International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

A survey on Privacy Preserving The Data Privacy And Copyrights During Image Retrieval in Cloud

Dr. Sarabu V Balamuralidhar & Bhavani Govardhan

Abstract- *Current generation uses the images and photosmore 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 out sourcing, 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

 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.

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].

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. Related Work

Piva, A., and De Rosa, A., (2010),Watermarking in Client-Side implanting frameworks have proposed as conceivable answer for copyright insurance in substantial content of the scale dispersion conditions. The proposed approach licenses to effectively consolidate the security of customer side install ding with the strength of educated implanting techniques. Since this approach licenses to effectively consolidate the safe implanting of fingerprints at the customer agree with the predominant heartiness of educated installing systems, giving another intense apparatus to the protected dispersion of brilliant interactive media sub-stance. Be that as it may, the security isn't upgraded and when the server appropriates encoded image it cannot be ideally com-squeezed. Open issues in the proposed structure to be tended to later on inquire about concern the requirement for higher security and the pressure overhead. Rial, A.,andPreneel, B., (2010),proposed security definitions for visually impaired and intelligible watermarking plans and for unknown BSW conventions. Recent BSW conventions are not furnished with the formal investigation of their security of properties. In this paper, they just focus on security properties. They didn't stretch out to different properties. So the future work should be directed to adjust or stretch out definitions to conventions that offers extra properties. For instance, attractive property for on-line business conventions is exchange decency and hence characterizing and outlining protection safeguarding reasonable BSW conventions is an intriguing objective. Chen, B. and

Wornell, G.W., (2001)they presented new classes of installing strategies, named quantization list regulation (QIM) and mutilation repaid QIM (DCQIM), and create helpful acknowledge as what we allude to as dither adjustment.QIM strategies are most likely superior to added substance spread range and summed up LBM against limited annoyance and free assaults and are close ideal for Gaussian channels, for which DC-QIM is optimal. Future work is required around there to empower the utilization of QIM systems in watermarking applications, and in reality, these speak to some particularly intriguing outline challenges. Cheng, B and Zhuo, L.,(2014),proposed the reversed file is produced utilizing visual expressions of pictures and after that scrambled dually by randomized twofold encoding and a key-based Gaussian arbitrary grid separately, creating a protected file. The proposed strategy can give secure, successful and precise recovery execution for clients without decoding, and accomplish practically identical recovery execution to the traditional huge scale picture recovery without uncovering data about picture substance and clients' protection. Manjunath, B.S and Ohm, J.R.,(2001)the shading and surface descriptors that are depicted in this paper have experienced broad assessment and improvement. Every one of these descriptors has been thoroughly tried and assessed following the MPEG-7 Core Experiment techniques to guarantee their viability and effectiveness in a wide assortment of uses in view of a sight and sound substance portrayal. For engineered pictures or for extremely particular spaces, for example, bio-therapeutic symbolism, refinements of existing descriptors or potentially extra descriptors might be required. Wang, C., and Lou, W., (2012) proposed a scheme used for encryption is ranked searchable encryption scheme. This scheme over-comes the disadvantages in another scheme that cloud server needs to directly navigate the entire file of the considerable number of reports for each inquiry ask for, while this is effective as SSE plans which is existing one with just consistent hunt money on the server. The disadvantage of this is the current implementation of secure ranked keyword search is not fully optimized. The Future work is an extension of experimental results will make this work more efficient. Hsu, C.Y., and Pei, S.C., (2012) proposed a approach utilized is this, protection safeguarding highlight ex-traction and representation address the issue of extricating and speaking to media includes in the encoded area while permitting display of intrinsic properties in the plain-text/unscrambled space. The weakness of this plan accomplishes better outcomes however the computational many-sided quality should be expanded. In Future work, they demonstrate that the proposed Paillier cryptosystem-based Privacy Preserving scale-invariant element change Privacy Preserving scaleinvariant feature transform (PPSIFT) plot accomplishes provable security in light of Data Loss Prevention Data Loss Prevention (DLP) and Rivest Shamir AdlemanRivest Shamir Adleman(RSA), however the computational intricacy should be additionally diminished. Lu, C.S. and Liao, H.Y., (2001)proposed two integral watermarks are inserted utilizing mixed drink watermarking and they can be indiscriminately removed without access to the host picture. The execution of their

multipurpose watermarking plan is to be sure eminent as far as vigor and delicacy. Future work will consider joining delicate watermarking and fingerprinting together. Overall, the previously mentioned instrument is as yet an open issue and requires to be additionally investigated. Lu, C.S. and Huang, S.K., (2000) novel picture security conspire called "mixed drink watermarking" is proposed in this paper. Mixed drink watermarking plan is strikingly powerful in opposing different assaults, including consolidated ones. The need of different bits as a payload containing data about the proprietor or dealer of a given picture in a copyright assurance framework is likewise required. Lu, C.S. and Liao, H.Y., (2003) proposed A new structural digital signature (SDS) scheme has been proposed for image authentication. Their plan is extremely hearty to content-saving controls and delicate to content-evolving bends. Their future work will consider geometric bends, for example, revolution and interpretation, which can't go on without serious consequences in this paper on the grounds that the basic computerized signature worked in the wavelet space is the variation to pivot and interpretation.

4.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 canretrieve

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.

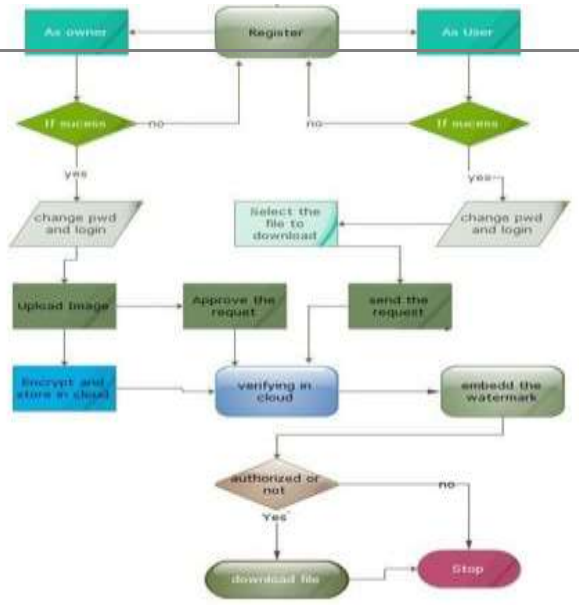

Fig.1 Flowchart of proposed system

5. 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 avoidillegal 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 ImageRetrieval Scheme in Cloud Computing", IEEETRANSCATION 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.

AUTHORS PROFILE:

Dr.Sarabu V Balamuralidhar has received his **Ph.D. degree** in Computer Science from University of Allahabad, Allahabad, India, **Master of Technology** degree in Database Systems from SRM University, Tamil Nadu, India and **Bachelor of Technology** degree in Information Technology from Jawaharlal Nehru Technological University, Ananthapur, India. He received **Gold Medal** from President of India, Dr. Pranab Mukherjee for emerging topper at SRM University, Tamil Nadu, India in 2012. He is currently as Software Developer in Mahantech Corporation, Charleston, USA. His research interests include optimization, security and privacy in Cloud Computing.

Bhavani Govardhan has received his B.Tech in Information Technology from Narayana Engineering College- Nellore, affiliated to JNTU-Ananthapur University in 2009, and M.Tech degree in Computer Science & Engineering from Bharath University in 2011. He is dedicated to teaching field from last 7.5 Years. He has guided 44 U.G students and 3 P.G students. At present he is working as Assistant professor in Rise Krishna Sai Gandhi Group of Institutions in JNTU, Kakinada in AP, India.