International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-11, Feb 2019

# A Survey on Image Privacy Protection using Encryption Steganography and CBIR

[*]Swapnali R. Pawar, [#]Prof. Dr. D.M.Thakore,

[*]Student, [#]HOD, Department of Computer Engineering, Bharati Vidyapeeth (Deemed To Be University) College of Engineering, Pune, Maharashtra, India.

[*]swapnalipawar2157@gmail.com, [#]dmthakore@bvucoep.edu.in

**Abstract - In this paper study on Image Privacy protection is carried out and we tried to find solution for identified problem. Large number of images are stored, shared and searched on internet using cloud storage. Most of images contain some sensitive information about users or any place or any event.So, privacy protection of user images becomes necessary. The present cloud service providers give little support to image security and privacy protection. Keeping record of images and performing operations without learning contents or indices of image is challenging for cloud.In our proposed solution TRIC - for image privacy protection which will store ,share and search images securely. Image privacy will be preserved using private CBIR(Content Based Image Retrieval),Homomorphic encryption and unique DImId (Digital Image Id) per user which is hidden in image using steganography.The system will protect the image privacy on cloud from cloud service provider and helps in finding origin of image and also prevents unauthorized access using access policy and Encrypted results of image search.Reverse steganography will be used for finding owner of image.**

***Keywords — Image privacy protection, Feature Extraction, Content-based image retrieval, Homomorphic Image Encryption, SITI, DImId, Steganography , Cloud.***

## I. INTRODUCTION

With advancement in digital technology powerful electronic devices like mobiles, digital cameras with high resolution capacity and quality are developed. Using such devices the craze of capturing photos and selfi is increased which results in rapidly increasing images and photos. Storing of all images on personal device like mobile or laptop requires large memory. With rapid increase in images it is inefficient to store them on personal device due to limited storage and performance reasons. Thus need to use cloud storage as service. The personal images consist of user's private information that needed to be prevented from unauthorized access. So to store these images there is need of secure personal Image storage that protects user's privacy from unauthorized users.

The drawback of cloud computing is vendor lock in and security concern. The cloud administrator has full rights to access data on cloud .so the cloud can able to learn about user's contents, user interest and can gain knowledge about user using user search queries and data storage on cloud. Also sharing of images as it is on cloud is not secure .So there is need to store share and search images privately with privacy protection on cloud. Image consist of sensitive information about user like users face , location details, event details that are needed to keep secure from unauthorized access to maintain user's privacy. On internet most of copyrighted images with watermark are displayed as it is but download option is not provided to prevent its misuse. But using watermark the image contents cannot protected as they are displayed so any one can copy its content and can misuse it. Also watermark can be removed using different techniques eg Zhang's algorithm can extract watermark. Most of services provided on internet are not trusted. Some hackers create phishing websites or spoofed site to hack users confidential information by gaining belief of user. Some mobile applications like antivirus applications and cloud based storage applications steals users' information without users knowledge. So, risk of un-trusted services is increased Content based image search retrieves the images based on its content. In content based image search, image features are extracted based on colour, edge and texture detection and using this image feature vectors image is searched. Content based image search gives good matching search results.

Once images are uploaded on internet they are at risk and not remain secure as internet is highly used for information sharing purpose. Number of service providers support image or video services based on cloud. Content based

 DOI : 10.18231/2454-9150.2019.0028 

image search allows to search images /videos based on their contents and used in many applications like criminal investigation and personal image or video management. Image search system extracts the distinctive feature descriptors of images to measure their content similarity. Image usually consists of hundreds of feature vectors .Large number of images uploaded on cloud will consist of billions of feature vectors. So, it's necessary to use indexing for search process. But most of efforts taken previously did not support image privacy protection.

The image can be reconstructed using feature vectors and is seem to be absolutely identical to original image and gives a good match with original image. So to protect personal images the private content based system is necessary. TRIC –will keep the user images secure from cloud service provider using homomorphic encryption. The images, user data and search results are prevented from cloud learning. Upload image on TRIC first, so it will be protected with unique DImId which act as user's copyright, then download it and use that downloaded image on internet to protect image and prevent its misuse.

## II. RELATED WORK

| Sr No | Paper Name | Year | Methodology Used | Result |
|---|---|---|---|---|
| 1 | Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices | 2015 | Distributed Computing Systems | Small storage overhead and communication overhead. |
| 2 | Real-time semantic search using approximate methodology for large-scale storage systems | 2016 | Parallel And Distributed Systems with data analytics, semantic correlation | Fast identification of correlated files |
| 3 | Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data. | 2016 | Image Processing | Performs better and practical |
| 4 | A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. | 2016 | Information Forensics And Security | Proposed watermarking based method is Not very robust |
| 5 | Privacy preserving multi-keyword ranked search over encrypted cloud data. | 2014 | Parallel And Distributed Systems | In communication and computation low overhead is introduced |
| 6 | Privacy Preserving Content-Based Image Retrieval in the Cloud. | 2015 | Reliable Distributed Systems | High performance and scalability. |
| 7 | Towards Privacy preserving Content-based Image Retrieval in Cloud Computing. | 2015 | Cloud Computing | Information leakage as cloud knows images related to each other are in same bucket. |
| 8 | Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories. | 2017 | Cloud Computing | High performance and scalability |
| 9 | Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT. | 2012 | Image Processing | Computational complexity, Provable security, Exists various method to attack their system |
| 10 | Enabling Privacy-preserving Image-centric Social Discovery. | 2014 | Distributed Computing Systems | High quality and compatible with human understanding. |
| 11 | Verifiable private multiparty computation: Ranging and ranking. | 2013 | Parallel And Distributed Systems | Efficient in communication and computation |
| 12 | Collusion-tolerable privacy preserving sum and product calculation without secure channel . | 2014 | Dependable And Secure Computing | linear Computation complexity for number of participants |

 DOI : 10.18231/2454-9150.2019.0028 

| | | | | |
|---|---|---|---|---|
| 13 | A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. | 2016 | Parallel And Distributed Systems | affected Search precision due to dummy keywords in EDMRS strategy |
| 14 | Enabling secure and efficient ranked keyword search over outsourced cloud data. | 2012 | Parallel And Distributed Systems | Efficient and effective |
| 15 | Efficient feature selection and classification for vehicle detection. | 2014 | Circuits And Systems For Video Technology | Speeded up feature selection process and superior in vehicle detection classification ability |

**Table 1-Study of Existing System**

[1] This System provides privacy protection for photo sharing and searching without leakage of query contents and result. Personalized private content can be defined using checkbox configuration. This system either automatically or manually determines rectangular ROP(Region of Privacy).Then ROP is separated into public and secrete part. To prevent sensitive information, secrete part is encrypted. Only legitimate users can access secrete part and retrieve ROP with key. For ROP separation the technique reviewed are Mask, P3,Blur [1].

[2] This system aims to minimize redundant data for enhancing query proficiency and minimizing operation cost. The main function is to fast identify similar images from massive image dataset in cloud [2].

[3] In this system, without exposing owner's data privacy the feature descriptors which are based on secrete data are acquired. First each image set is encrypted and then cipher text is distributed to two independent servers. Then server returns encrypted feature descriptors to owner of data who is able to retrieve actual feature descriptors [3].

[4] The proposed system supports CBIR over encrypted images without leaking the sensitive information to the cloud server. Firstly, for representing images their feature vectors are extracted. Then, by using locality-sensitive hashing the pre-filter tables are constructed to enhance search proficiency. The water marking technology used to prevent illegal distribution of images. Watermark is directly implanted into images that are encrypted. It also allows searching over encrypted images [4].

[5] In this work problem multi-keyword ranked search over encrypted data with privacy-protection in cloud computing (MRSE) is defined and solved. Performs multi keyword ranked search over encrypted data. Encrypted index that is searchable from data documents is used. For measuring similarity coordinate matching and inner product similarity is used [5].

[6] The proposed framework provides storage and retrieval of images in large image repositories with privacy protection. It is based on Image Encryption Scheme called IES-CBIR that displays properties dependent on Content-Based Image Retrieval. All data sent to cloud is encrypted for ensuring users privacy. Image texture is encrypted using probabilistic encryption for protection purpose. Colour information is encrypted using deterministic encryption. Colour information is used for image retrieval and content based image indexing. The solution enables encrypted storage as well as searching using CBIR queries with privacy protection [6].

[7] This proposed work, allow to deploy the CBIR service and image database to the cloud with privacy protection without displaying the real content of the database to the cloud server. Uses the local features for retrieving image based on its content. Uses EMD –Earth Movers Distance for calculating similarity of images. For improving search efficiency similar images are grouped together. The owner is responsible for producing searchable index before forwarding data to cloud. This scheme allows searching and CBIR on encrypted data. Authorised user uses encrypted query for searching image on cloud [7].

[8] This framework is designed to store search and retrieve images that are dynamically updated with privacy protection on cloud. The main aspect is to reduce overhead of client. Image colour information and texture information is separated that allows to use different encryption techniques. Global Colour features are encrypted using deterministic encryption and used for indexing and searching of images based on similarity. Encrypted images stored on cloud and Search query is encrypted [8].

[9] In this paper SIFT(Scale Invariant Feature Transform) and homomorphic encryption is used for preserving privacy of images Difference of Gaussian transform is executed for extracting the feature points. The images are twisted together with Gaussian Filters. Dissimilarity is calculated between two adjoining Gaussian blurred images. Using homomorphic encryption image is encrypted to maintain user's privacy. Focus on homomorphic comparison of encrypted data. Two encrypted data are compared based on their locations.

 DOI : 10.18231/2454-9150.2019.0028 

Pixels, locations are not encrypted and thus SIFT feature location is public and will not break privacy as feature vectors related to them are in encrypted form. Demanding issue of homomorphic comparison is resolved in this paper [9].

[10] This system is designed to perform social discovery based on images to increase the friends list of user depending on their common interest securely and efficiently using encryption. The social interest of user determined based on BOW(Bag Of Word) representation. Then compact and secure similarity index is designed which enables fast and scalable similarity based search on millions of encrypted images of user's profile vectors and is done by using BOW model by extracting visual content with similarity [10].

[11] In this work, the problem of verifiable privacy preserving multiparty computation is focused. They presented ranging protocol based on two party thresholds which is justifiable for both input and output and provides privacy protection. They also proposed testable ranking protocol for participant and aggregator model [11].

[12] In this paper, without using secure communication channel or trusted key issuers the privacy protected sum and product calculation protocols are accomplished. They proposed some protocols that give assurance of data privacy under semi honest cloud model. Then also proposed some advanced protocols which sustain up to k passive adversaries who do not interfere with computation [12].

[13] In this work, they designed searchable encryption that supports precise multi-keyword ranked search and flexible functioning on document. Top search efficiency can be achieved by implementing proposed Greedy Depth First Search algorithm. The proposed system is designed to support multi keyword query, ranking accurate results and also provides dynamic insertion and deletion operation on document collection [13].

[14] In this work, effectual usage of encrypted data which is remotely stored on cloud is accomplished by solving problem of giving support to efficient ranked keyword search. Also the accuracy of file retrieval is established [14].

[15] In this approach, the problem of feature selection and vehicle detection classification is focussed. They have designed enhanced normalization algorithm for chosen feature values to minimize in intra class difference and to increase inter class variability. The proposed solution for vehicle detection is based on features like Haar and RBF-SVM. To show its efficiency this approach is theoretically and experimentally analysed [15].

## III. Existing Approach

In most of the existing approach encryption techniques are used to prevent images against cloud administrator. For searching images with perfect match CBIR is used. For user authentication purpose secrete key sharing is also used. For providing copyright, watermarking technique is also used but it is neither robust nor is it fault tolerant. But after original images are outsourced on internet they will not remain secure from misuse.

## IV. Problem Identification

There are many techniques has been developed to prevent data from cloud learning which includes some encryption techniques, key sharing techniques, watermarking techniques. But once images are downloaded by authorized person then it is obvious that images will be spread on internet. Then any one can edit that images and is able to misuse or is able to spread some wrong information using that image . So, it's difficult to identify from where that particular image is spread and who misused that image. The purpose of this survey is to find solution for Sharing Storing and searching images with privacy protection on cloud.

## V. Proposed Approach

The main idea is to hide unique DImId (Digital image Id) and DoImId (Download Image Id) in image using stegnography .The DImId will identify owner of image while DoImId will identify who downloaded that image. Every time depending on downloader of image DoImId will be changed. One user will have unique DImId for all of his images which will act as hidden copyright.

The Aim of proposed approach is to prevent the image privacy of user from unauthorized access for that it uses access policy-Public, Private and Only me. System hides DImId in image using steganography to find originality of image source. History of users who downloaded image will be maintained for criminal investigation.

To implement TRIC - First all feature vectors should be extracted & DImId(Digital Image ID) should be included in image using steganography. Second, image feature vectors, image and image data should be encrypted using homomorphic image encryption. System store this encrypted Image data on cloud. Third, the images with private access policy when searched, the result is displayed in encrypted form and cannot downloaded without a secrete key. Finally user will be able to store search and share images on cloud with privacy protection. For implementing these following algorithms will provide support-

1. Shape-Based Invariant Texture Index (SITI)
2. Homomorphic Encryption (Encode and Decode Image)
3. Steganography(LSB-Least Significant Bit)

 DOI : 10.18231/2454-9150.2019.0028 

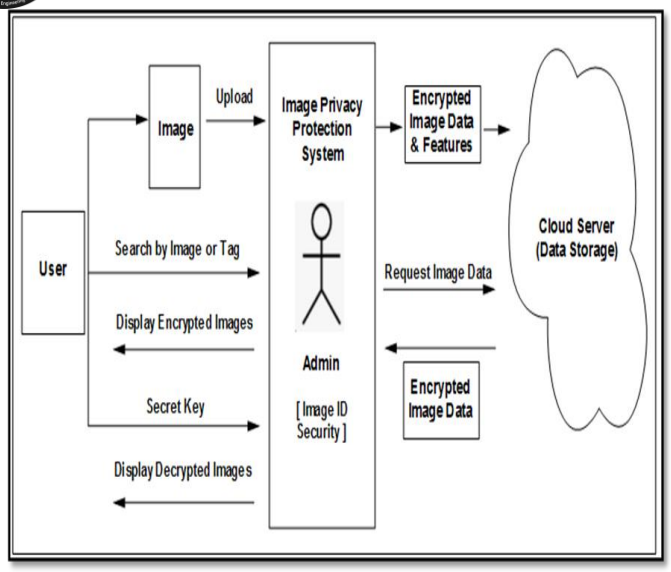


**Fig 1-Design of Proposed Approach**

## VI. CONCLUSION

The proposed system-TRIC will search store and share images securely with Image privacy protection on cloud.Images are searched using encrypted feature vectors so, query privacy will be preserved from cloud. Images are encrypted using homomorphic encryption and then stored on cloud so, image privacy will be prevented against cloud learning. Only authorized users will be able to share images using secrete key. It will also provide hidden copyright using unique DImId per user which is hidden in image using steganography.By using reverse steganography originality of image source can be identified.

## VII. FUTURE SCOPE

In this proposed approach we studied and analysed only image privacy protection, in future multimedia content privacy protection is needed. In Proposed approach we have used stegnography to provide hidden copyright to images which will identify image owner. In future stegnography can be used to provide hidden copyright for multimedia contents like image, video, audio etc.

## REFERENCES

[1] L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li, and Y. Liu, "Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices," in *ICDCS*. IEEE, 2015.

[2] Y. Hua, H. Jiang, and D. Feng, "Real-time semantic search using approximate methodology for large-scale storage systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1212–1225, 2016.

[3] [S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.

[4] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594–2608, Nov 2016.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, Jan 2014.

[6] Bernardo Ferreira, Jo˜ao Rodrigues, Jo˜ao Leit˜ao, Henrique Domingos, "Privacy Preserving Content-Based Image Retrieval in the Cloud". 2015 IEEE 34th Symposium on Reliable Distributed Systems

[7] Zhihua Xia, Yi Zhu, Xingming Sun, Zhan Qin, Kui Ren, "Towards Privacy preserving Content-based Image Retrieval in Cloud Computing". IEEE TRANSACTIONS ON COMPUTER COMPUTING, VOL. *, NO. *, SEPTEMBER 2015

[8] Bernardo Ferreira, Joao Rodrigues, Joao Leitao, Henrique Domingos, "Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories". IEEE Transactions on Cloud Computing, Year: 2017, Volume: PP, Issue: 99

[9] C.-Y. Hsu, C.-S. Lu and S.-c. Pei, "Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT," IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, 2012.

[10] X. Yuan, X.Wang, C.Wang, A. Squicciarini, and K. Ren, "Enabling Privacy-preserving Image-centric Social Discovery," in ICDCS'14. IEEE, 2014.

[11] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, "Verifiable private multiparty computation: Ranging and ranking," in *IEEE INFOCOM*, 2013.

[12] T. Jung, X.-Y. Li, and M. Wan, "Collusion-tolerable privacy preserving sum and product calculation without secure channel". In *IEEE TDSC*, 2014.

[13] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 2, pp. 340–352, Feb 2016.

[14] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, Aug.2012.

[15] X. Wen, L. Shao, W. Fang, and Y. Xue, "Efficient feature selection and classification for vehicle detection," IEEE Trans. Circuits Syst. Video Technol, DOI: 10.1109/TCSVT.2014.2358031.

 DOI : 10.18231/2454-9150.2019.0028 