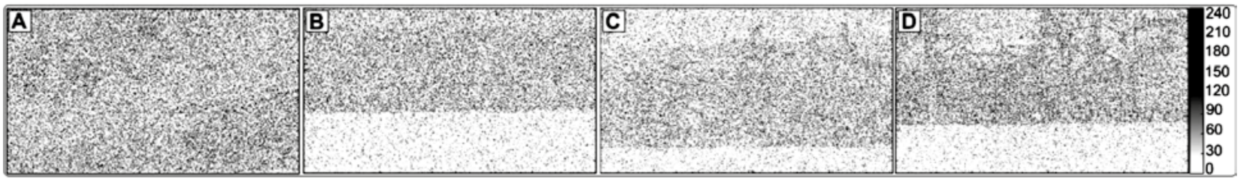
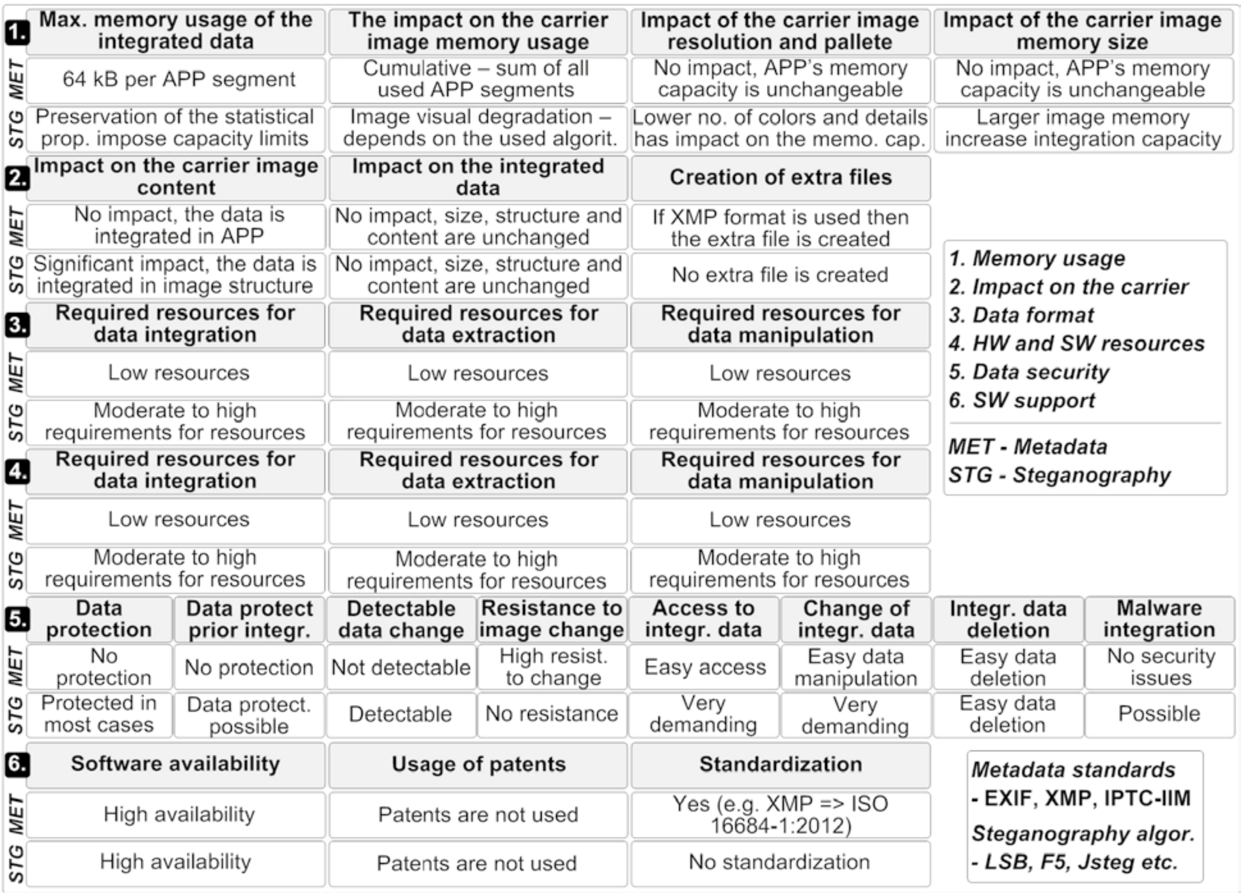


Figure 6 – Arrangement of integrated message within JPEG format structure



1.	Max. memory usage of the integrated data	The impact on the carrier image memory usage	Impact of the carrier image resolution and pallete	Impact of the carrier image memory size
MET	64 kB per APP segment	Cumulative – sum of all used APP segments	No impact, APP's memory capacity is unchangeable	No impact, APP's memory capacity is unchangeable
STG	Preservation of the statistical prop. impose capacity limits	Image visual degradation – depends on the used algorit.	Lower no. of colors and details has impact on the memo. cap.	Larger image memory increase integration capacity

2.	Impact on the carrier image content	Impact on the integrated data	Creation of extra files
MET	No impact, the data is integrated in APP	No impact, size, structure and content are unchanged	If XMP format is used then the extra file is created
STG	Significant impact, the data is integrated in image structure	No impact, size, structure and content are unchanged	No extra file is created

3.	Required resources for data integration	Required resources for data extraction	Required resources for data manipulation
MET	Low resources	Low resources	Low resources
STG	Moderate to high requirements for resources	Moderate to high requirements for resources	Moderate to high requirements for resources

4.	Required resources for data integration	Required resources for data extraction	Required resources for data manipulation
MET	Low resources	Low resources	Low resources
STG	Moderate to high requirements for resources	Moderate to high requirements for resources	Moderate to high requirements for resources

5.	Data protection	Data protect prior integr.	Detectable data change	Resistance to image change	Access to integr. data	Change of integr. data	Integr. data deletion	Malware integration
MET	No protection	No protection	Not detectable	High resist. to change	Easy access	Easy data manipulation	Easy data deletion	No security issues
STG	Protected in most cases	Data protect. possible	Detectable	No resistance	Very demanding	Very demanding	Easy data deletion	Possible

6.	Software availability	Usage of patents	Standardization
MET	High availability	Patents are not used	Yes (e.g. XMP => ISO 16684-1:2012)
STG	High availability	Patents are not used	No standardization

1. Memory usage
2. Impact on the carrier
3. Data format
4. HW and SW resources
5. Data security
6. SW support

MET - Metadata
STG - Steganography

Metadata standards
- EXIF, XMP, IPTC-IIM
Steganography algor.
- LSB, F5, Jsteg etc.

Figure 7 – Comparison of characteristics of methods of data integration

are synchronised, i.e. the values of the collected data have to be steganographically integrated at the identical moment. The time of storing the transport-relevant data can connect the gathered data from different locations into one logical unit. The gathered data can be extracted into a separate database for further analysis or may be divided and exchanged with the elements of one's own, neighbouring systems or with users who are interested in these data. In order to insure credibility and authenticity of the steganographically processed recording the methods of public cryptographic key can be used. The procedure of collecting and steganographic integration of data is presented in *Figure 8*.

Control data that can be prepared in advance or calculated on the basis of currently available gathered data are added to the record. In order to save the memory space and remove the repeating samples of data the textual file with analytic data is compressed. The procedure of compression is protected by the

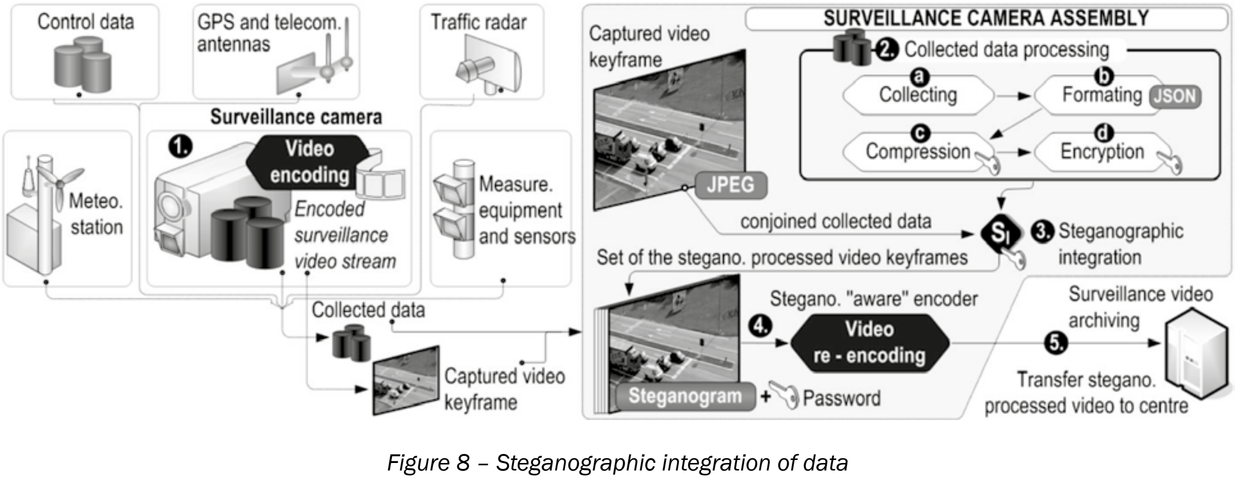

Control data
GPS and telecom. antennas
Traffic radar
Surveillance camera
1.
Video encoding
Meteo. station
Encoded surveillance video stream
Measure. equipment and sensors
Collected data
Captured video keyframe
Captured video keyframe
SURVEILLANCE CAMERA ASSEMBLY
2 Collected data processing
a Collecting
b Formating
JSON
c Compression
d Encryption
JPEG
conjoined collected data
S
3 Steganographic integration
Set of the stegano. processed video keyframes
Stegano. "aware" encoder
4.
Video re - encoding
Steganogram
+ Password
Surveillance video archiving
5.
Transfer stegano. processed video to centre

Figure 8 – Steganographic integration of data

password, and then encryption of data is done by private cryptographic key of the surveillance centre. The prepared data are steganographically integrated in the structure of the video recording frame, and with the purpose of additional security the steganographic key defined by the surveillance centre is used. After steganographic processing, the image (or video) record is transferred via information-communication network towards the surveillance centre.

The procedure of steganographic extraction of the traffic-relevant data is presented in *Figure 9* and it is inverse to the previously described procedure of integration.

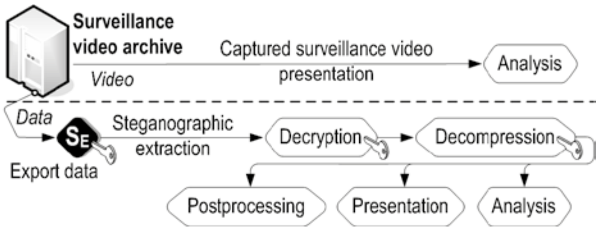

Surveillance video archive
Video
Captured surveillance video presentation
Analysis
Data
SE
Export data
Steganographic extraction
Decryption
Decompression
Postprocessing
Presentation
Analysis

Figure 9 – Steganographic extraction of data

After storage, the steganographically processed image (or video recording) contains visual presentation and concrete transport-relevant data about the condition on the supervised segment of ITS. With the procedure of steganographic extraction of the gathered data they are exported into the form which is suitable for presentation or analysis. The image or video recording further keep their basic function and the user does not notice the decline of quality in the form of reducing details, colour, occurrence of samples or deformation of image. The user who has no authority of access to data, has no installed software support or simply is not familiar with the steganographically integrated data, can see "common" stored image or video recording about the condition of the ITS part.

In order to realise access to steganographically integrated data about the condition of the supervised part of ITS, it is necessary to have, apart from adequate software equipment and support, user rights as the element of data security system. After the realised application of steganographic key (which has to be identical to the key used during steganographic integration), the application of the procedure of decryption and decompression of data the user has at disposal the textual file which contains the measured transport-relevant data. As previously already mentioned, a large number of applications support this format for the presentation or for their import in the database for data analysis.

In case of incident situations the transport experts can be focused on monitoring the condition on a single location, but they have available data about all locations for which the data have been steganographically integrated. In case there is need to access the collected data on other supervised locations at a certain moment it is possible to access simply and fast precisely these data and visual presentation of the condition. Since all the collected data at all locations are time-synchronised it is possible to steganographically extract only the desired data and to present them. For the analysis of the collected data it is necessary only to select the desired location and the time scope since the data are extracted directly from the transfer file, and thus it is not necessary to view the supervisory image or video recording to access the steganographically integrated data.

3.3 Structure and access to integrated data

As already mentioned, the system of collecting data can be extremely heterogeneous from the aspect of applied technical and technological solutions. The measurement instruments collect data that differ according to the source, type, values, precision, frequency of collecting, etc. The transport expert, regarding the field of interest of research selects the sources of data and collected information about the condition of the supervised section of the transport system or ITS. If all the supervised parts of the traffic system were taken into consideration as well as the data about its influence on the adjacent systems then a respectable source of transport-relevant information would be available.

The question is in what way the data should be organized for the transfer, later processing, import into the database and presentation, so that at the same time the format itself does not generate a large amount of meta-data. All data need to be hierarchically structured in order to accurately determine the location, time and device which collected the transport-relevant data. JSON (JavaScript Object Notation) is the format for data exchange which can preserve the hierarchical structure of data, and it has a very simple structure and it is not dependent on the hardware or software platform [23, 24]. Beside JSON there is also XML [25] format which is standardized and it is used in many systems and applications. The reason why the JSON format is chosen instead of XML, lies in the fact that JSON possesses some significant advantages over XML [24]: it requires less data for the same amount of information, much simpler structure, format is human readable and understandable, it is suitable for data exchange (while XML is suitable for document exchange) and faster and easier processing than XML.

The collected transport-relevant data are formatted according to JSON format and stored in a textual file. In order to save memory space, the file can be

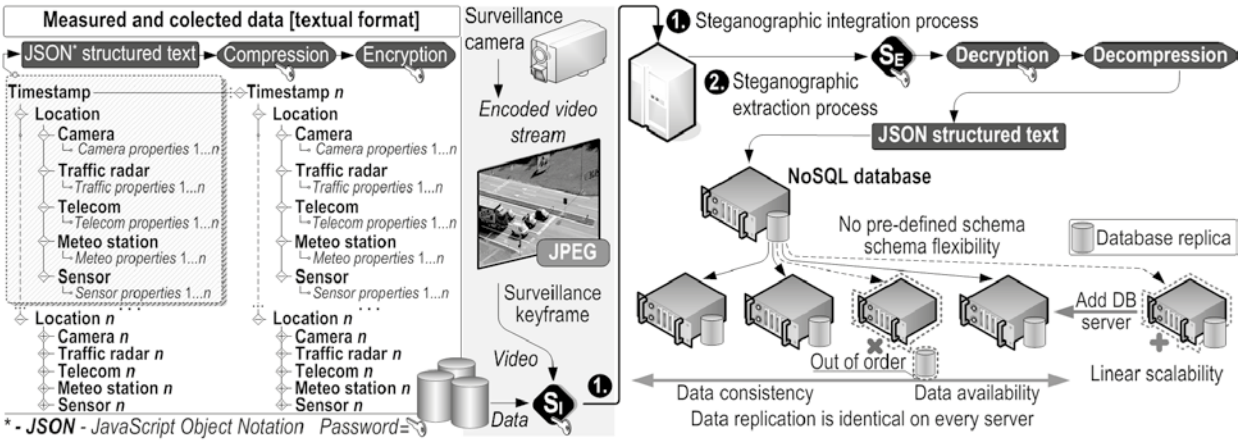


Figure 10 – Transfer and storage of collected data in NoSQL database

processed and encrypted because of data security against unauthorized access and manipulation. The compressed and encrypted file is steganographically integrated into the image structure. If there is need for analysis or presentation of the gathered data, the steganographic extraction, decryption and decompression form the JSON formatted file which can be easily introduced into the database or application which will present them in the appropriate format.

Regarding the heterogeneity of the data collection system using a large number of criteria it may be concluded that it is not possible to define the fixed structure of the database for their storage. In case of changing the device, software support or change of working parameters, the existing defined structure will not be able to store the collected data. SQL (Structured Query Language) relational databases have a strictly defined structure, whereas the so-called NoSQL databases have dynamic structure which changes very easily, the database is (horizontally) scalable and the failure of one of the servers does not affect the system operation [26]. *Figure 10* shows the system of transferring and storing the transport-relevant data within NoSQL database.

NoSQL bases are adapted to working with large amounts of data that have a changeable structure and content. Regarding the previously mentioned characteristics of the data collection system NoSQL databases can represent a suitable solution for their storage, analysis and presentation.

As mentioned previously, NoSQL system does not require static data scheme, it supports JSON and it is very suitable for heterogeneous data collection system, but also has certain drawbacks. Due to the fact that collected data is shared on the network, the CAP theorem [27] should be considered. CAP is an acronym for the three desirable properties of the distributed system: consistency (C), availability (A) and partition tolerance (P). The CAP theorem states that the system can have at least two of three mentioned properties. Since the presented NoSQL storage system prefers availability and partition tolerance, the consistency may be compromised in some cases. In practice, it is important to decide what will happen if time-out takes place during data fetching. Due to the fact that steganographically embedded data content can present valuable source of information for the traffic experts, the proposed system should primarily ensure data consistency - not availability. If error or time-out take place, the system should be able to repeat steganographic extraction from surveillance video frames and store data into database. Depending on the system purpose it is possible to provide certain consistency and availability trade-offs. Group of authors [28] implemented an extension to YCSB (Yahoo Cloud Services Benchmark) tool [29]. Application extension is able to count the numbers of stale reads in real time and can be used in evaluation of the consistency and availability trade-offs (the proposed model also takes latency into account).

4. EXAMPLES OF USING STEGANOGRAPHIC INTEGRATION

Next examples will present the possibilities provided by the mentioned system of steganographic integration. It should be emphasized that the first example is associated to the data protection while the second example is associated with the law enforcement topic. Since the steganographic data are part of the image structure, every change of the file content causes damage or complete destruction of integrated data. The mentioned characteristic can present a reliable indicator that the image content has been manipulated. *Figure 11* shows the procedure of integrating control data. Regardless of the degree of data content change (even one pixel) the integrated data will be destroyed. The impossibility of extracting control data qualifies the image as a non-authentic and non-credible source of information.

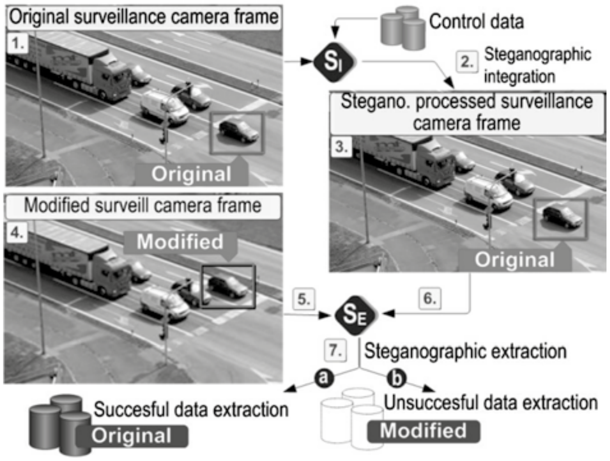

Original surveillance camera frame
1.
Original
Control data
S_I
2. Steganographic integration
Stegano. processed surveillance camera frame
3.
Original
Modified surveill camera frame
4.
Modified
5.
6.
S_E
7. Steganographic extraction
a
b
Succesful data extraction
Original
Unsuccesful data extraction
Modified

Figure 11 – Steganographic integration of control data

In the following example in *Figure 12* the procedure of detecting a traffic violation is presented, and informing the person who did it and visual and analytic presentation of the incident situation.

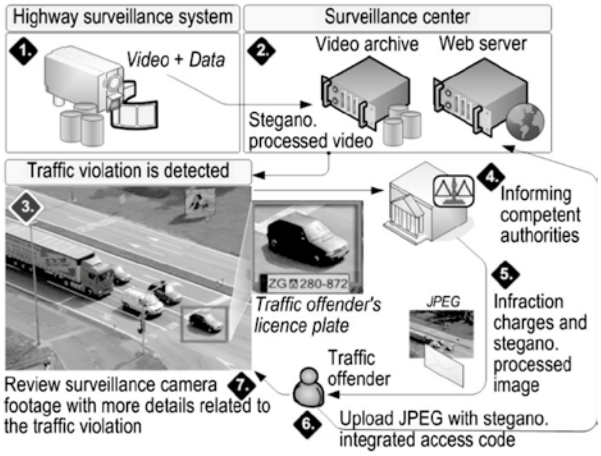

Highway surveillance system
Surveillance center
1.
Video + Data
2.
Video archive
Web server
Stegano. processed video
Traffic violation is detected
3.
4.
Informing competent authorities
ZG 280-872
Traffic offender's licence plate
JPEG
5.
Infraction charges and stegano. processed image
Traffic offender
Review surveillance camera footage with more details related to the traffic violation
7.
6.
Upload JPEG with stegano. integrated access code

Figure 12 – Communication with the traffic offender

After traffic violation detection the identity of the person who did it is checked. Within the image or video recording there are data about the condition of the road at the moment of incident occurring. The traffic offender can be informed about the committed traffic violation via e-mail containing steganographically processed image attachment in JPEG format. The message contains steganographic integrated data which can be used by the transport offender to access the system in which they will be able to receive more information about the state of the road and the surroundings during the violation.

5. CONCLUSION

The research work has presented the possibility of forming a unified source of transport-relevant data. By combining the visual and measured data and by using the infrastructure of the public cryptographic key, transport experts have available authentic and credible data with legal force about the situation on the supervised section of the road.

The data integration methods through meta-data or by using the steganographic mechanisms have been analysed. The steganographic method has the advantage due to the possibility of data integration in the desired digital format within the image structure. The analysis results indicate that the change in the carrier image content is invisible for the human eye, statistical properties are slightly changed, and the integrated data before integration and after extraction are fully identical.

Because of the heterogeneity of data collection system from the technical-technological aspect, it was suggested that the collected data should be structured in the JSON format. Furthermore, NoSQL type of database for the storage of the collected data has been suggested since they do not require strictly defined data structure, have a high level of scalability without influence on the operation and functioning of the system.

Future research is directed to the development of steganographic algorithms that support integration of large amounts of data within the video recording. When forming the video recording the change of the image content structure would be performed thus directly influencing the integrated data. If the video encoder were "aware" that within some images there are integrated data, then it would integrate them into the video recording without change. Thus the video recording would keep their primary intention of presenting the situation on the road, whereas certain images (i.e. video recording frames) would contain integrated data. By extracting data the transport experts obtain detailed information about the values of the transport-relevant data for the situation presented by the video recording.

Dr. sc. **ADAM STANČIĆ**[1]
E-mail: adam.stancic@vuka.hr
Doc. dr. sc. **IVAN GRGUREVIĆ**[2]
E-mail: ivan.grgurevic@fpz.hr
Prof. dr. sc. **ZVONKO KAVRAN**[2]
E-mail: zvonko.kavran@fpz.hr
[1] Veleučilište u Karlovcu,
Meštrovićeva 10, 47000 Karlovac, Hrvatska
[2] Sveučilište u Zagrebu,
Fakultet prometnih znanosti,
Vukelićeva 4, 10000 Zagreb, Hrvatska

INTEGRACIJA PROMETNO RELEVANTNIH PODATAKA UNUTAR SLIKOVNOG ZAPISA NADZORNOG SUSTAVA

SAŽETAK

Integracija prikupljenih informacija na prometnici unutar slikovnog zapisa snimljenog nadzornim sustavom formira objedinjen izvor prometno relevantnih podataka o nadziranoj situaciji. Osnovna pretpostavka je da postupak integracije slikovni zapis mijenja u mjeri koja je nevidljiva za ljudsko oko, a integrirani podaci zadržavaju identičan sadržaj. Navedena pretpostavka dokazana je ispitivanjem statističkih svojstava slikovnih zapisa i integriranih podataka matematičkim modelom modeliranim u programskom jeziku Python uz korištenje kombinacije funkcija dodatnih biblioteka (OpenCV, NumPy, SciPy i Matplotlib). Model je korišten za usporedbu metode unosa meta-podataka i metode steganografske integracije korekcijom koeficijenata diskretne kosinusne transformacije JPEG komprimiranog slikovnog zapisa. Za postupke steganografske obrade podataka korišten je steganografski algoritam F5. U radu su analizirane prednosti i nedostaci metoda integracije te primjeri situacija u prometu u kojima bi formirani objedinjeni izvori prometno relevantnih informacija mogli biti korišteni.

KLJUČNE RIJEČI

integracija; inteligentni transportni sustav; meta-podaci; nadzorni sustav; steganografija;

REFERENCES

[1] JEITA CP-3451. Exchangeable image file format for digital still cameras: EXIF Version 2.2. [cited 2016 Sep 1]. Available from: http://www.exif.org/Exif2-2.PDF

[2] Extensible Metadata Platform (XMP). [cited 2016 Sep 1]. Available from: http://www.adobe.com/products/xmp/index.html

[3] ISO News. Adobe XMP becomes an ISO standard. [cited 2016 Sep 1]. Available from: http://www.iso.org/iso/home/news_index/news_archive /news.htm?refid=Ref1525

[4] IPTC Core and Extension. Spec. version 1.1, 2010. [cited 2016 Sep 1]. Available from: http://www.iptc.org/std/photometadata/specification/IPTC-PhotoMetadata(200907)_1.pdf

[5] Katzenbeisser S, Petitcolas FAP. Information hiding techniques for steganography and digital watermarking. Boston: Artech House; 2000.

[6] Westfeld A. F5 - A steganographic algorithm: High capacity despite better steganalysis. In: Moskowitz, IS (editor). Information Hiding. 4th International Workshop, IH '01. Pittsburgh, USA; 2001. p. 289-302.

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

[8] Curran K, Bailey K. An evaluation of image based steganography methods. International Journal of Digital Evidence. 2003;2(2):1-40.

[9] Kharrazi M, Sencar HT, Memon N. Image steganography: Concepts and practice. WSPC / Lecture Notes. New York, USA: Polytechnic University, Brooklyn; 2004.

[10] Ratnakirti R, Suvamoy C. Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach. International Journal of Security and Its Applications. 2016;10(4):179-196.

[11] Python 2.7. [cited 2016 Sep 1]. Available from: https://www.python.org/download/releases/2.7/

[12] OpenCV 3.1. [cited 2016 Sep 2]. Available from: http://opencv.org/downloads.html

[13] NumPy. [cited 2016 Sep 2]. Available from: http://www.numpy.org/

[14] SciPy. [cited 2016 Sep 2]. Available from: http://www.scipy.org/

[15] Matplotlib. [cited 2016 Sep 2]. Available from: http://matplotlib.org/

[16] Briffa JA, Schaathun HG, Wahab AWA. Has F5 Really Been Broken?. Proceedings of the 3rd International Conference on Crime Detection and Prevention (ICDP 2009). 2009 Dec 3; London, UK; 2009. p. 1-6.

[17] C# Implementation of F5 Algorithm for JPEG Steganography. [cited 2016 Sep 2]. Available from: https://github.com/otuncelli/f5-steganography

[18] Westfeld Andreas homepage (author of the F5 algorithm). [cited 2016 Sep 2]. Available from: http://www2.htw-dresden.de/~westfeld/

[19] Kulkarni M. An information hiding system using 16*16 quantization table. 2014 International Conference on Advances in Communication and Computing Technologies (ICACACT). 2014 Aug 10-11; Mumbai, India; 2014. p. 29-232.

[20] Khedekar A, Ilag A, Pooja M, Tatwadarshi PN. Steganography in Audio/Video files using Modified F5 Algorithm. International Journal of Computer Applications (0975 – 8887). National Conference on Role of Engineers in Nation Building (NCRENB-15). 2015 May; New York, USA; 2015. p. 9-12.

[21] Neufeld A, Ker AD. A study of embedding operations and locations for steganography in H.264 video. Proceedings of SPIE 8665. Media Watermarking, Security, and Forensics. 2013 Mar 22; doi: 10.1117/12.2022495

[22] Pennebaker WB, Mitchell JL. JPEG Still Image Data Compression Standard. Springer-Verlag US; 1993.

[23] ECMA-404. The JSON Data Interchange Standard. [cited 2016 Mar 5]. Available from: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

[24] JSON. [cited 2016 Mar 5]. Available from: http://www.json.org/

[25] Extensible Markup Language – XML. [cited 2016 Sep 2]. Available from: https://www.w3.org/XML

[26] Tsuyuzaki K, Onizuka M. NoSQL Database Characteristics and Benchmark System. NTT Technical Review. 2012;10(12):22-26.

[27] Brewer E. CAP Twelve Years Later: How the “Rules” Have Changed. IEEE Computer Society. Computer. 2012;45(2):23-29.

[28] Kumar SP, Lefebvre S, Chiky R, Gressier Soudan E. Evaluating consistency on the fly using YCSB. Computational Intelligence for Multimedia Understanding (IWCIM). 2014 International Workshop. Paris, France; 2014. p. 1-6.

[29] Cooper BF, et al. Benchmarking cloud serving systems with YCSB. Proceedings of the 1st ACM symposium on Cloud computing. SoCC ’10. 2010 June 10-11; Indianapolis, USA. New York: ACM; 2010. p. 143-154.