International Journal of Engineering & Technology, 7 (2.33) (2018) 151-154

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment

Dong hyeok Lee [1], Nam je. Park [2] *

[1] Elementary Education Research Institute, Jeju National University
[2] Department of Computer Education, Teachers College, Jeju National UniversityIljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
**Corresponding author E-mail: namjepark@jejunu.ac.kr*

Abstract

Background/Objectives: Big data environment is being realized. Recently, intelligent public safety environment on the foundation of the image processing technique based on big data is being introduced, and accordingly, processing CCTV images is becoming more important day by day.
Methods/Statistical analysis: In this paper, an efficient technique to send image information for mass cloud storage environment was proposed. With the offered method, only the ROI area is extracted and partial object images are transmitted, and it has the strengths of higher efficiency and protected privacy with the application of a masking technique.
Findings: it is general to apply the masking technique partially to face information, and in this study, the privacy of the image data registered in the cloud storage was to be protected based on this masking technique, and an efficient data transmission structure grounded on ROI area extraction was proposed.
Improvements/Applications: With the offered method, only the ROI area is extracted and partial object images are transmitted, and it has the strengths of higher efficiency and protected privacy with the application of a masking technique.

Keywords: *Virtual Facial; Privacy Protection; Intelligent CCT; Big Data; CCTV*

1. Introduction

Recently, CCTV (Closed Circuit TeleVision) surveillance service based on cloud is drawing attention. Image data taken by CCTVs has the feature of big volume demanding large storage space, so the CCTV surveillance environment is appropriate for cloud environment that can offer mass storage. However, cloud environment is exposed to different threats to security, for instance, hacking of communication and database by an outsider and an attack by an insider, so CCTV image data needs a strong security system. The development of cloud and big data environment has resulted in many changes. In particular, the image information processing technology is at the stage of making rapid progress repeatedly through big data, and recently, the rate of identifying image object has come close to a reliable level. With this technology, the environment of intelligent public safety based on CCTVs will expand more, and will offer us safer life surroundings. However, CCTV image data has the feature of mass data, and it brings about the limit in terms of data storage. It seems like the improved image quality of CCTVs later will make the size of image data bigger, which demands mass storage, and it is directly connected to the cost problem in image data processing. Therefore, at present, images taken by CCTVs are removed after a certain period. Of course, it's desirable to delete images from storage that have accomplished the goal of public safety, but in case of the images that should be stored for a particular purpose, they need to be kept for a long term, and a separate measure is necessary for the disposal of these mass images.

Figure 1 displays a cloud-based CCTV surveillance system model. Images taken by a CCTV are stored in a cloud server via the Internet, and the cloud server offers real-time image data to the surveillance system. In this process, encryption of CCTV image data is required. Yet, overhead of encryption itself exists in quality, so an efficient encryption method proper for mass data is necessary1-7.

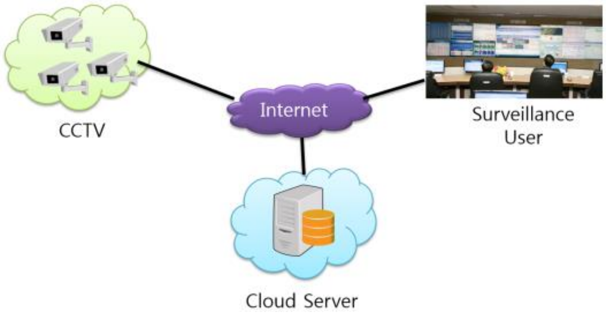

Fig. 1:. Cloud-CCTV Surveillance Model.

On the other hand, image data also has the problem of privacy protection. At present, the legislation of the personal image data protection law is proceeding, and the service provider dealing with images that make personal identification possible has the duty to protect objects' privacy safely. Cloud environment involves a variety of threatening factors including data leak by an insider and infringement by an outsider, so information protection must be considered. Yet, if all the image information becomes encrypted, decoding incurs expenses, so it's inefficient. Therefore, it's general to apply the masking technique partially to face information, and in this study, the privacy of the image data registered in the cloud storage was to be protected based on this masking technique, and an efficient data transmission structure grounded on ROI area extraction was proposed[8-13].

2. Related research

Currently, diverse products that manage CCTV image information safely have been released in Korea and other countries. A variety of products, such as Intelligent Video Analytics and Smart Surveillance System by IBM, exist, and New York City, U.S.A., has established and is running the DAS (Domain Awareness System) developed with the cooperation of Microsoft. When the images of a CCTV are processed, the protection of the privacy of the objects in the images is essential, and different ways have been suggested to protect the image information of CCTVs. In particular, the method most frequently used in order to protect the privacy of objects is the masking technique, the object non-identification way to process the area of face by masking so that it cannot be discerned. As a similar technique, the technique of scrambling the privacy area with the standard format of MPEG-4 has been proposed, and the method to extract and encrypt a ROI area of real-time video images has been suggested, too [1].

On the other hand, the Ministry of National Defense is proceeding the D-Net Project that analyzes the images taken by CCTVs and drones as big data and takes action, and DARPA in the U.S.A. is proceeding the VIRAT Project to automatically recognize certain actions of image data, and the Mind’s Eye Project to analyze situations and behaviors and anticipate what's going to happen next. In this paper, the way to protect image data of CCTVs more efficiently and safely was to be proposed. The suggested way is not sending the whole image, but treating image through privacy masking targeting ROI area based on object recognition and then sending it, so it is safe and efficient[13], [14-17].

3. Suggested method

The outline of the way suggested in this research is as in (Figure 2). A CCTV sends target data images to a cloud server. At this point, it doesn't send the whole images but just some parts after judging the ROI of the images. ROI gets rid of fixed area on the ground of object identification based on big data and then sends only the object area. As for the fixed background area, image files are stored separately and if necessary, images can be combined and processed. A cloud server receives this partial image data and keeps it in storage. The background image around a CCTV is registered in a cloud server in advance, and regarding partial image data, this image information and partial image go through mapping and become stored.

Afterward, when a smart surveillance system asks for an image from a cloud server, the cloud server composes a target data image and a background image, and delivers the composed outcome to a smart surveillance system. At this point, if necessary for detailed decoding of the image information, the smart surveillance server can request a partial image or processes by demanding the background image separately. The main content of this method is not storing the whole images taken by a CCTV, but storing fixed background images as relatively small volume of images and not as video images, and it has the characteristic that, regarding image data, only moving objects based on object identification in the environment of big data are stored as video images.

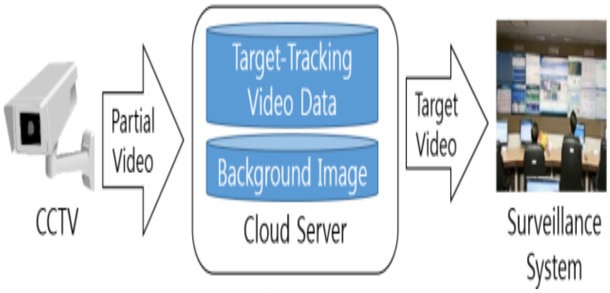

Fig. 2: ROI-based Efficient Video Data Processing.

The process of partial image sampling of a CCTV is as in (Figure 3).

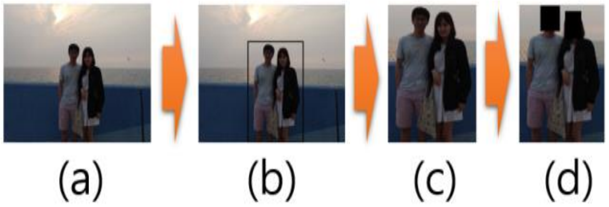

Fig. 3: The Process of Partial Image Sampling of A CCTV.

The detailed explanation about (Figure 2) is as the followings.

a) It shows the image as it is taken by a CCTV.
b) ROI area is extracted based on object identification.
c) Except for the ROI area, all the other background parts are eliminated.
d) For the protection of privacy, a target's face is recognized and processed by masking.

Only the partial images processed this way are sent to a cloud server. The masking images are sent and stored between a cloud server and a CCTV, so it is possible to protect the privacy of the object shot in images. A cloud server doesn't have the right to lift masking images. If masking needs to be lifted, object unmasking can be conducted in a smart surveillance system based on the encryption key shared by a CCTV and the smart surveillance system in advance. Encryption key is directly connected to the problem of personal information protection of the shot object, so it needs to be managed safely.

4. Proposed GCTR-AES encryption

Table 1: explains the suggested GCTR-AES encryption operation mode.

Table 1:.Abbreviation

Abbreviation	Content
ds	the size of the whole encryption data
sid	the initial value of a bucket I.D.
s	the seed value of pseudorandom numbers
$P(data)_n$	the occurrence value of the nth pseudorandom numbers with Data as the initial value
H(data)	H(data) the outcome value of the hash of data

Figure 4. shows the size of each bucket and how to create an ID. Prior to this, the sizes of the bucket groups need to be determined. In Figure 2, the size of the bucket group unit was decided as 100. In other words, plural bucket IDs are assigned to one bucket group unit, and each bucket ID has a different bucket size. Here, the bucket size is determined based on pseudorandom numbers with sid as an initial value. Figure [2] below shows five buckets included in one bucket group [16-23].

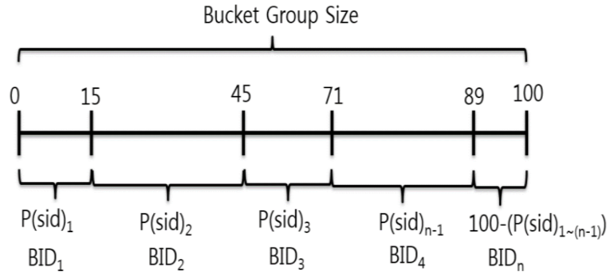

Fig. 4: Bucket Group.

The side necessary for pseudorandom numbers can be created as below with the initial seed and the XOR value of the whole encryption data size.

$$sid = H(s) \oplus H(ds)$$

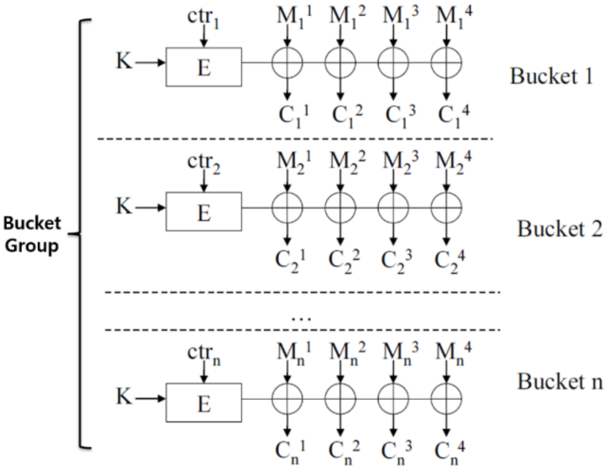
K
E
ctr_1
M_1^1 M_1^2 M_1^3 M_1^4
C_1^1 C_1^2 C_1^3 C_1^4
Bucket 1
ctr_2
M_2^1 M_2^2 M_2^3 M_2^4
C_2^1 C_2^2 C_2^3 C_2^4
Bucket 2
Bucket Group
...
ctr_n
M_n^1 M_n^2 M_n^3 M_n^4
C_n^1 C_n^2 C_n^3 C_n^4
Bucket n

Fig. 5:.AES-GCTR Mode.

Figure5 shows the process of how to encrypt into AES-GCTR operation mode. N buckets belong to one bucket group, and each bucket has the same encryption vector value. Therefore, when partial images are extracted in the unit of a particular bucket, they come to have the same encryption vector value, so can display more efficient encryption performance than AES-CTR mode. In other words, for encryption and decoding, AES-CTR operation mode needs the creation of different encryption vectors for each counter, but the proposed method is efficient because only one time of vector calculation is carried out within the same bucket.

5. Safety analysis

The suggested method can be analyzed as follows in terms of efficiency and safety.

1) In terms of efficiency : As not all the whole image data is sent but only the ROI area where an object has been identified is transmitted partially, the efficiency of transmission can be improved much, and bandwidth can be reduced in sending data.
2) In terms of safety: Data with face area processed by masking is transmitted between a CCTV and a cloud server, so even when a sniffing attack occurs against image information, an object's privacy can be protected. On the other hand, if image data of a cloud server becomes exposed by an outsider, only the masking data can be obtained, and the actual object cannot be identified, so it's safe.

6. Conclusion

In this paper, AES-GCTR mode that has improved AES-CTR mode was suggested. The proposed method can make encryption and decoding performance more efficient, and is expected to be easily applied to the image surveillance system based on CCTVs that demands high capacity processing and real-time streaming. The next-generation intelligent public safety environment will offer different services, such as object recognition and tracking based on big data, behavior recognition, anticipation of situation and etc., and it will guarantee safety in our life. In this paper, the way to process the images of CCTVs, the technique element indispensible in the environment of intelligent public safety, was examined. In particular, the method to send partial images based on ROI extraction which can enhance the efficiency of transmission and the technique to protect an object based on privacy masking were suggested. The area of processing CCTV-based images and personal information protection will become more and more important, and it needs continued research.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [2017-0-00207, Development of Cloud-based Intelligent Video Security Incubating Platform] and this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (NRF-2016R1D1A3A03918513).

References

[1] S. Aramvith, S. Pumrin, T. Chalidabhongse, and S.Siddhichai, "Video Processing and Analysis for Surveillance Applications", in Proc. Int. Symp.Intelligent Signal Processing and Communication Systems pp.607-610, 2009.
[2] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, Howon Kim, WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", LNCS, Advanced Web and Network Technologies and Applications, 2016, Vol.3842, pp.741-748.
[3] H. M. Moon and S. B. Pan, "A New Human Identification Method for Intelligent Video Surveillance System", in Proc. IEEE Int. Conf. Computer Communications and Networks, Switzerland, Aug. 2010.Park, J., Shin, S., Kang, N., Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things, J. Korea Inf. Commun. Soc., 2013, 38, pp.707–714.
[4] Hae-Min Moon, Sung-Bum Pan, "The Analysis of De-identification for Privacy Protection in Intelligent Video Surveillance System", Journal of Korean Institute of Information Technology 9(7), pp.189-200, 2011.7.
[5] Park N, Bang H-C, Mobile middleware platform for securevessel traffic system in IoT service environment, Security Communication Network, 2016, 9(6), pp.500–512.
[6] H. M. Moon, C. H. Seo, Y. W. Chung, and S. B.Pan, "Privacy Protection Technology in Video Surveillance System", in Proc. Int. Conf. Embedded and Multimedia Computing, pp. 160-165, Dec. 2009.
[7] Lee D, Park N, Geocasting-based synchronization ofAlmanac on the maritime cloud for distributed smart surveillance, J Supercomput, 2016, 73(3), pp.1103–1118.
[8] Park N, Hu H, Jin Q, Security and privacy mechanisms forsensor middleware and application in internet of things (IoT), IntJ Distrib Sens Netw, 2016, Article 2965438.
[9] Do-Kim Gwon Woo, Han Jong Wook, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 1623-1624, 2009.
[10] Park N, Kang N, Mutual authentication scheme in secureinternet of things technology for comfortable lifestyle, Sensors, 2016, 16(1), pp.1–16.
[11] Yeonghae Ko, Namje Park, A Study of IT Centered Smart Grid's STEAM Curriculum and Class for 3rd and 4th Graders in Elementary School, Journal of the korean association of information education, 2013, Vol.17 No.2 pp.167-175.
[12] Jaewan Shin, Shin Dong Kyoo, Shin Dong Il, "Design of Brain-Computer Interface System for User Intention Recognition", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 2013.6, pp. 790-791
[13] Park N, Kim M, Implementation of load management application system using smart grid privacy policy in energy management service environment, Clust Comput, 2014, 17(3), pp.653–664.

[14] Chang Gi Kim, Jeong Min Seo, "An Design and Implementation of Navigation System for Visually Impaired Persons Based on Smart Mobile Devices", JOURNAL OF THE KOREA CONTENTS ASSOCIATION, 2015, 15(1), pp.24-30.

[15] Park N, Implementation of inter-VTS data exchange formatprotocol based on mobile platform for next-generation vessel trafficservice system, Int Inf Inst (Tokyo) Inf, 2014, 17(10A), pp.4847–4856.

[16] Dong-Eun Kim, Kwee-Bo Sim, "A Study on the Relation between EEG and Strength for Artificial Hand Control", Proceedings of Symposium of the Korean Institute of Intelligent Systems, 2013.10, pp.121-122.

[17] Park N, Park J, Kim H, Inter-authentication and sessionkey sharing procedure for secure M2M/IoT environment, Int InfInst (Tokyo) Inf, 2015, 18(1), pp.261–266.

[18] Dong-Eun Kim, Je-Hun Yu, Kwee-Bo Sim, "EEG Feature Classification for Precise Motion Control of Artificial Hand", Journal of Korean Institute of Intelligent Systems 25(1), 2015.02, pp.29-34

[19] Park N, Implementation of inter-VTS data exchange formatprotocol based on mobile platform for next-generation vessel trafficservice system, Int Inf Inst (Tokyo) Inf, 2014, 17(10A), pp.4847–4856.

[20] Luo, Ying, Shuiming Ye, and S. Cheung Sen-ching, "Anonymous subject identification in privacy-aware video surveillance." Multimedia and Expo (ICME), 2010 IEEE International Conference on. IEEE, 2010.

[21] Park N, Implementation of terminal middleware platformfor mobile RFID computing, Int J Ad Hoc Ubiquitous Comput, 2011, 8(4), pp.205–219.

[22] Lee Hyun Ju, Shin Dong Il, Shin Dong Kyoo, "A Study on the system design for analysis of EEG signals", Proceedings of Symposium of the Korean Institute of communications and Information Sciences , 2014, pp.610-611

[23] Park N, Performance analysis for VTS-based dataexchange protocol in e-navigation environment. Int J MultimedUbiquitous Eng., 2016, 11(1), pp.337–344.

[24] Yong-Hee Lee, Chun-Ho Choi, “Pattern classification of the synchronized EEG records by an auditory stimulus for human – computer interface”, Journal of the Korea Institute of Information and Communication Engineering, 2008, 12 (12) , pp. 2349-2356.