A SURVEY ON PRESERVING THE DATA PRIVACY AND COPYRIGHTS DURING IMAGE RETRIEVAL IN CLOUD

Madhurya JA

PG Student, Dept of CSE, Acharya Institute of technology, Bangalore, Karnataka, India

---***---

Abstract- *Current generation uses the images and photos more than the text messages. Images consume more time and space than the text messages for both retrieval and storage respectively. Hence there is a need for efficient storage and retrieval of images. Cloud computing is the best choice for cloud storage outsourcing. So that the image owner can directly outsource the images to the cloud rather than maintaining local image database. In order to preserve the privacy of confidential images like personal and medical images, it has to be encrypted first before outsourcing it to the cloud. Next in order to access the encrypted images in cloud we use a technology called content based image retrieval. In this paper we use standard block cipher for image encryption and for copy-deterrence and privacy preserving purpose, watermark is embedded to the retrieved images.*

Key Words: Cloud Computing, privacy-preserving, copy-deterrence, image encryption, watermark embedding

1. INTRODUCTION

With the emergence of a number of practical vision systems, security of visual information is becoming important. For instance, in current generation people are giving more importance to images in their day-to-day communication and images are shared more than text messages. In recent years there is a rapid increase in image collections. It plays a crucial role in different fields like medicine, journalism, advertising, design, education and Social media etc., In order to make use of it, the images should be organized for efficient storage , searching and retrieval.

Smartphones and digital camera produce high quality images which require huge amount of storage space. If those images are stored in local database then the images can not be retrieved efficiently because local image database consists of millions of images. Sometimes, one digital image may have million dimensions and its size can be above 40 megabytes. Hence cloud computing is the best choice for cloud storage outsourcing , so that the person need not to maintain local image database.

When once the images has been stored efficiently in the cloud server, it has to be retrieved securely. So for this purpose we are using a emerging technology called content based image retrieval. For example, clinicians may use CBIR to retrieve the similar case of the patients which helps to take right decisions. As another example, law enforcement agencies usually compare the evidence from the crime scene with the records in their archives.

In order to preserve the privacy of images, firstly image owner encrypts the image and outsource the encrypted image along with its database to the cloud server and also enable the search over encrypted images. An authorized data user can query the cloud without interacting with the data owner and can obtain the requested images. Despite the tremendous benefits, privacy is the biggest concern. For example, patients does not want to disclose their medical images to any others except to a specific doctor. In order to protect the privacy of images and to avoid illegal distribution, following are the measures that are summarized as:

- To provide privacy to images, firstly image owner encrypts the images by using standard block cipher and then outsource the images to the cloud server[1].
- To avoid illegal distribution watermark based protocol is designed. Specifically, after the search operation, a unique watermark based on authorized user will be embedded to the retrieved images and then encrypted and watermark based images will be sent to requested user[1].
- Watermarking technique is different when compared to common watermarking. Here the proposed protocol directly embeds the watermark to encrypted images via cloud server. And the decryption should not affect the watermark present in the image.

2. LITERATURE SURVEY

1. “Private Content Based Image Retrieval [02]”, this deals with the retrieval of similar images without revealing the content of the query request to the database. They achieved it by exchanging the messages between the user and the database. They developed a method in which the database does not get to known anything about the query but the user gets the result for their query. Here query was in encrypted form but database was unencrypted.

2.“Enabling Search over Encrypted Multimedia Databases [03]”, this paper focuses on retrieval of similar images over encrypted databases, where both the query and database documents are encrypted and their privacy is protected. To achieve this, they proposed some techniques which enable efficient retrieval of images in the encrypted domain, without multiple rounds of communications between user and server. They demonstrated the proposed techniques using images.

3."Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing [04]" this paper focused on providing a privacy to the images which were uploaded to the cloud server. For this purpose , they proposed a privacy-preserving and retrieval scheme, which allows the data owner to outsource the images and its database to the cloud in an encrypted form, without revealing the actual content of the database to the cloud server.

4."A Provably Secure Anonymous Buyer–Seller Watermarking Protocol [05]" , focused on providing a copyright protection to digital content. For this they proposed buyer-seller watermarking protocol. Here the buyer chooses a secret key and sends that key to the seller. Then buyer and seller execute a protocol at the end of which the buyer obtains a watermarked content with the buyer's secret, while the seller does not get any information about that secret key.

5."Reversible data hiding in encrypted image[06]" , focused on reversible data hiding scheme. Here they use to create a copy of target image from original image and then use to embed a notation to target image, and sends this target image to the user.

6. "Protocols for Watermark Verification [07]" focused on adding a watermark to the digital image that can later be extracted or detected in the image. There are two types of watermark : visible and invisible. Visible watermarks means a particular content contains visible messages or company logos indicating the ownership of the image. Invisible watermarks, on the other hand are unobtrusive modifications to the image and the invisible watermarked image visually appears similar to the original image.

3. PROPOSED SCHEME

This paper explains the strategy involved to store and retrieve images. Here along with the image encryption, watermark is also used in order to increase robustness and to avoid illegal distribution of images.

A. SYSTEM MODEL

The entities mainly involved here are,

1. Image Owner
2. Image user
3. Cloud server
4. Watermark authority

1. Image Owner – Image owner encrypts the images by using AES encryption and then outsource the encrypted images along with its index to the cloud server.
2. Image User – are authorized user who can retrieve images from cloud server.
3. Cloud Server – cloud server is used to store all the encrypted images which are outsourced from the image owner.
4. Watermark authority – it generates unique watermark for each authorized user based on ID and embeds it via cloud server.

B. Working procedure of proposed scheme

As flowchart shown below Fig .1, Image owner needs to register and then login to the cloud server. Next to upload the images, image owner will encrypt it by using AES encryption and then outsource the images to the cloud by providing a tag name to the image. Image owner sends the user authentication information to the cloud server to check the identity of user during image retrieval. Additionally, the image owner sends the authorized user's authentication information to watermark authority to generate unique watermark based on user id. Here single owner is considered.

In order to obtain particular images from the cloud, firstly image user need to send a request to the cloud server by specifying a name of image that are needed for user. Cloud server based on request searches for the particular images. After obtaining the search results, watermark authority provides a unique watermark which is generated based on user id. So the cloud server will embed the watermark to the retrieved images and sends this watermarked image to the requested user.

Image user after obtaining requested images from cloud, will decrypt it by using decryption keys to obtain original images. Even after the decryption, the watermark present in the image will not be affected.

Illegal distribution of retrieved images can be easily identified based on unique watermark, which is generated based on user id. Hence the watermark technique will avoid the illegal distribution.

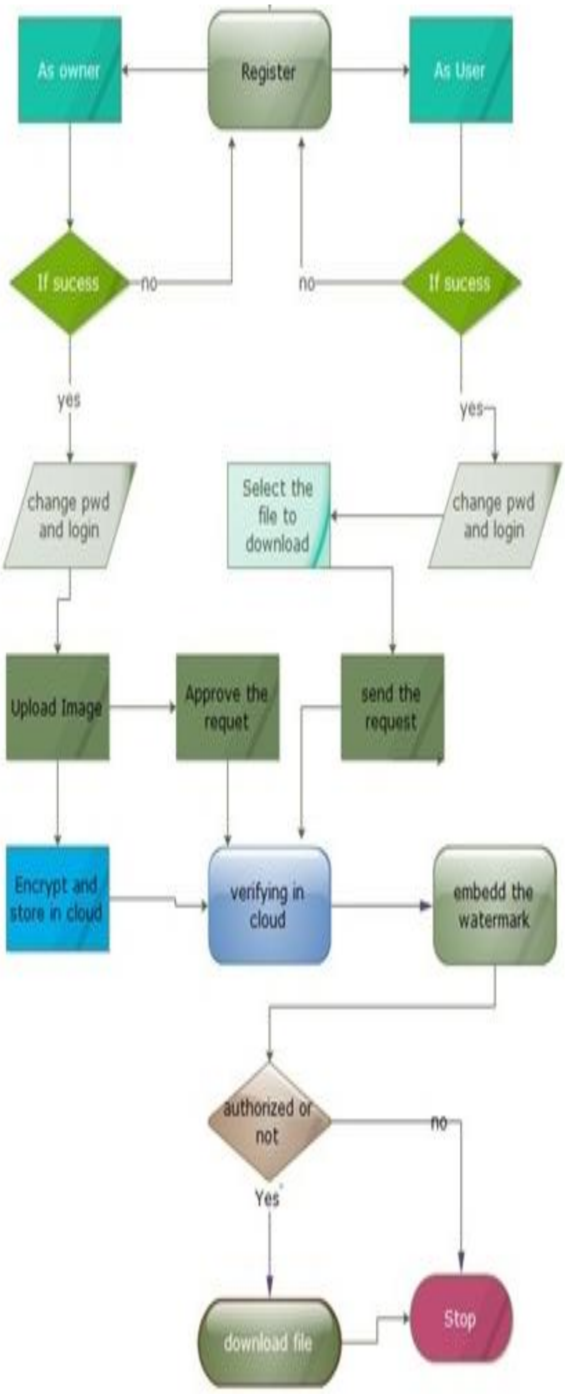

Fig.1 Flowchart of proposed system

4. CONCLUSION

In this paper, we proposed a privacy preserving and copy-deterrence content based image retrieval scheme in cloud computing. AES encryption is used for image encryption, thus providing a privacy to a image. For copy-deterrence purpose a watermark technique is used which generates unique watermark based on user id. Thus helps to avoid illegal distribution and can easily identify the illegal distributor or dishonest user. Comparatively it is more better than Zhang's algorithm[6] because it embed notations to the target image, where target image is the copy of original image, which is not specific as watermark which is used here.

As future work, there are some aspects could be improved like to consider multiple owner in this scheme.

REFERENCES

[1] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun and Kui Ren, "A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing", IEEE TRANSCATION ON INFORMATION FORENSIC AND SECURITY, VOL. , NO. , SEPTEMBER 2016.

[2] J . Shashank, P. Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in Proc. of IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2008, pp. 1–8.

[3] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in Proc. of IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2009, pp.725 418–725 418.

[4] Z . Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2015.

[5] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," Information Forensics and Security, IEEE Transactions on , vol. 5, no. 4, pp. 920–931, 2010.

[6] X . Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters , vol. 18, no. 4, pp. 255–258, 2011.

[7] K . Gopalakrishnan, N. Memon, and P. L. Vora, "Protocols for watermark verification," IEEE MultiMedia , no. 4, pp. 66–70, 2001.