UDK: 351.811.123(497.11)

Originalni naučni rad

LEGAL ASPECTS OF DATA MINING ALGORITHMS FOR STREAM PROCESSING IN TRAFFIC SURVEILLANCE

Zaklina Spalevic[1]
Singidunum University, Belgrade
Milos Ilic[2]
Nebojsa Arsic[3]
University of Pristina
Faculty of Technical Science, Kosovska Mitrovica

Summary: A major challenge that all law-enforcement and intelligence-gathering organizations are facing is to accurately and efficiently analyze the growing volumes of crime data. In many fields, video surveillance can be used for that purpose. Video surveillance systems are now commonly used at various places like banks, hotels, schools, supermarkets. These systems are applicable for real-time monitoring or post checking. Current video surveillance systems have lower intelligence and it need people to monitor them. Today, video surveillance systems are used for traffic cameras, too. Traffic cameras are an innovative and extremely functional application of video surveillance technology. Whether they are recording traffic patterns for the future study and observation or monitoring traffic and issuing tickets for moving violations, traffic cameras are an explosively popular form of video surveillance. One way to find traffic

[1] Assistant Professor, zspalevic@singidunum.ac.rs
[2] Teaching assistant, milos.ilic@pr.ac.rs
[3] Full Professor, nebojsa.arsic@pr.ac.rs

patterns or to prevent traffic accidents and provide better road security is to use data mining techniques. With data mining, stream from many traffic cameras can be processed in real time. Property like this could provide some intelligence upgrade within systems, so they could make decision on their own without the need of people to monitor them. In this paper the authors described the data mining techniques for stream processing, pattern and abnormality detection in traffic surveillance systems. Each video recording and the use of recorded video on the court must be covered by legal regulations. The authors investigated and extracted the appropriate articles from concrete Laws of Republic Serbia, covering this kind of problems.

Keywords: Clustering, Data Mining, Stream Processing, Traffic Surveillance, Law Regulation, Jurisprudence.

Introduction

In recent years cars, public transportation and driving from one point to another become inseparable part of people's everyday life. People travel to work, on a holiday, to the supermarket, dinner, picnic, etc. Because of that, traffic congestion has become a significant problem. Every town has some streets or blocks that represent traffic bottleneck. Traffic accidents become a common occurrence on all type of roads. To prevent them and to secure people's lives as much as possible, many countries are setting up video cameras on the roads. Video cameras are first placed over the crossroads, and after that on the less frequented streets. The functionality and the effectiveness of the measurement of the traffic scene using surveillance systems based on computer vision and image processing should substantially assist in better traffic control, incident management and traffic low enforcement[4]. The ability to monitor and collect the data about traffic, using the relevant surveillance systems will help understanding the mechanics of traffic network. When this technology is integrated with other forms of surveillance and traffic monitoring systems, it is going to start an expansion of the next generation of advanced traffic control. With the development of software and hardware, video surveillance systems have been not only widely used in the security realm, but also in our daily life and work, in hotels, supermarkets, banks, schools and so on.

These applications are used for real-time monitoring and detecting the unusual events. System like this can be used to extend traffic control and video

[4] V. Kale; F. Momin, Video Data Mining Framework for Surveillance Video, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 2/3, pp.54-57.

from public cameras. In that way an authorized user will have video of the streets from the different angles. To use a video from public cameras, which are not in the government ownership, agencies must uphold the Law on Electronic Communications[5]. Nowadays video surveillance systems are not autonomous, meaning that they need an employee to operate them. So, it is urgent to extract video content features and semantic information and there is a need for some kinds of models due to the increasing demands of intelligence. To provide better video stream processing and traffic pattern creation, data mining can be used[6]. Data mining is very active research topic nowadays and is the process of extracting previous knowledge and detecting interesting patterns from large set of data. Data mining encompasses the process of discovering hidden patterns and relationships in large amounts of information. This also allows us to make accurate and reliable predictions of the future events, based on the identification and characterization of these patterns and trends in historical data. The primary use of data mining is to find something new in the data, to discover a new piece of information that no one knew previously. For traffic stream processing and pattern creation, a data mining techniques named clustering can be used. Clustering is the widely used data mining technique which groups similar items, to obtain meaningful groups/clusters of data items in a data set. These clusters represent the dominant modes of behavior of the data objects determined using a similarity measure. A data analyst can get a high level of understanding of the characteristics of the data set by analyzing the clusters. Clustering provides an effective solution to discover the expected and unexpected modes of behavior and to obtain a high level understanding of the network traffic.

1. Processing Video from Traffic Surveillance System

Traffic surveillance system consists of different types of cameras, road sensors or motion sensors above the roads. From those cameras a video control center gets different resolution video streams, specific for each camera. Video can be recorded from different angles and could contain packets with different data from sensors. Video stream in combination with the data from sensors (air temperature, car speed, car distance, etc.) must be processed by the employee in control center. It is vitally important that the surveillance staff in the control centers are actually able to see what is happening at the

[5] The Law of Electronic Communications, „Official Gazette of the RS", № 44/2010, 60/2013 - decision US and 62/2014.

[6] A. Ingle; S. Dongre, A Survey on Data Mining Techniques for Surveillance of Real Time Video Streams, , *International Journal of Advanced Computer Research*, vol. 2/4, pp. 397-400.

trouble spots along the route and in particular in the areas where there is a greater likelihood of critical situations such as delays, accidents and traffic jams occurring. They are able to use such images to instigate any safety or control measures required in sufficient time to guarantee the highest level of safety to motorway users and therefore as little discomfort as possible. Camera position on the street is very important. On the one hand, higher mounting position allows better angle and wider view, covering all lanes on the road by one camera. On the other hand, lower mounting heights would not provide effective images as some vehicles may hide part of other vehicles from the scene. Today's hardware solutions and high definition cameras, provides the best video quality. The simplest use is to watch video recordings and use the information from the recordings for traffic control or police reports.

The better uses are statistical information about road safety, anomaly of specific part of the roads or information about some accidents. All these pieces of information can be used to provide batter road security. This is very simple if we have a couple of cameras and enough employees in the control center. But what will happen if we have hundreds of cameras just for one city block, or if we have different kind of cameras? In that way it is impossible to watch all cameras at the same time. First we must process video streams from all cameras. Stream processing is a complex task that depends on processing demands, the input video format and on the desired output video format. In general, stream processing system consists of the blocks presented in Figure 1.

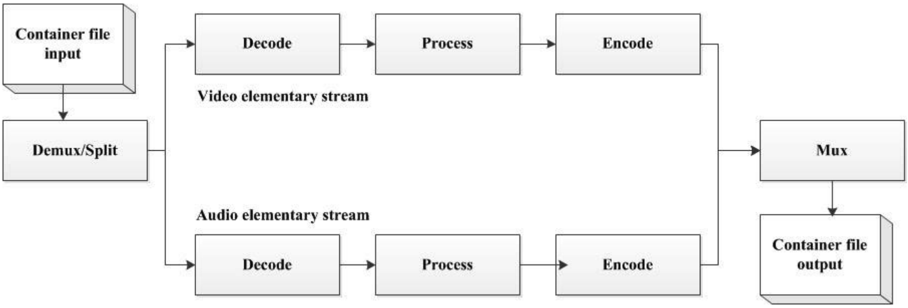

Figure 1: *A generic transcode pipeline*

From the figure presented above, we can see that the videos from cameras must be divided into packets that are of the same size. Divided packets must be translated through some kind of network to the end user, who is employed in a control center. Typically, most source content is not in an elementary stream format. Rather, it is a combination of both video and audio "muxed" together into a single file via a container format. It must be demuxed to a video elementary stream before the decoder can begin to work. There are many tools available to demux video streams from their containers. Demultiplexer is a software component that demultiplexes individual elementary streams of a media file, e.g., audio, video, or subtitles and sends them to their respective decoders for actual decoding. They are often specialized for a specific container type. It can be helpful to check what types of streams have been muxed together with a tool compatible with a wide variety of containers. A container or a wrapper format is a metafile format whose specification describes how different elements of data and metadata coexist in a computer file. By definition, a container format could wrap any kind of data. Most container formats are specialized for specific data requirements. For example, a popular family of containers is found for use with multimedia file formats. Since audio and video streams can be coded and decoded with many different algorithms, a container format may be used to provide a single file format to the user. Container does not describe how data or metadata are encoded, and because of that the appropriate software tool must decode each container and send the data from it to the processing. Decode takes a bit stream as input and produces surfaces as output. However, there are also some fundamental design characteristics to keep in mind to fully utilize the performance benefits. Each video file format has specific decoder, and that decoder provides the appropriate decoding. Per definition video codec is a device or software that enables compression or decompression of digital video. A codec encodes a data stream or signal for transmission, storage or encryption, or decodes it for playback or editing.

Codecs are used in videoconferencing, streaming media and video editing applications. Because of the design of analog video signals, which represent luma and color information separately, a common first step in image compression in codec design is to represent and store the image in YCbCr color space. The conversion to YCbCr provides two benefits. First, it improves compressibility by providing decorrelation of the color signals, and second, it separates the luma signal, which is perceptually much more important, from the chroma signal, which is less perceptually important and which can be represented at lower resolution to achieve more efficient data compression. In video, luma represents the brightness in an image, and chroma is the signal used in video systems to convey the color information of the picture. It is common to represent the ratios of information stored in these different channels in the following way Y:Cb:Cr. Different codecs will use different chroma subsampling ratios as appropriate to their compression needs. In the systems like traffic surveillance or any other surveillance, video quality is very important. The bad side of many of the most popular codecs in the software world is that they reduce quality by some amount in order to achieve compression. Often, this type of compression is virtually indistinguishable from the original uncompressed sound or images, depending on the codec and the settings used. In order to provide the best video quality the systems must use software solution in which there are different types of decoders implemented. One of the most widely used standards, and the standard that we propose for traffic video processing is H.264. That is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. Figure 2 shows the encoding and decoding process in H.264.

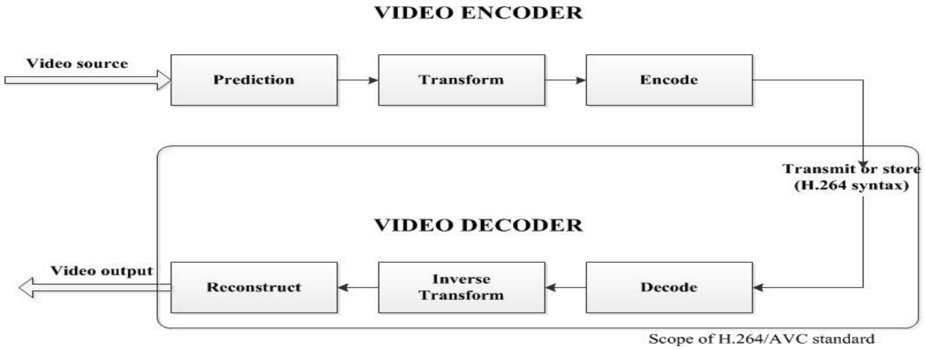

Figure 2: *The H.264 video coding and decoding process*

Here the encoder carries out prediction, transform and encoding process to produce a compressed H.264 bit stream. Encoder processes a frame of video in units named macroblocks. These units are 16x16 displayed pixels[7]. Encoder forms a prediction of this macroblock based on previously-coded data, either from current frame which represent intra prediction, or from other frames that have already been coded and transmitted which represent inter prediction. For encoder prediction it is important to form a residual sample. In the next step a block of residual samples is transformed using an approximate form of the discrete cosine transform, which is named integer transform.

This transform outputs a set of coefficients, each of which is a weighting value for a standard basis pattern. A block of transformed coefficients must be quantized, which means that each coefficient is divided by integer value.

Quantization reduces the precision of the transform coefficients according to a quantization parameter. The result is a block in which most or all coefficients are zero, with a few non-zero coefficients. Higher value for quantization parameter means that more coefficients are zero. Settings like this resulting in high compression at the expense of poor decoded image quality. If the quantization parameter sets to a low value, which means that more not – zero coefficients remain after quantization, resulting in better

[7] I. Richardson, *An Overview of H.264 Advanced Video Coding*, Vcodex, United Kindom, 2011, pp.1-7.

decoded image quality but lower compression which is better in our case. The final step in encoder is bitstream encoding. This is important because video coding process produces values that must be encoded to form the compressed bitstream. These values and parameters (syntax elements) are covered into binary codes using variable length coding and/or arithmetic coding. Each of these encoding methods produces an efficient, compact binary representation of the information. Binary stream like this can be stored or transmitted or used in some other processing.

Stream like this can be used and processed by some data mining methods, and in that way some patterns or anomalies can be noticed. More about this is presented below. Block video decoder represents a block in which video stream is decoding. Decoder receives the compressed H.264 bitstream, decodes each of the syntax elements and extracts the information described above. This information is then used to reverse the coding in the block which is named inverse transform and recreate a sequence of video images. For each macroblock, the decoder forms an identical prediction to the one created by the encoder. The decoder adds the prediction to the decoded residual to reconstruct a decoded macroblock which can then be displayed as part of a video frame. With reconstruction the decoding process is over. H.264 standard is very good for video processing, and the biggest advantage is its compression performance. For example if we compare this standard and some others, H.264 provide better image quality at the same compressed bitrate, or lower compressed bitrate for the same image quality.

In the video processing from traffic and public cameras the image quality is crucial. Because of different camera quality, the distance from the road and vehicles, like we said above, one video standard is not enough. Processing speed is very important, too. For example, if we have a big number of cameras, video processing from each camera is a complex job. Because of that the decoder must use hardware that will provide fast processing. Most of today's video decoders are implemented to use graphics processing unit (GPU) for encoding and decoding[8]. Modern GPUs are very efficient at manipulating computer graphics and image processing, and their highly parallel structure makes them more effective than general-purpose CPUs for algorithms where processing of large blocks of data is done in parallel[9]. If we look at all standards and properties that must be satisfied in surveillance video processing, for that purpose we can use Nvidia's CUDA Video Decoder. That is a video decoder that utilizes a parallel processing platform, known as CUDA. CUDA takes advantage of the GPU's ability to perform high sized amounts of work in

[8] Cuda Samples, Nvidia Corporation online available: https://www.clear.rice.edu/comp422/resources/cuda/pdf/

[9] M. Kim, et al, GPU-accelerated H.264 Decoding for Video Surveillance, poster paper P4161, *GPU Technology Conference*, Category: Performance Optimization – P003

a very short period of time[10]. This is a good property for video processing because we can include additional filters during playback or processing, which can improve video quality by doubling or even quadrupling the video size, then apply downscaling algorithms which render the final frame to the screen. For our case this means that we can include some pattern recognition and data mining algorithms to provide much more of just video playback. The above mentioned video standard H.264 is perfect for implementation on CUDA, because the H.264 video encoder is equipped by the latest generations of GPU. This encoder, being dedicated H.264 hardware on the GPU chip, does not use the GPU's graphics engine and can work together with CUDA applications. The hardware is optimized to provide excellent quality at high performance, enabling a wide range of applications that require video encoding capabilities. For example, H.264 video encored on some distributions of NVIDIA GPU is capable to compress image sequences with resolution 1920x1080 (24-bit) at frame rate up to 160 fps. For image resolution 1024x768 one could get up to 400 fps for High Performance Preset[8]. For comparison, CPU-based H.264 codec can compress the same image sequence with Full HD resolution at frame rate up to 34 fps on processor with Core i5-3330 CPU, 3.00 GHz 3.20 GHz. H.264 CUDA-based encoder can be utilized together with image processing pipeline on GPU, which means that we can start from raw data which we get from a camera and finish with compressed stream[6]. Video processing like this supports the maximum of sixteen HD cameras, and each camera upper 27 fps. For traffic video systems it is more than enough to record one intersection or one part of road with sixteen cameras especially if all cameras record from different angles.

2. Data Mining Algorithms for Traffic Surveillance Video Streams

Data mining is a powerful tool that enables investigators who may lack extensive training as data analysts to explore large databases quickly and efficiently. Computers can process thousands of instructions in seconds, saving precious time. Traditional data mining techniques such as association analysis, classification and prediction, cluster analysis, and outlier analysis identify patterns in structured data[11]. These techniques can be used for traffic video analysis as well. Any of these techniques can extract or mark some kind

[10] Nvidia cuda video decoder, Reference Guide, Nvidia Corporation, online available: http://cseweb.ucsd.edu/ classes/wi15/cse262-a/static/cuda-5.5 doc/pdf/CUDA_Video Decoder. pdf

[11] S. Nagesh, Roll of Data Mining in Cyber Security, *Journal of Exclusive Management Science*, vol. 2/5, pp. 1-5.

of entity that is specific for some research at the moment. Entity extraction identifies particular patterns from data such as text, images, video or audio materials. It has been used to automatically identify persons, addresses, vehicles, and personal characteristics from some structured or unstructured source material. Here we define video data mining as finding correlations and patterns previously unknown, the current status of video data mining remains mainly at the pre-processing stage, in which the preliminary issues such as video clustering, and video classification are being examined and studied for the actual mining. Classification is a way to categorize or sassing class labels to a pattern set under the supervision. Decision boundaries are generated to discriminate between patterns belonging to different classes. The data set is initially partitioned into segments and the classifier is trained on the former[12]. Automated video classification from an input video stream is becoming of increased significance in multimedia information processing. For example, applications include identifying close-up video frames before running a computationally expensive recognizer. Each frame image can be transformed using discrete cosine transform or Hadamard transform.

For some video records, full video frame rate is not necessary, and frames can be decimated in time so that only one of several frames is transformed. This can reduce storage costs and computation times dramatically. The transform is applied to the frame image as a whole, rather than to small sub-blocks as is common for image compression. The transformed data are than reduced by discarding less significant information. This can be done using one of a number of techniques, for example, truncation, principal component analysis or linear discriminant analysis. With sufficient data reduction, it is simple to train a classifier to discriminate between typical traffic video scenes such as vehicles, traffic lights or pedestrians. For classification like this the principal component analysis works especially well, because the frames of similar images will have similar features. Clustering techniques group data items into clusters with similar characteristics to maximize or minimize intra cluster similarity, for example, to identify critical places on the road where accidents happens in similar way. This is especially important if the percentage of accidents on that road is high. Clustering consists of partitioning data into homogeneous groups, based on some objective function that maximizes the inter-cluster distance. Video clustering has some differences with conventional clustering algorithms. Due to the unstructured nature of video data, preprocessing of video data by using image processing or computer vision techniques is required to get structured format features. Another difference in video clustering is that the time factor should be considered while the video data is processed. Video clustering depending on some criterion clustering algorithms works with

[12] H. Chen, et al, Crime data mining: a general framework and some examples, *Computer,* vol. 37/4, pp.50-56.

video frames. The above mentioned video processing at the end of algorithm gives video output that must be watched and some critical frames marked. In computed based video processing pattern recognition algorithm puts markers through the video on critical places defined in advance by pattern recognition criteria. For example, if we want to trace specific car on some parts of road which is recorded with multiple cameras, we will define criterion for pattern recognition algorithm based on the car properties[13]. When all markers are sets, we can start clustering algorithm. For video clustering depending on the purpose we can use multiple clustering algorithms.

2.1 K-means Video Clustering

One of the clustering algorithms which can find abnormality in the video is k-means clustering algorithm. The k-means algorithm makes clusters which minimizes intra-cluster distance. Here it is important that k-means works with segments of video data. That means that video processed and compressed with H.264 decoder must be divided into segments and after that clustered. Clusters represent the relationship of the segments. In this context the segments are generated from incoming frames[14]. K-means clustering begins with k randomly placed centroids (points in space that represent cluster centers), and assigns every item to the nearest one. The algorithm then moves the cluster centers around in space in order to minimize distance between centroid and segments in created cluster. This is done iteratively by repeating two steps until a stopping criterion is met.

1) For every p P compute its nearest center in {c1, . . . , ck}. Partition P into k sets C1, . , Ck such that Ci contains all points whose nearest center is ci. Here P represents the input instance, and Ci represents clusters.

2) For every cluster C_i compute its centroid $C(C_i)$, i.e. the optimal center of that cluster. Then set $c_i = C(C_i)$ for every $1 \le i \le k$.

Another approach is heuristic. This approach selects random samples of points, and clustering these by k-means, selecting their initial k points arbitrarily. The *k* points that are the final centers are then used as initial centers in clustering the full dataset. This is known as *buckshot* technique and, like its namesake, its advantage is not in having any particular strong point, but is useful because it covers a wide area in which the intended target is likely to be found. Another advantage of the heuristic approach is its fast running

[13] D. Saravanan; S. Srininvasan, Video Image Retrieval Using Data Mining Techniques, *Journal of Computer applications*, vol. V/1, pp. 39-42.

[14] D. Dailey; F.Cathey; S. Pumrin, An algorithm to estimate mean traffic speed using uncalibrated cameras, *IEEE Transactions on Intelligent Transportation Systems*, vol.1/2, pp. 97-108.

time, which is especially important in video stream processing. In case of the data with a natural good k-clustering with reasonably sized clusters, this seed heuristic is very likely to pick one seed from each of the *k* intended clusters. Another technique developed for information retrieval purposes is bisecting k-means. Bisecting k-means have different approaches than traditional k-means. This technique groups the dataset initially into k clusters. Algorithm begins by treating the dataset as a single cluster. It repeatedly selects a cluster to split and computes several random two-means on the cluster. The lowest cost of these becomes the split, and the process repeats until k clusters are developed. This produces a hierarchy, or can be treated as a flat partition. The authors which proposed this technique used it on the largest cluster and found little difference compared to other techniques. Which technique will be selected for video processing depends on the current needs, the size of a video file and required processing speed.

Like we said earlier, k-means clustering algorithm is iterative algorithm. Processing speed in video clustering is very important. To speed up k-means clustering for big video data sets, and to speed up traffic pattern creation it is the best to use k-means implementation on the GPU[15]. For video compression we used GPU capabilities, and we can create, and cluster video segments on GPU, too. The motivation is to reduce the number of operations in the fragment processor. Data points to be clustered are stored in textures. The distance of each data point to every centroid is computed in parallel. The cluster label of each data point is identified after the computation of distances of each data point to all centroids is done. The computed distances are assigned to the depth buffer by the fragment program. The current distance in the depth buffer is compared with the distance that arrives from the fragment program. Writing the distances into the depth buffer continues until the distance computations to all the centroids are completed. In the implementation multiple depth buffers and stencil buffers are required to match the number of initial cluster centroids. The result is a speed-up in clustering between 1.5 to 3 times compared to the CPU implementation. For k-means implementation and for each GPU-based algorithms implementation some parts of algorithms are better to execute on CPU. More precisely, the best implementation is when we combine CPU and GPU performance. In that way we can take the best performance from both CPU and GPU architectures. From Figure 5 we can see that complex operations we can execute on GPU and less complex operations we can execute on CPU.

[15] A. Shalom; M. Dash; M. Tue, K-means Clustering Using Accelerated Graphics Processors, *Proceedings of 10th International Conference DaWak*, Turin, Italy, 2008, pp. 166-175.

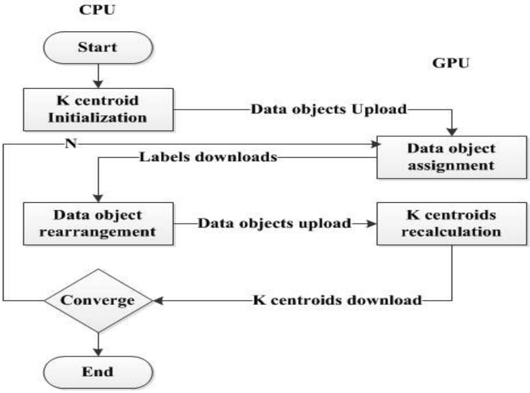

Figure 3: *The frame of GPU-based k-means*

When we use k-means clustering for video stream processing of the segments which are usual for that kind of road or some other road, a part will be concentrated in the cluster which represents the cluster with appropriate properties. Segments or frames which are unusual for that video or segments which have abnormal properties will not be in any cluster. For those segments we must see what that segments represents and what is abnormal in that part of the video. In this way we can create patterns of accidents on some critical road points, and try to find the solution for greater security.

3. Legal Regulations behind Software Implementation

All the mentioned facts about video monitoring, traffic surveillance, video clustering and video pattern recognition can be implemented in practice. Success rate depends on the hardware and software quality, and on the proper software use. The above presented idea for traffic surveillance solution cannot be implemented and used in real time without the appropriate legal regulations. For the purpose of legal regulations the authors focused on two laws: The Law on road traffic safety, and Criminal procedure code. These two laws are selected because of the logical need. For appropriate traffic surveillance, and pattern behavior creation we must know traffic safety regulations first. When all important articles are observed we can monitor traffic and record defects. At the end if some traffic accident or traffic offense is recorded we must have the legal regulations that describe how to use video materials as evidence in court. The Criminal procedure code provides such regulations. The most important connections between traffic video surveillance and legal regulation from these two laws are described below.

3.1 The Law on Road Traffic Safety

The Law on road traffic safety regulates the rules of traffic, the conduct of traffic participants, traffic restrictions, traffic signals, signs and instructions to which all traffic participants shall adhere, the conditions which drivers shall meet in order to drive a vehicle, driver's education, passing driving tests, right to drive a vehicle, issuing of driving licenses, issuing of the labels for disabled persons' vehicles, the demands vehicles shall meet, technical examinations, inspections and vehicle registration, special measures and powers applied to road traffic, as well as other issues related to road traffic safety[16]. This law shall regulate the basic prerequisites roads shall meet regarding the traffic safety, too. Traffic surveillance system in the purpose of traffic regulations and safety can be used by two institutions. These two institutions are defined in the Articles 2 and 9 of the Law on road traffic safety. Article 2 states that the control and direct regulation of road traffic shall be conducted by the Ministry of Interior – Traffic Police Department and the district police departments[16]. This article can be applied on the civilian population. Article 9 states: The Government, at the proposal of the Ministry in charge of the issues of traffic, shall establish the Traffic Safety Agency as a public agency. What Agency shall do is defined in paragraph 2. Points one to three from the paragraph 2 are important for traffic surveillance implementation, and they are presented in continuation. The Agency shall analyze, monitor and improve the traffic safety system (the development and application of a unified database essential for traffic safety); work on improvement of safety for drivers and other traffic participants as well as the enhancement of the traffic safety system from the perspective of vehicles; execute preventive and promotional activities in cooperation with centers for the promotion of public health and the Institute for Public Health, founded in accordance with regulations related to health protection, and shall conduct traffic safety campaigns.[17] Another road traffic coordination body is defined in Article 8. For the purpose of establishing cooperation and harmonized work efforts in order to improve road traffic safety, as well as initiation and monitoring of preventive or other activities related to road traffic safety, the Government shall form the Road Traffic Safety Coordination Body (hereinafter: the Coordination Body), as a coordination body of the Government composed of ministers in charge of the issues of traffic, interior affairs, health, labour, justice, education and trade and services. Executive bodies of autonomous territorial units or local self-government units and

[16] The Law of road traffic safety, "Official Gazette of the RS", № 41/2009, 53/2010, 101/2011, 32/2013 - decision US and 55/2014, article 2, paragraph 1.

[17] The Law on road traffic safety, "Official Gazette of the RS", № 41/2009, 53/2010, 101/2011, 32/2013 - decision US and 55/2014, article 9, paragraph 1, paragraph 2, point 1, 2 and 3.

municipal or city councils shall be allowed to establish a coordination body (a commission, council, etc.) aimed at harmonization of road traffic safety activities within their respective units. Establishment of expert work groups for the need of the Coordination Body, as well as organization and work of the Coordination Body shall be regulated by the act of the Government or the competent executive bodies.[18] When we are talking about traffic and traffic participants recording using the appropriate devices this Law declares that recording is possible and legal. According to Article 286: The authority responsible for traffic issues and the authority responsible for police issues are authorized to screen traffic, for the purpose of documenting traffic offences, conduct of traffic participants, traffic safety and flow. With this article all kinds of traffic video recording for the purpose of traffic surveillance are possible. The above mentioned authorities are not only the two organs that can record traffic on the road, but they are the basic ones. The authority responsible for traffic issues may, after previously obtaining the consent from the authority responsible for police issues, authorize the road manager, public enterprise and institution for traffic screening for the purposes referred to in previous paragraph.[19] In practice, this article provides for the use of vehicles with or without external police markings for traffic participants screening. For us here it is important that traffic video recording is legal, and that it can be implemented through the different public enterprise and institutions. Beside the mentioned use of the recorded video materials, these materials can be used in education too, more precisely in theoretic education. The curriculum for the theoretic education is defined in Articles 213 and 214 of this Law. Theoretical training for operating vehicles shall have elements which will enable the candidate to, after completing the training, acquire necessary knowledge and skills to independently and safely operate a vehicle in the road traffic. Video material can provide knowledge about driving behaviour, good and bad habits of drivers and a future driver can see different critical situations. In addition to this, based on video the instructors can explain which situations are legal, and which are not.

3.2 The Criminal Procedure Code

The third Criminal procedure code contains the rules whose aim is that no innocent person is convicted, and that perpetrators of criminal offences are sanctioned in accordance with the requirements provided for by the

[18] The Law of road traffic safety, "Official Gazette of the RS",№ 41/2009, 53/2010, 101/2011, 32/2013 - decision US and 55/2014, article 8, paragraphs 1 to 3.

[19] The Law of road traffic safety, "Official Gazette of the RS",№ 41/2009, 53/2010, 101/2011, 32/2013 - decision US and 55/2014, article 286, paragraphs 1 and 2.

Criminal Code and based on the lawfully conducted proceedings[20]. This Code also establishes the rules on conditional release, rehabilitation, termination of security measures and legal consequences of conviction, exercise of the rights of persons wrongly deprived of liberty and wrongly convicted, confiscation of proceeds from crime, resolution of restitution claims and issuance of wanted circulars and notices. Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required. The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files. One of the digital evidence can be traffic videos. In our country the criminal procedure code from 2010 provides in which cases video material can be used in court. Photographs or audio and video recordings of actions performed in accordance with this Code may be used as evidence and the court may base its decision on them. Photographs or audio and video recordings not encompassed by the provision of paragraph 1 of this Article may be used as evidence in criminal proceedings if their authenticity has been established and the possibility excluded of deliberate alterations of photographs and video recordings and if the photograph or video recording were made with the tacit or explicit consent of the suspect or accused person, where his image is on the photograph or his voice is on the recording. Photographs, audio recording, or audio and video recordings made against the wishes of the suspect of accused person, if his image is on a photograph or his voice is on a recording, may be used as evidence in criminal proceedings if the photograph or audio or audio and video recording contains another person, or the voice of that person, who tacitly or explicitly agreed to the making of the photograph, audio, or audio and video recording.[21] Article 132a, paragraph six, defines in which conditions video material can be used in court, in the case when material is recorded without permission of the person on the video. Photographs, audio recording, or audio and video recordings made without the tacit or explicit consent of a suspect of accused person but who are in them or whose voice is audible in

[20] The Law of Criminal procedure code, Gazette of the RS", Nos. 58/2004, 85/2005, 115/2005, 85/2005 – other law, 49/2007, 20/2009 – other law, 72/2009 and 76/2010, article 132a, paragraph 1,3,4.

[21] The Law of Criminal procedure code, Gazette of the RS", Nos. 58/2004, 85/2005, 115/2005, 85/2005 – other law, 49/2007, 20/2009 – other law, 72/2009 and 76/2010, article 132a, paragraph 1,3,4.

them, may be used as evidence in criminal proceedings, if the photographs, audio recording, or audio and video recordings were recorded as part of general security measures undertaken in public areas – streets, squares, parking lots, schoolyards, the compounds of various institutions and other similar public areas, in public facilities and premises – buildings housing public authorities, institutions, hospitals, schools, airports, bus and railway stations, sports stadiums and halls and other such public premises and attached open areas, as well as in shops, stores, banks, currency exchange offices, commercial facilities and other similar facilities where recording is regularly performed for security reasons.[22] From all these facts we can conclude that traffic video surveillance is legal and can be used as evidence in many cases. The question that arises is the accuracy of the video material that is used in court. The science of forensic video analysis is not what it used to be. The migration from analog video to digital video recording (DVR) systems changed the foundation of recording technology and the way video evidence is processed. The switch from analog to digital has also brought a dramatic change to the way the courts look at video evidence. Any investigator or prosecutor who hopes to use video in court must first ask the question of "authentication" when determining the admissibility of that video evidence. Yet, image accuracy is rarely considered, even when that evidence is crucial to support a criminal charge, or when that evidence is presented at trial.

3.3 Video as Evidence on Court aboard

Many courts in the United States have applied the Federal Rules of Evidence to digital evidence in a similar way to traditional documents, although important differences such as the lack of established standards and procedures have been noted. In addition, digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. Law-enforcement agencies in the United States are losing valuable video evidence daily because of poor practices, inadequate training and lack of equipment. Because of that they employed special investigators and organizations established to teach police how to properly recover, analyze, and interpret video evidence. For each video surveillance footage presented in court, it must be ascertained how the video was recorded, what influence the recording process had on the documented video, whether the transporting of the video deposition compromised the reliability of the footage and if all

[22] The Law of Criminal procedure code, Gazette of the RS", Nos. 58/2004, 85/2005, 115/2005, 85/2005 – other law, 49/2007, 20/2009 – other law, 72/2009 and 76/2010, article 132a, paragraph 6.

important video has been acquired of the episode in question. Consequently, video evidence must be above-board in order to gain credibility in court. There are so many things that come into play when using video surveillance as evidence in court. One thing is for sure, it's here to stay. In fact, studies reveal that when juries are presented with surveillance footage, the suspect is more likely to receive a conviction than if no video surveillance was used at all. However, it is not enough to bring video evidence to court and setup as if it was entertainment. Juries need to "get it" and to make sure that they do, the video must be clarified by one or several qualified professional witnesses. Over the past decade the US had become a surveillance society.

The events of 9/11 — along with concerns for responding to crime in our communities — have spawned an increase in government and business use of surveillance cameras. Chicago, for instance, has utilized a Department of Homeland Security grant to increase its city surveillance and projects a camera on every street intersection by 2016. Law enforcement's challenge with this proliferation of potential video evidence is in obtaining and preserving the images captured for future evidentiary value. The Office of the Privacy Commissioner of Canada issued in March 2006 a set of Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities.[23] Video surveillance of public places nonetheless presents a challenge to privacy, to freedom of movement and freedom of association, all rights taken for granted in Canada argues the Commissioner. This is especially true when the surveillance is conducted by police or other law enforcement authorities. The use of video surveillance to detect, deter and prosecute crime has increased significantly over the last few years. Police and law enforcement authorities increasingly view it as a legitimate tool to combat crime and ward off criminal activity—including terrorism. It is widespread in the United Kingdom and increasingly used by law enforcement and anti-terrorism authorities.

In the UK in case of a digital camera records, it is probable that the original would be the digital file representing the image. This does not represent a problem under the Law of England and Wales because if the original of a document no longer exists, copies or even copies of copies are admissible as evidence and it is irrelevant that the original was destroyed by the person seeking to produce the copy as evidence. Nor is it a problem in Scotland because although the general rule that copies of documents are admissible whether or not the originals still exist does not apply to visual images, copies of a document which no longer exists are admissible under the best evidence rule. The fact that a document is a copy goes to its weight as evidence, not

[23] Office of the Privacy Commissioner of Canada - Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities published on March 2006 and extracted on July 5, 2015 online available: https://www.priv.gc.ca

its admissibility. It will therefore be necessary for the user to be able to give evidence of the procedures used for generating, processing and storing digital images. So as to be able to prove that the image produced to the court is an accurate copy of the original. In general the court is likely to admit the evidence. However, the judge will direct the jury on the weight they should consider attaching to it.

In India the courts will have severe implications in all the cases where the prosecution relies heavily on the electronic data specially those cases where the audio-video recordings are produced in the form of CD/DVD before the court. The anticorruption cases are generally based on a lot of electronic/digital evidence and the CD/DVD forwarded to the courts are without a certificate and shall therefore not be admissible as evidence u/s 65B Evidence Act, which makes it mandatory to produce a certificate u/s 65 B(4). The failure to provide the certificate u/s 65 B(4) further occludes the judicial process as the expert view in that matter cannot be availed of until the preceding condition is fulfilled. It has been specified in the judgment that Genuineness, Veracity or Reliability of the evidence is looked into by the court subsequently only after the relevance and admissibility is fulfilled. The requirement to ensure the source and authenticity, pertaining to electronic records is because it is more vulnerable to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to mockery of justice.[24]The original recording in Digital Voice Recorders/mobile phones need to be preserved as they may get destroyed, in such a case the issuance of certificate under section 65B(4) of the Evidence Act cannot be given. Therefore such CD/DVD is inadmissible and cannot be exhibited as evidence, the oral testimony or expert opinion is also barred and the recording/data in the CD/DVD's do not serve any purpose for the conviction.

Ukraine courts are often left to sort out the he-said-she-said mess of traffic accidents. Because of the prevalence of scams, corruption, and insurance-motivated lying, judges rarely accept verbal evidence in these cases. The Ukraine Civil Code allows judges a ton of latitude in determining what evidence can be presented in court. Eyewitness testimony can be offered, but it is rarely given much weight because of the myriad of issues discussed above. Because of that in Ukraine the courts accept recorded video as evidence. Article 85-2 provides that each video recorded in pretrial can be used in court. By this article filming and video recording may be used during inspection, search, and reproduction of situation and circumstances and in the conduct of other investigative actions. Participants to the investigative action before its beginning are informed that filming, video recording will be used in the conduct of investigative action.

[24] Electronic Evidence/Digital Evidence & Cyber Law in India, January 6, 2015, online available: https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-

After filming, video recording and preparing film tape, video tape, the latter are shown to all participants to the investigative action and a separate record is drawn up thereon. Procedural processing of the filming, video recording, film tape and video tape demonstration in the conduct of another investigative action, in presenting records of the case in connection with completion of the pre-trial investigation, as well as during trial should be made in accordance with Article 85-1 of the Code of criminal procedure. The right which is most frequently referred to in this context and is generally most juxtaposed against the use of video surveillance is the right to privacy. The right to protection from arbitrary invasion of privacy is a fundamental human right, laid down in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. This means that everyone has the right to the protection of the law against such interference or attacks.

The European Convention on Human Rights also contains a similar provision protecting the privacy of its citizens. Claims in the European Court of Human Rights (ECHR) have been made pursuant to Article 8 of the European Convention on Human Rights which protects the "right to respect for private life". Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In the United States of America citizen's privacy is safeguarded by The Fourth Amendment. The Fourth Amendment's goal of protecting citizen privacy against unreasonable searches and seizures has been the major driving force behind much of the Supreme Court's Fourth Amendment jurisprudence. In court practice we can find some exceptions to the Fourth Amendment application. In 2001, the Court ruled on two Fourth Amendment cases involving aerial surveillance.[25] The first, California vs. Ciraolo, involved a defendant who grew large quantities of marijuana in his backyard. Since the defendant's yard was surrounded by a ten-foot-high fence, the police flew a plane over his house and took pictures of his marijuana crop. The police used these pictures to obtain an arrest warrant and, after failing to get the pictures suppressed, the defendant pled guilty to the cultivation of marijuana. The Supreme Court held that the aerial surveillance did not violate the defendant's rights. While acknowledging that the curtilage of one's property is generally protected under the Fourth Amendment, the Court made clear

[25] Video Surveillance as Legal Evidence, online available: https://www.linkedin.com/pulse/video-surveillance-legal-evidence-mike-bomas-llb-ll-m-acf.

that the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. The court decision like this provides free pass using for all video recorded over public areas.

3.4 Video as Evidence in the Republic of Serbia

In the Republic of Serbia the court practice shows that opinions about video use as evidence are divided. One case from the court in the town of Valjevo shows that the defendant was acquitted despite the video used as evidence. This defendant was employed in the market, and he was accused for stealing money from the cash register. The owner of the market presented the video from the surveillance camera to the court showing the accused taking money from the cash register. This video was dismissed as evidence because the accused did not know that the camera recorded him. The court found that the video cannot be used as evidence because it was not made with the tacit or express consent of the defendant, and was not created as a part of general security measures in the supermarket. This video was recorded only as a confirmation of the owner's doubts about the defendant's morality[26]. In another case, the appellate court in Belgrade rejected the appeal of the Prosecutor for Organized Crime and confirmed the verdict of the Higher Court in Belgrade K. Po1. br. 258/10 of 18. 07. 2012, based on the video recorded by the camera and audio recordings of telephone calls[27]. In this case the court found that it was not proven that the defendant (the owner of the car workshop) knew the origin of the vehicle. Also it was not proven that he knew how the vehicle was obtained, nor is it in any way involved in the actions that preceded the shipment of vehicles to his workshop. Video recordings from dashboard cameras, mounted in private cars, are not commonly used as evidence in court. Although the legal acts do not define the possibility of using video records that are obtained from the natural or legal persons, beside the authority for such processing prescribed in the law, video recordings from security cameras installed by such facilities, which are not authorized for treatment prescribed in the law, surely would not automatically be accepted by the courts. They should not be admitted as evidence by default, without first establishing the facts concerning the circumstances under which the recording was made, whether it is a snapshot of the result of the offense under Art. 144, 146, or another criminal offense defined by the Criminal Code. Another fact is that data processing must be

[26] Court practice –online bulletins, online available: http://www.sudskapraksa.com/sudske-odluke-presude-pravna-shvatanja.-najveca-baza-sudske-prakse-u-srbiji.html.

[27] Appellate court in Belgrade, online available: http://www.bg.ap.sud.rs/lt/articles/sudska-praksa/pregled-sudske-prakse-apelacionog-suda-u-beogradu/krivicno-odeljenje/organizovani-kriminal/kz1-po1-22-12.html.

carried out in accordance with the Law on Protection of Personal Data. As long as this area is not fully regulated by law (or laws), in precise and clear way, that will leave space for different interpretations, namely the use of such images in various administrative and judicial proceedings (misdemeanor, criminal, civil).

Conclusion

With increasing number of motor vehicles traffic, video surveillance systems become inevitable. From system like this an employee in control center can get a lot of information about traffic conditions, road bottleneck or vandal behavior. As we mentioned earlier, the operator must provide appropriate network transportations to the control center for all information that are collected from public cameras. According to Article 128 the operator is obliged to keep all data about electronic communications. These data must be kept at least twelve months from the date of the communication with the device[5]. The operator is obliged to keep data in original form, or as a data processed during the performance of activities electronic communications, which must be of the same quality and the level of protection as the data in its original form. On the other hand, the operator is not obliged to keep the data that are not manufactured or processed by him. The operator is obliged to retain the information so it can be accessed or supplied without delay. The data collected from road cameras or motion sensors could be more or less interesting for the employee in the control center. This means that in a concrete case some data are more important than others. Usually traffic conditions and the usual behavior of road users are not especially interesting. However, unusual or abnormal situations are especially interesting and important. Situations like these must be marked and processed. A lot of important information can be extracted from some parts of traffic video records. This information is used in order to provide better road security, reduce number of accidents and to provide easier prosecution of the culprits in road accidents. Better video processing means that some software solution must be used. Computer hardware architecture, and software implementation provides for a good quality of video processing. Different video standards for different records must be used in video processing.

All standards can be implemented for fast execution on GPU. With this processing we will get quality video output, but this is not enough. From this moment, data mining must be used. Data mining video classification and video clustering techniques are used to fast extract the required information from video recordings. In this way data mining techniques create patterns of accidents that occur in the same places from video recordings. That information is used to amend this section of the road and to prevent possible future accidents. Clustering can find abnormality in the traffic, so just the segment that represents a specific situation from the video record can be cut. These techniques would reduce processing time and provide for greater security and precision in video processing. Good processing of traffic video surveillance and mining of collected information will always provide for traffic improvement. For the future research the authors plan to use algorithms that can work with symbiosis of video and sensors dataset. From this symbiosis a lot of information could be provided for surveillance agencies. Systems like this provide digital evidence. Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence, it is vital that the determination of its relevance, veracity and authenticity is ascertained by the court and to establish if the fact is hearsay or a copy is preferred to the original. Different countries have different laws about video record as evidence on the court. As we explained above, this means that in some cases video recording will be used in the form of evidence and in the some cases will not.

References

1. Chen, H., Chung, W., Xu, J.J, Wang, G; Crime data mining: a general framework and some examples, Computer, Vol. 37, Iss. 4, pp. 50-56, 2004.
2. Cuda Samples, Nvidia Corporation [online], available: https://www.clear.rice.edu/comp422/ resources/cuda/pdf/ CUDA_Samples.pdf (30.01.2015.)
3. Dailey, D., Cathey, F., Pumrin, S.; An algorithm to estimate mean traffic speed using uncalibrated cameras. IEEE Transactions on Intelligent Transportation Systems, Vol.1, Idd. 2, pp. 97-108, June 2000.
4. Ingle, A., Dongre, S; A Survey on Data Mining Techniques for Surveillance of Real Time Video Streams, International Journal of Advanced Computer Research, Vol. 2, Num. 4, Iss. 6, December 2012.
5. Kale, V., Momin, F; Video Data Mining Framework for Surveillance Video, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 2, No.3, 2013.
6. Kim, M., Ok, S., Kim, D., Kim, S; GPU-accelerated H.264 Decoding for Video Surveillance, poster paper P4161, GPU Technology Conference, Category: Performance Optimization – P003.
7. Nagesh, S; Roll of Data Mining in Cyber Security, Journal of Exclusive Management Science, Vol. 2, Iss. 5, pp. 1-5, 2013.

8. Nvidia cuda video decoder, Reference Guide, Nvidia Corporation [online], available: http://cseweb.ucsd.edu/ classes/wi15/cse262-a/static/cuda-5.5 doc/ pdf/CUDA_Video Decoder. pdf (30.01.2015.)
9. Richardson, I; An Overview of H.264 Advanced Video Coding, Vcodex, 35 Regent Quay, Aberdeen AB11 5BE, United Kindom, pp.1-7, 2011.
10. Saravanan, D., Srininvasan, S.; Video Image Retrieval Using Data Mining Techniques, Journal of Computer applications, Vol. V, Issue 1, pp. 39-42, 2012.
11. Shalom, A., Dash, M., Tue, M.; Efficient K-means Clustering Using Accelerated Graphics Processors, Proceedings of 10th International Conference DaWak, Turin, Italy, pp. 166-175.
12. Thuraisingham, B., Khan, L., Masud, M., Hamlen, M; Data Mining for Security Applications, published in: International Conference on Embedded and Ubiquitous Computing, pp. 585-589, 2008.
13. The Law of Electronic Communications, „Official Gazette of the RS“, № 44/2010, 60/2013 - decision US and 62/2014.
14. The Law of Road Traffic Safety, „Official Gazette of the RS“, № 41/2009, 53/2010, 101/2011, 32/2013 - decision US i 55/2014.
15. The Law of Criminal Procedure Code, „Official Gazette of the RS“, № 89/2011.
16. Court practice –online bulletins [online], available: http://www.sudskapraksa.com/sudske-odluke-presude-pravna-shvatanja.-najveca-baza-sudske-prakse-u-srbiji.html,(10.2.2016).
17. Appellate court in Belgrade [online], available: http://www.bg.ap.sud.rs/lt/articles/sudska-praksa/pregled-sudske-prakse-apelacionog-suda-u-beogradu/krivicno-odeljenje/organizovani-kriminal/kz1-po1-22-12.html (10.2.2016).

PRAVNI ASPEKTI ALGORITAMA ZA ANALIZU PODATAKA ZA OBRADU NEPREKINUTOG TOKA PODATAKA U NADZORU SAOBRAĆAJA

Žaklina Spalević
Univerzitet Singidunum, Beograd
Miloš Ilić
Nebojša Arsić
Univerzitet u Prištini
Fakultet tehničkih nauka, Kosovska Mitrovica

Sažetak: Glavni izazov sa kojim se suočavaju sve bezbednosne organizacije i organizacije za prikupljanje obaveštajnih podataka jeste da precizno i efikasno analiziraju sve veći obim podataka o kriminalu. U mnogim oblastima video nadzor se može koristiti za tu namenu. Sistemi video nadzora se danas uobičajeno koriste na različitim mestima poput banaka, hotela, škola, samoposluga. Ovi sistemi u primeni su za nadzor u realnom vremenu ili za naknadnu proveru. U ovom trenutku sistemi za nadzor nemaju visoku inteligenciju i potrebni su ljudi da ih prate. Danas sistemi za video nadzor koriste i kamere za nadzor saobraćaja. Bilo da snimaju saobraćajne obrasce za buduća proučavanja ili služe za posmatranje i praćenje saobraćaja i izdavanje kazni za prekršaje, saobraćajne kamere su izuzetno popularan oblik video nadzora. Jedan od načina da se utvrde saobraćajni obrasci ili da se spreče saobraćajne nezgode i osigura bolja bezbednost na putu jeste i korišćenje tehnika za analizu podataka. Uz pomoć analize podataka, neprekinuti tok podataka sa mnoštva saobraćajnih kamera može se obraditi u realnom vremenu. Ovakvo svojsto moglo bi da obezbedi da se dogradi inteligencija u okviru sistema tako da bi oni mogli sami da donose odluke bez potrebe da ih ljudi prate. U ovom radu autori opisuju tehnike analize podataka za obradu neprekidnog niza podataka, otkrivanje obrazaca i nepravilnosti u sistemima za nadzor saobraćaja. Svaki video zapis i upotreba snimljenog video zapisa na sudu mora da bude pokrivena pravnim propisima. Autori su pregledali i izvukli odgovarajuće članove iz konkretnih zakona Republike Srbije koji se bave ovom vrstom problema.

Ključne reči: klasterovanje, analiza podataka, obrada neprekidnog toka podataka, nadzor saobraćaja, pravna regulativa, pravni sistem.