Jestr Journal of Engineering Science and Technology Review 6 (3) (2013) 119- 121

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Research Article

Intelligent Model for Video Survillance Security System

J. Vidhya, V. Deepika and K. John Singh*

School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India

Received 5 August 2013; Accepted 6 December 2013

Abstract

Video surveillance system senses and trails out all the threatening issues in the real time environment. It prevents from security threats with the help of visual devices which gather the information related to videos like CCTV'S and IP (Internet Protocol) cameras. Video surveillance system has become a key for addressing problems in the public security. They are mostly deployed on the IP based network. So, all the possible security threats exist in the IP based application might also be the threats available for the reliable application which is available for video surveillance. In result, it may increase cybercrime, illegal video access, mishandling videos and so on. Hence, in this paper an intelligent model is used to propose security for video surveillance system which ensures safety and it provides secured access on video.

Keywords: intelligent model, video surveillance

1.Introduction

In this hectic world CCTV's are being part of the routine life. The usage of CCTV's is increasing throughout the world due to the increase in burglary and terror campaign. It helps to solve and prevent from violence and protects the recruits and the public and private sectors like banks, hospitals and so on. As, the use of CCTV's increasing the threats are arising in so many ways. Security model has to be developed by considering all the possible threats that threatens the security and safety. In public places in order to provide security CCTV's are playing the major role[5]. This situation is very similar in business world like super markets, jewelry shops and so. In such places the requirement for CCTV's increasing more to tighten up the security system, which might reduce the robbery and solve theft cases. But in some places the video information might be sensitive and has to be kept confidential. At that point, when malicious people hacks such confidential videos, it might lead to many possible risks. For example, the video of an big private sector which is highly confidential is leaked out to in public which in result have caused an big economic problem. Countries throughout the world are aware of such situations, and in order to secure peace and security of their homel and they are trying to take necessary steps to prevent and protect from terrorism. Because of this reason, the progress in developing and deploying video surveillance technology are increasing rapidly [3]. As the evolution in video surveillance technology continues, technology advanced from CCTV to the digital recorder by using the IP based technology. As the need increases, researches to come up with solution to overcome the threats available in video surveillance system are also increasing and it is expected to continue in later years. USA government invests on video surveillance technology which is one among the four technologies it invests. Commonly, CCTV's are placed in public places and it records the video information. As the CCTV's deployed with prior permission, people who appear in it cannot create chaos. Such gathered video information can be used to solve criminal and theft cases. Even though there is numerous advantages in video surveillance system, people are alarmed due to the wide use CCTV's. Because, gathered video information that might be misused by malicious people. So, here this paper is to propose an intelligent model for video surveillance system to ensure the security and the safety of gathered video information[2].

2. Realted works

ICCTV (Intelligent Closed Circuit TV)uses a super computer to evaluate the videos of human activities to avoid the unusual activities occur. The CCTV's are mostly deployed on the real time environment on the bases of vendor's request. And by default it is deployed in the public areas such as road, hospitals, bank and so on. Deploying the CCTV's not only surveillances but also helps to protect from huge accidents. For example, it may able to detect the terrorist, who is acting too normal like others in a public place. Praetorian is an integration of many surveillance technologies which includes COTS (commercial off the shelf) [1].

I n Praetorian operators act actively to stop the active threats as there were allowed to see the actual video by which their can able to analysis the threats that cause damage to the video. Praetorian increases the awareness on the active threats, and also the operator can able to realize the responsibilities there are in, which in result ensures the security of the video. DRM based frame work is used for video surveillance which protects the privacy of the people

* E-mail address: johnsinghaj@yahoo.com

who are surveilled and also supports for effective surveillance. In the intra macro block, the coefficients are transformed to flip the sign Pseudo-randomly.

In the Open Network Video Interface Forum the Network Video Client and the Network Video Transmitter are used. In that, Network Video Transmitter(NVT) is used to send the data through an IP network to the Network Video Client(NVC). And the NVC is used to control the device which is used to transfer video through an NVT. By this way the transparency of the video can be secured. The sign of transform coefficients for intra macro-block is pseudo-randomly flipped, which in result only the authorized user can able to decode it[4].

3. Proposed system

An IP(Internet protocol) camera is an kind of digital camera mostly deployed for monitoring in the public areas and it can able to send data back and forth through computer network. IP camera is used for the surveillance purpose and in the process of surveillance it captures the activities and things going around the place. IP camera not only captures the video simply but also stores the video. In order to monitor and use it as evidence if any accident occurs. It Stores the video captured in the temporary memory. Mostly IP cameras are deployed in the public places which involves so many people in it. Since it is an sensitive matter, the video has to be protected from malicious people which may arise sensitive issue. To avoid this type of situation video is to be encrypted.

So, that only the authorized users may able to access and view the video. As soon as the data is captured from the camera it gets stored in the temporary memory. In the process of capturing video several steps are taken. Firstly, using an ADC (Analog to Digital Converter) the analog signals is digitalized. The chrominance and the luminance are separated if it is an composite video. In order to produce color variance the chrominance is to be demodulated. So, the modification in data such as adjusting the brightness, saturation and contrast can be done. And for the convenient usage of data in any color space standard, color space converter is used to transform the data. And the video encoding is done along with that process. After that the data has to be encrypted from main memory. And to access the video file, user has to able to clear the authorization control part. To access the encrypted video password must be provided which is set by the sender or administrator. Then user can able to view the decrypted video. Normally, videos are transmitted to monitor through the video cable or a Digital Video Recorder (DVR) which is a type of network camera that transmits video through data connection like USB. In order to transfer video through the network, all the requirements are put up into single unit. Then it can be directly connected through network and the video is saved in the memory space of another device to which the network is connected based on the type of camera in which the video is captured.

In security for video encryption many algorithms where proposed to implement it in real time. Here in order to protect video from intruders we proposed AES(Advanced Encryption Standard) algorithm which secures the data by doing perfect job in encryption. In fig 1, the main purpose of encryption is to secure the confidentiality of the video. AES algorithm encrypts the video by splitting it into key. AES algorithm splits the data into number of rows and columns. And using the Sub Bytes step, the bytes will be replaced with the Sub Bytes. It is possible using an 8 bit substitution process. So, it changes the actual content of the original video. And using the Shift Rows, the bytes in the each row are shifted to their left. The numbers of count in shifting bytes differ in each row. And the four bytes in the state is taken as input which in result gives four bytes as output. Even a single byte in the input affects all four bytes in output. It creates diffusionin cypher by using Mix Columns and the Shift Rows together. It encrypts the data in a way which is not easy to decrypt. But smart hackers always have their way to decrypt the encrypted video. In fig 1, to protect video from that type of situation, the video is saved into PDA form instead of avi or mpeg. The original data will be in the avi format. When the video is encrypted, the video format is automatically changed into the pda form. So, that the malicious people would have no idea about the file. After changing the file format we are going to use AES algorithm and the video gets encrypted. It increases the security of the video and also reduces the possibility of intruders trying to access it. And also the quality of video will be same after decrypting as before encrypting. This proposed work is an efficient way to increase the security of the video surveillance system.

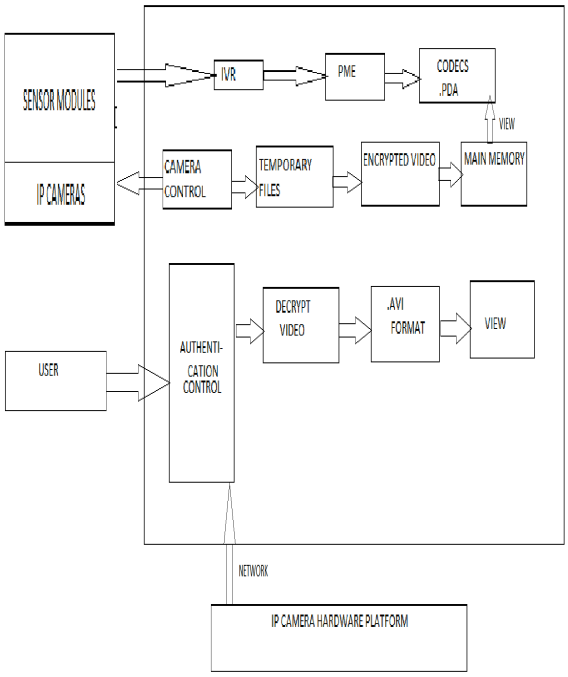

Fig 1. Working of ip camera and encryption, decryption of surveillance video

4. Results & Discussion

Firstly, the surveillance video is loaded. Then the video which needs to be encrypted is loaded. The video in the .avi format can be converted into PDA file. And accessing file would be difficult. As the format of data is changes from .avi to PDA, reduces the threats for video and ensures security. And then we used AES algorithm to encrypt with more security level. Now the video which is to be decrypted is loaded. And then the encrypted file will be decrypted back to original video. The security on video surveillance is becoming quite a challenging task.

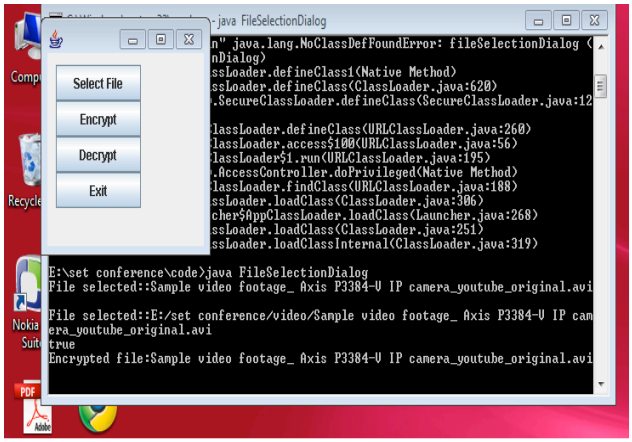

Fig 2..Encrypting video

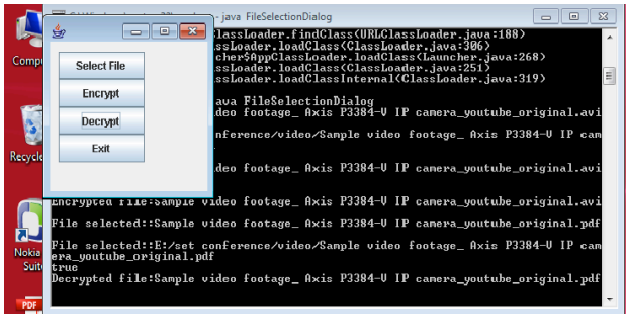

Fig 3. Decrypting video

To ensure the privacy of people in the surveilled video, it has to be secured. So, in order to secure the video it needs to be encrypted and the attention drawn to it as to be reduced. To achieve this video is to be changed from one format to other. Here we proposed a model where in ensures the security of video and also changes video from the actual format to some other format. So, it reduces the possibility of intruders accessing it.

5. Conculsion

This paper provides an intelligent model for protecting and ensuring the video surveillance system. And to ensure the security of the data video is encrypted. In the process of encryption, AES (Advanced Encryption Standard) algorithm is used which involves so many steps which in result it increases the complexity in encryption. So, it increases the security of the video. And the quality of the data remains the same after encryption and decryption. After encrypting video, it doesn't look like an actual video. The video will be displayed in like some other video. AES algorithm also applied for providing more security. So, that it reduces the possibility of intruders. This paper ensures the security of video surveillance system.

References

1. B. Karasulu, "Review and evaluation of well-known methods for moving object detection and tracking in videos",In Proceedings of Journal of Aeronautics and space technologies, pp 1-10,2010.
2. Jing wang, **"**Video Volume Segmentation for Event Detection", In Proceedings of IEEE International Conference on Computer Graphics ,Imaging and Visualization, pp.311-316, 2009.
3. P. Carrillo and H. Kalva and S. Magliveras, "Compression independent object encryption for ensuring privacy in video surveillance", In Proceedings of IEEE International Conference on Multimedia and Expo, pp 273-276, 2008.
4. ShensJie and ZhengXiaoYu,"Security for Video Surveillance with Privacy", In Proceedings of IEEE International Conference on Internet Technology and Applications, pp 1-4, 2010.
5. F. Dufaux and T. Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems", IEEE Transactions on Circuits and Systems for Video Technology, pp 1168-1174, August 2008.
6. Geon-Woo Kim and Jong –Wook Han "Security model for video surveillance System", In Proceedings of IEEE International Conference on ICT Convergence, pp 100-104, 2012.