International Journal of Smart Home
Vol.8, No.2 (2014), pp.7-14
http://dx.doi.org/10.14257/ijsh.2014.8.2.02

Design of City Logging System using Searchable Image Encryption System of Streaming Service

NamHo Kim[1] and SeongHo Lee[2]

[1] *Dept. of Internet Contents,Honam Univ., Korea*
[2] *UC Ltd, Korea*
nhkim@honam.ac.kr, wideview06@hanmail.ne

Abstract

In this paper, we propose a city-logging system to collect various types of data around the roads using mobile observation equipment. Since the collected image data from CCTV contains several things which can violate someone's privacy, we present a secure method to search CCTV image using searchable image encryption system. In addition, we illustrate a city-info service which can be provided by analyzing the collected data. Implementation and testing of the proposed system will be carried out in future.

Keywords: *City logging, Life logging, Searchable image encryption system (SIES), CCTV images*

1. Introduction

According to the advancement of the Internet and information technology, both systems and services related to life logging are on the increase. Life logging is called as a service to upload data on certain web sites regardless of the location and time [1, 2]. These life logging systems include Facebook, twitter and so on.

Life logging is caused by the demand to record all things of our life and to implement a complete memory. In order to actualize an era of complete memory, the mobile devices of digital sensing and digital recording for life logging have been developed. In addition, the technology of retrieval and analysis for the stored information has been developed, which improves the usability of data. City logging is a variation on life logging where the concept of life logging is applied to city information. In other words, the city information is recorded by a city logging system with respect to city environmental information and the urban interaction images.

In this paper, we propose a city logging system to collect city information in relation to roads using mobile observation equipment. The city information includes CCTV images, GPS, temperature, humidity, luminous intensity and so on. The city information may include private information in connection with CCTV images of the urban interaction. To resolve the problem of private life images, we apply searchable image encryption system (SIES) to our city logging system. SIES provide privacy and authentication on streaming media of the cloud computing environment [3].

This paper is organized as follows. In Section 2, we show the architecture of our city logging system. In Section 3, the secure method for CCTV image search using SIES is presented. In Section 4, we illustrate a city-info service which can be provided by analyzing collected data. Finally, we present our conclusion and future work in Section 5.

2. Related Work

ISSN: 1975-4094 IJSH

In this section, we describe the related work of video compression to apply SIES and City Logging System.

2.1. Searchable Encryption System

In searchable encryption system (SES), the subject of information referred the document. That is, the document is the information users want to hide. Hence, the user provides information on a server to retrieve documents is called a keyword. In general, the data contained in the document as a set of keywords is defined as Eq. 1:

$$D=\{W_1, W_2, \cdots, W_n\} \quad \text{(Eq. 1)}$$

The searchable encryption system consisting of four steps is pictured in Figure 1.

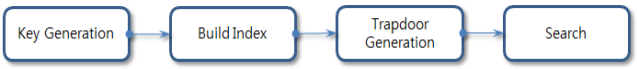

Figure 1. The 4 Steps of Searchable Encryption System

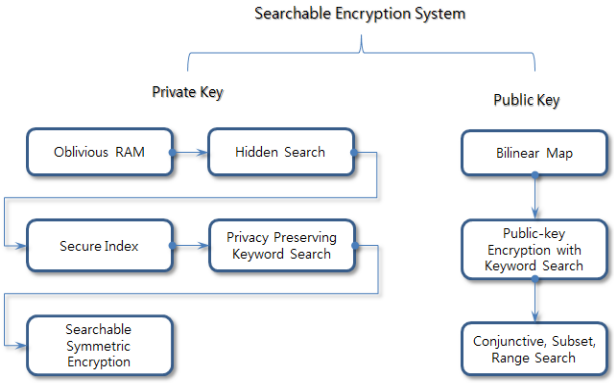

Figure 2. Private Key and Public Key of SES

The searchable encryption systems of personal information stored in external storage space that occur as a workaround for the many problems have been studied until now. As shown in Figure 2, SES of the users' encryption keys can be classified into public key and private key [4-10].

2.2. Data Compression

In computer science and information theory, data compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation. Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it. The process of reducing the size of a data file is popularly referred to as data compression, although it's formal name is source coding (coding done at the source of the data before it is stored or transmitted). Compression is useful because it helps reduce resources usage, such as data storage space or transmission capacity. Because compressed data must be decompressed to use, this extra processing imposes computational or other costs through decompression; this situation is far from being a free lunch. Data compression is subject to a space-time complexity trade-off. For instance, a compression scheme for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being

decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage. The design of data compression schemes involves trade-offs among various factors, including the degree of compression, the amount of distortion introduced (*e.g.*, when using lossy data compression), and the computational resources required to compress and uncompressed the data.

2.3. Video Compression

Video compression uses modern coding techniques to reduce redundancy in video data. Most video compression algorithms and codecs combine spatial image compression and temporal motion compensation. Video compression is a practical implementation of source coding in information theory. In practice, most video codecs also use audio compression techniques in parallel to compress the separate, but combined data streams as one package. The majority of video compression algorithms use lossy compression. Uncompressed video requires a very high data rate. Although lossless video compression codecs perform an average compression of over factor 3, a typical MPEG-4 lossy compression video has a compression factor between 20 and 200. As in all lossy compression, there is a trade-off between video qualities, cost of processing the compression and decompression, and system requirements. Highly compressed video may present visible or distracting artifacts. Some video compression schemes typically operates on square-shaped groups of neighboring pixels, often called macroblocks. These pixel groups or blocks of pixels are compared from one frame to the next, and the video compression codec sends only the differences within those blocks. In areas of video with more motion, the compression must encode more data to keep up with the larger number of pixels that are changing. Commonly during explosions, flames, flocks of animals, and in some panning shots, the high-frequency detail leads to quality decreases or to increases in the variable bitrate.

2.4. H.264

H.264/MPEG-4 Part 10 or AVC (Advanced Video Coding) is a video compression format, and is currently one of the most commonly used formats for the recording, compression, and distribution of video content. The final drafting work on the first version of the standard was completed in May 2003. H.264/MPEG-4 AVC is a block-oriented motion-compensation-based codec standard developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC JTC1 Moving Picture Experts Group (MPEG). The project partnership effort is known as the Joint Video Team (JVT). The ITU-T H.264 standard and the ISO/IEC MPEG-4 AVC standard (formally, ISO/IEC 14496-10 – MPEG-4 Part 10, Advanced Video Coding) are jointly maintained so that they have identical technical content. H.264 is perhaps best known as being one of the codec standards for Blu-ray Discs; all Blu-ray Disc players must be able to decode H.264. It is also widely used by streaming internet sources, such as videos from Vimeo, YouTube, and the iTunes Store, web software such as the Adobe Flash Player and Microsoft Silverlight, and also various HDTV broadcasts over terrestrial (ATSC, ISDB-T, DVB-T or DVB-T2), cable (DVB-C) and satellite (DVB-S and DVB-S2). H.264 is typically a lossy compression, but it is possible to create lossless encodings with H.264.

3. Architecture of a City Logging System

Our proposed city logging system is composed of mobile observation equipment and a city logging server. Mobile observation equipment is installed on running vehicle which senses the information of environment around the road. After sensing, mobile observation equipment transfers its obtained data to a city logging server. The server stores streaming data and text

received from much mobile observation equipment on roads. And then, the server analyzes its stored data for city-info services which will be provided in future. Figure 3 shows the sequence diagram for our city logging system.

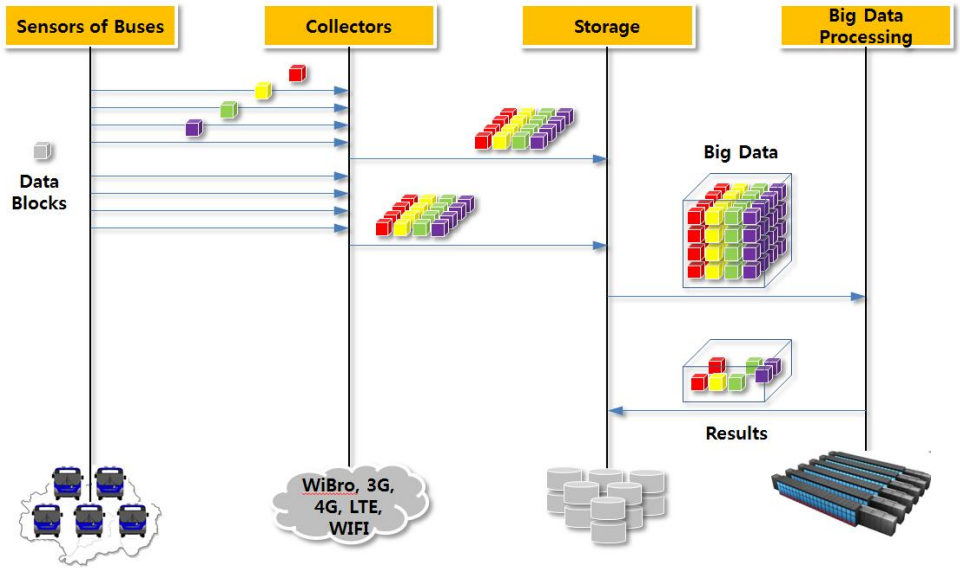

Figure 3. The Schematic Outline of our proposed App

4. Applying SIES to Our System

Our city logging system collects various data including CCTV image, GPS data, temperature, humidity, luminous intensity, and so on from mobile observation equipment. Among several types of data, image data from CCTV is dealt with securely because it contains features which can violate people's privacy. So, we apply SIES to our system.

SIES has extended searchable document system using keyword to streaming media. SIES adopt a Content-based Image Retrieval (CBIR) technique [11] to extract image keyword from streaming images. CBIR is the application of computer vision techniques to an image retrieval problem, which is the problem of searching for digital images in large databases. "Content-based" means that search will analyze the actual contents of an image rather than the metadata such as keywords, tags, and descriptions associated with the image. The actual contents of an image refer to colors, shapes, textures and so on.

SIES consists of three phases: 1st index and extracted image keyword, 1st and 2nd key for encryption of streaming media, and Encryption and Decryption of Streaming Media.

4.1. 1st Index and Extracted Image Keyword

SIES extracts image keyword and 1st index in streaming media by CBIR technique as shown in Figure 4. Among sequential image frames, we extract an image which can be representative of that frames and consider it as image keyword. Poster cut in Figure 2 is the collection of image keywords. And we perform user's authentication to do access control to that poster cut.

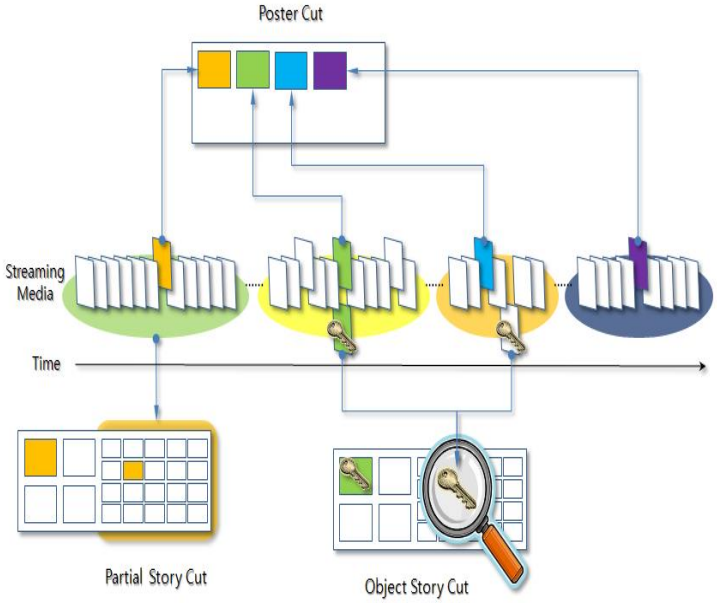

Figure 4. Process for Making 1st Index and Extracting Image Keyword

4.2. 1st & 2nd Key for Encryption of Streaming Media

In pre-subsection, we describe the process of 1st index and image keyword extracted one part of streaming media. Figure 5 shows the streaming media and extracted image keyword in one part of streaming media.

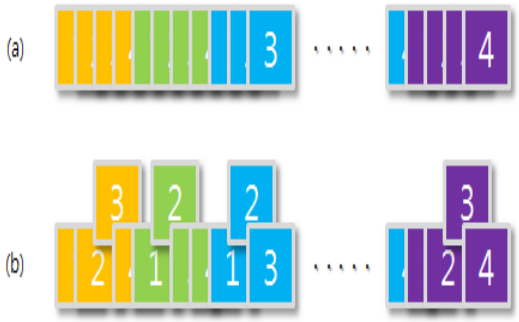

Figure 5. (a) Streaming Media, (b) Extracted Image Keyword in Streaming Media

Figure 5 and Figure 6 show the encryption and decryption process of streaming media by 1st key and 2nd key groups. And Figure 8 shows the poster cut area for image keyword extraction on streaming media by CBIR technique. CBIR is the application of computer vision techniques to the image retrieval problem, that is, the problem of searching for digital images in large databases. "Content-based" means that the search will analyze the actual contents (refer to colors, shapes, textures, or any other information) of the image rather than the metadata such as keywords, tags, and/or descriptions associated with the image.

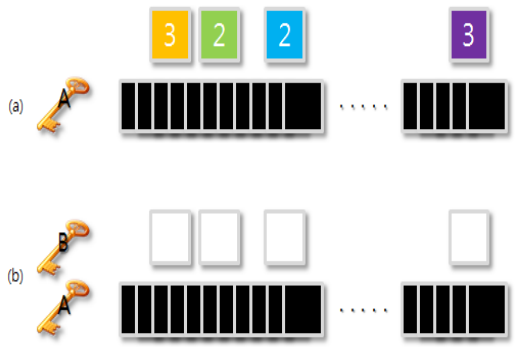

Figure 6. Encryption of Streaming Media and Image Keyword

4.3. Encryption and Decryption of Streaming Media

We showed the process for making 1st index and extracting image keyword from sequential image frames in previous subsection. Now, we are going to encrypt and decrypt CCTV images that can be searched by image keyword. For this, we utilize 1st keys and a 2nd key [3]. In the first, we describe the process for encrypting searchable images. We encrypt a group of sequential image frames by each 1st key. And then, we encrypt all the image keywords using a 2nd key. When we intend to search stored images, we should decrypt image keywords by a 2nd key. If we find an appropriate image keyword and acquire access permission to the corresponding sequential image frames, we will decrypt that image frames by obtaining the corresponding 1st key.

5. Application Scenario

After collecting data around the roads, a city logging system analyzes the collected data and provides city-info services using the analyzed data. For example, our system recognizes cars around a road by analyzing CCTV images and enumerates traffic volume on the road. Based on the enumerated value, the system provides a city-info service for observing traffic volume. We will display it on a web site using d3.js [12]. D3.js is a JavaScript library for manipulating documents based on data. Figure 5 shows the example for recognizing cars around a road. And Figure 6 shows the example of a web page for displaying traffic volume on roads using D3.

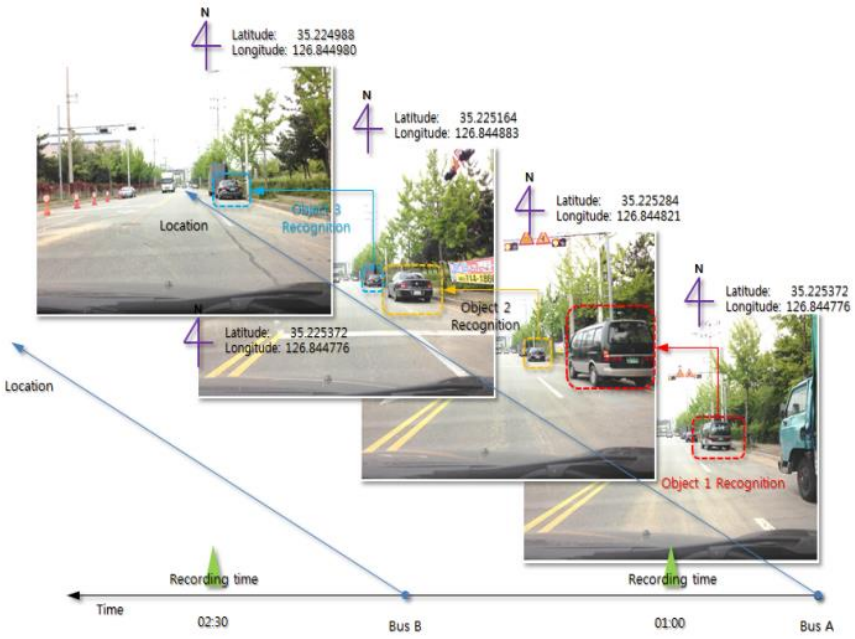

Figure 7. The Example for Recognizing Cars around a Road

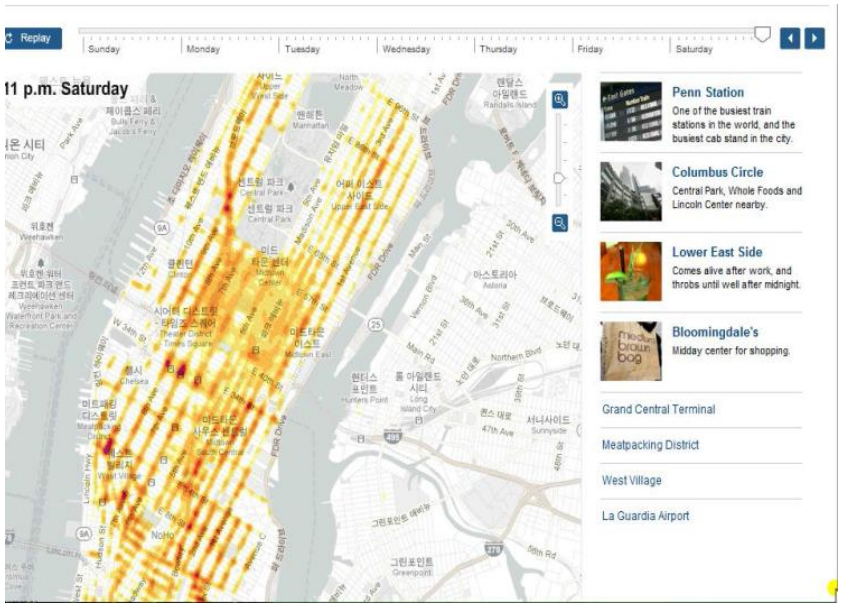

Figure 8. The Example of a Web Page for Displaying Traffic Volume

6. Conclusion and Future Work

In this paper, we proposed a city-logging system to collect various types of data around the roads using mobile observation equipment. Because the collected image data from CCTV contains the features which can violate the personal privacy, we proposed a secure method to search CCTV image using SIES. And then, we illustrated a city-info service which can be provided by analyzing the collected data. In the future, we will implement our proposed system and tests will be carried out.

Acknowledgements

This study was supported by research fund from Honam University, 2012.

References

[1] J. Gemmel, G. Bell and R. Lueder, "A Digital Life", Scientific American, **(2006)** March.
[2] G. Bell and J. Gemmel, "MyLifeBits: A Personal Database for Everything", Communications of the ACM, vol. 49, no. 1, **(2006)** January, pp. 88-95.
[3] J. G. Jeong, B. R. Cha and J. W. Kim, "Feasibility Study of Searchable Image Encryption System of Streaming Service based on Cloud Computing Environment", Proceedings of International Conference on Data Mining and Computer Engineering (ICDMEC'2012), Bangkok Thailand, **(2012)** December 21-22.
[4] N. S. Jho and D. W. Hong, "Technical Trend of the Searchable Encryption System", ETRI Journal, vol. 23, no. 4, **(2008**) August.
[5] P. Golle, J. Staddon and B. Waters, "Secure Conjunctive Keyword Search over Encrypted Data", Applied Cryptography and Network Security Conference, **(2004)**.
[6] B. Waters, D. Balfanz, G. Durfee and D. Smetters, "Building an Encrypted and Searchable Auditlog", NDSS, **(2004)**.
[7] R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data", Crypto, **(2005)**.
[8] J. Bethencourt, H. Chan, A. Perrig, E. Shi and D. Song, "Anonymous Multi-Attribute Encryption with Range Query Conditional Decryption", Technical Report, C.M.U., **(2006)**.
[9] R. Ostrovsky, "Software Protection and Simulations on Oblivious RAMs", ACM Symp. on Theory of Computing, **(1990)**.
[10] P. Golle and R. Ostrovsky, "Software Protection and Simulation on Oblivious RAMs", Journal of ACM, vol. 43, no. 3, **(1996)**, pp.431-473.
[11] http://en.wikipedia.org/wiki/Content-based_image_retrieval.
[12] D3.js – Data-Driven Documents, http://d3js.org.

Authors

NamHo Kim has been a professor in the Department of Internet Contents, Honam University, Korea, since 1998. He received the MS degree in Information & Communication from POSTECH, Korea. and received Ph.D. degrees from Chonnam National University, Gwang-ju, Korea, in 2013. His research interests include future internet, ubiquitous computing, big data processing, cloud computing, and biometrics information security.

Seong-Ho Lee received B.S., M.S., Ph.D. degrees from Chonnam National University, Gwang-ju, Korea, in 1995, 1999, and 2005, respectively, all in computer science. In 2011-2013, he was with the Information Industry Research Institute at the Mokpo National University, Mu-an, Korea, as a researcher. From July 2013, he has joined as a research head at Universal Community Co. Ltd., Gwang-ju, Korea. His research interests include big data processing, cloud computing, NFC technology, and security.

