Survey on Feature Extraction Techniques for Outsourced Encrypted Multimedia Content Data Analysis

Supriya Pentewad[1] , Prof. Dr. Siddhivinayak Kulkarni[2]
Department of Computer Engineering
[1, 2]MIT College of Engineering,Savitribai Phule Pune University,Pune, India.

Abstract-*In recent most of the data owners interested inoutsourcing their huge amount of personal multimedia data onto the cloud as it is the cost efficient and flexible solution. Such data is used by most of the service providers or any other applications for various purpose such as learning, searching or for behavioral advertising. In such cases sometimes this outsourced multimedia data may disclose the data owner's private information. So there is a need of the strong protocol of privacy preserving computation over outsourced multimedia data when feature extraction method apply on encrypted image data. In recent most of the techniques has been developed that support the efficient and secure feature extraction over outsourced multimedia data. These surveys also make the comparative analysis of such techniques, which represents the advantages and limitations. Also after analysis of the techniques authors gives a general framework of the system which will be better than the proposed system.*

Keywords-Privacy preserving outsourcing,Homomorphic image encryption, Feature descriptors, Content based search, Cloud computing.

I. INTRODUCTION

With the increasing popularity of cloud-based data services, data owners are highly motivated to store their huge amount of (potentially sensitive) personal multimedia data files and computationally expensive tasks onto remote cloud servers [16]. While enjoying the abundant storage and computation resources for cost saving and adaptability, the outsourcing of data storage and computation to the cloud additionally raises great security and privacy concerns because of the diverse trust domains the data owner and the cloud belong to [17].

As Cloud Computing gets to be predominant, more and more sensitive data are being centralized into the cloud, for example, emails, personal health records, private videos and photographs, company finance data, government documents, and so on. By putting away their information into the cloud, The data owners can be relieved from the burden of data storage and maintenance so as to enjoy the on-demand high quality data storage service. In any case, the way that data owners and cloud server are not in the same trusted domain may put the outsourced data at risk, as the cloud server may no longer be completely confided in such a cloud situation because of various reasons: the cloud server may leak data information to unauthorized entities or be hacked. It follows that sensitive data usually should be encrypted prior to outsourcing for data privacy and combating unsolicited accesses [21].

However, data encryption makes powerful information use an exceptionally difficult task given that there could be a lot of outsourced data files. Additionally, in Cloud Computing, data owners may share their outsourced information to an extensive number of clients [22, 23]. The individual clients may need to only retrieve certain particular data files they are occupied with amid a given session. One of the most popular ways is to specifically data files through keyword-based search instead of retrieving all the encrypted files back which is totally impractical in cloud computing scenarios. Such keyword-based search strategy permits clients to specifically retrieve files of interest and has been generally applied in plaintext search scenarios, for example, Google search. Tragically, data encryption confines client's capacity to perform keyword search and hence makes the traditional plaintext search techniques unsuitable for Cloud Computing. Other than this, data encryption additionally requests the assurance of protection of keyword privacy since keywords usually contain important information related to the data files. Despite the fact that encryption of keywords can protect keyword privacy, it further renders the traditional plaintext search systems useless in this scenario.

In the existing literature, efforts on privacy-preserving outsourcing calculation have been dedicated to different numerical issues including modular exponentiation, linear equations and kNN search. These works primarily focus on Engineering computation issues over numerical information or text data. Only in recent years, privacy-preserving data search in the cipher text domain has been extended to content-based multimedia retrieval, face recognition and fingerprint identification. The researcher

investigated how to enable secure image search in the data outsourcing environment. All things considered, they all accept that the images have been pre-processed by some feature extraction algorithms to get their vector representations [18, 19]. Because of the significance of image feature extraction in multimedia data processing and its substantial operations on massive information, particularly for satellite information for its enormous size and expansive number of feature points, the extraction or identification of image features from the ciphertext domain has began to attract more and more research interest.

Organization of the paper:

Paper start by presenting the related work in Section II.Our system is defined in Section III. Section IV gives some discussion of the proposed system. At last section V concludes the paper.

II. LITERATURE SURVEY

In paper [1] Hu S.et. Al. proposed an effective and practical privacy-preserving computation outsourcing protocol for the prevailing scale-invariant feature transform (SIFT) over massive encrypted image data. They first show that the previous solutions to this problem have both efficiency/security or expediency reasonableness issues, and none can well save the imperative qualities of the original SIFT in terms of distinctiveness and robustness. Then present a new scheme design that achieves efficiency and security requirements simultaneously with the preservation of its key characteristics, by randomly splitting the original image data, designing two novel effective conventions for secure duplication and examination, and deliberately conveying the feature extraction computations onto two independent cloud servers.

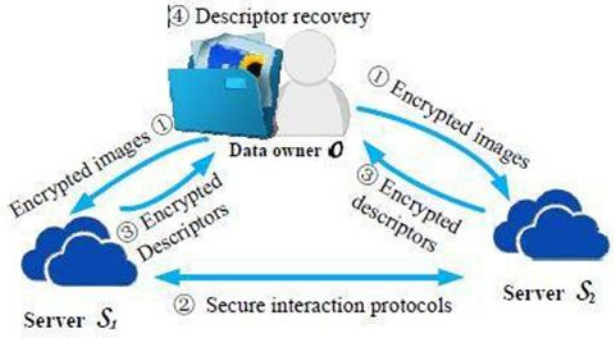


Fig.1 System Architecture [1]

In paper [2] Q. Wang et. al. presented a new and novel privacy preserving SIFT outsourcing protocol. Authors carefully analyze and extensively evaluate the security and effectiveness of our design. Also experimental results shows that our protocol outperforms the state-of-the-art and performs comparably to the original SIFT and is practical for real-world applications.

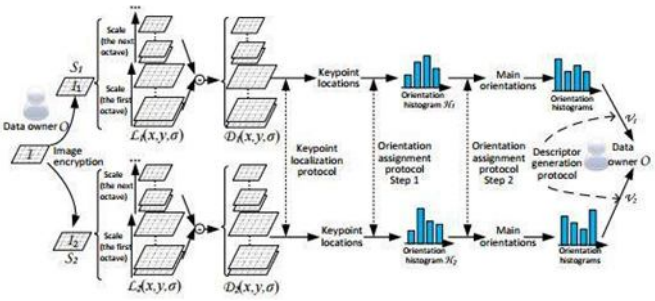


Fig.2 System Architecture [2]

In paper [3] the K. Ren et.al. outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

In paper [4] Z. Fu et al studied and solve the problem of personalized multi-keyword ranked search over encrypted data (PRSE) while preserving privacy in cloud computing. To tackle the restrictions of the model of “one size fit all” and keyword exact search, they propose two PRSE schemes for different search intentions.

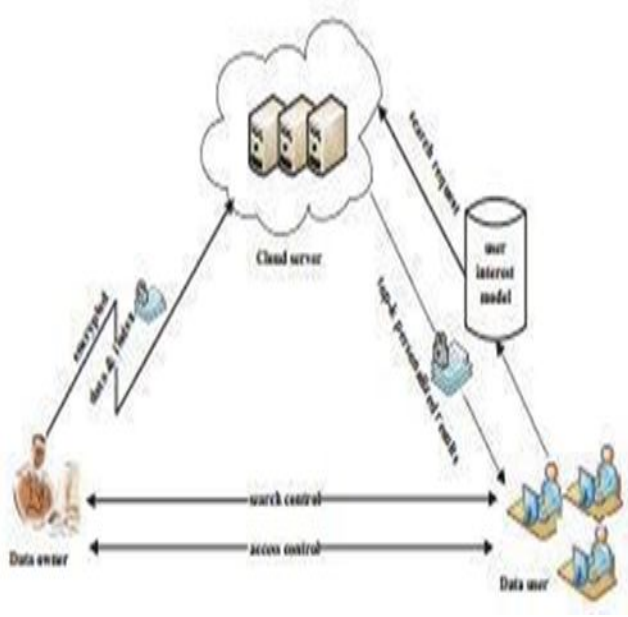


Fig.3 System Architecture [4]

In paper [5] Z. Xia et al constructed a special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The proposed plan can accomplish sub-direct search time and manage the deletion and insertion of documents flexibly

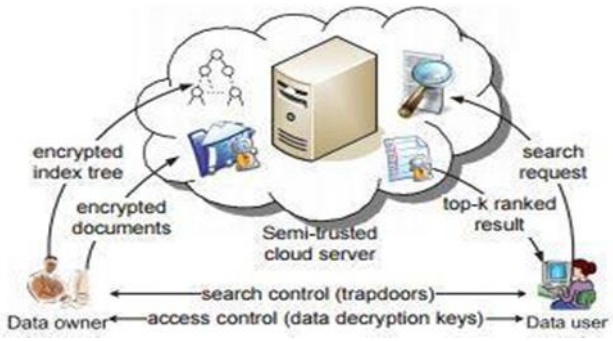


Fig.4 System Architecture [5]

In paper [6] S. Salinas et al develop an efficient and practical secure outsourcing algorithm for solving large-scale LSEs, which has both low computational complexity and low memory I/O complexity and can secure clients' privacy well. Author actualize their calculation on a real-world cloud server and a portable workstation. They find that the proposed algorithm offers significant time savings for the client (up to 65%) compared to previous algorithms.

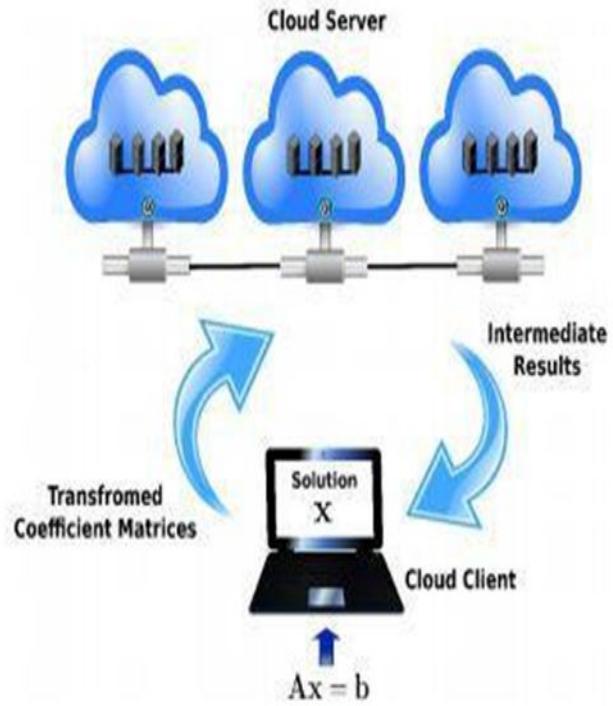


Fig.5 System Architecture [6]

In paper [7] L. Weng et al introduce the concept of tunable privacy, where the privacy protection level can be adjusted according to a policy. It is acknowledged through hash-based piecewise rearranged indexing. Two unique developments of robust hash calculations are utilized. The outcomes demonstrate that the security upgrade marginally enhances the recovery execution.

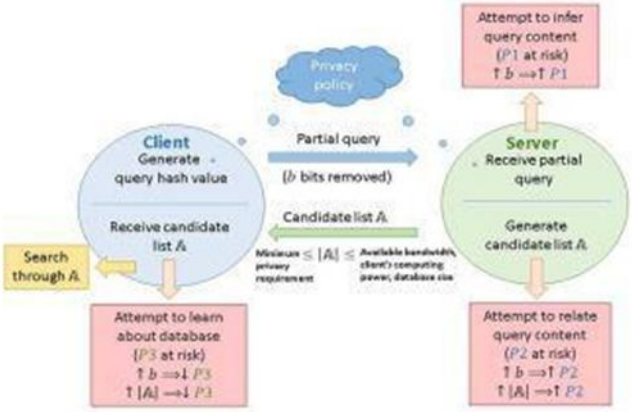


Fig.6 System Architecture [7]

In paper [8] C.-Y. Hsu et al propose a privacy-preserving realization of the SIFT method based on holomorphic encryption. They show through the security analysis based onthe discrete logarithm problem and RSA that PPSIFT is secure against cipher text only attack and known plaintext attack.

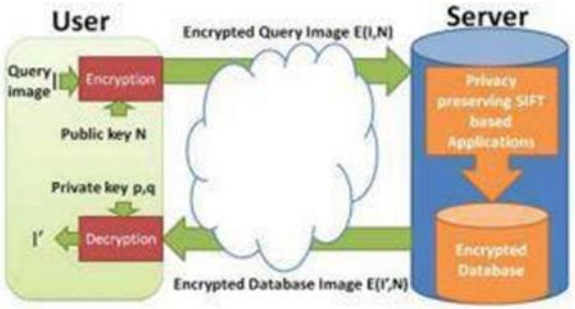
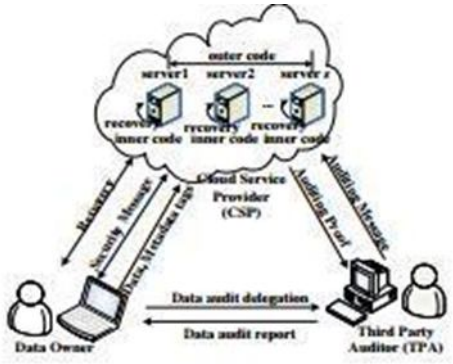


Fig.7 System Architecture [8]

In paper [9] Z. Brakerski and V. Vaikuntanathan present a somewhat holomorphic encryption scheme that is both very simple to illustrate and examine, and whose security (quantumly) reduces to the worst-case hardness of problems on ideal lattices. They then transform it into a fully holomorphic encryption scheme using standard “squashing” and “bootstrapping” techniques introduced by Gentry (STOC 2009).

In paper [10] Z. Ren et al given dynamic proof of retrievability scheme for coded cloud storage systems. Network coding and erasure codes are adopted to encode data blocks to achieve within-server and cross-server data redundancy, tolerating data corruptions and supporting communication-efficient data recovery. By utilizing rb23Tree and an improved version of ASBB scheme, our construction can support efficient data dynamics while defending against data replay attack and pollution attack. Security analysis and experimental evaluations demonstrated the practicality of our construction in coded cloud storage systems



In paper [11] Y. Elmehdwi et al proposed two SkNN protocols on encrypted data in the cloud. The first protocol, which acts as a basic solution, leaks some information to the cloud. Also authors says that developed second protocol is fully secure, which is, it protects the confidentiality of the data, user's input query, also hidesThe data access patterns. The second protocol is more expensive compared to the basic protocol.

In paper [12] M. Osadchy et al developed SCiFI, a system for Secure Computation of Face Identification. The system performs face identification which compares faces of subjects with a database of registered faces. The identification is done in a secure way which protects both the privacy of the subjects and the confidentiality of the database. A specific application of SCiFI is reducing the privacy impact of camera based surveillance.

Fig.9 Examples of variation in test images

In paper [13] L. Zhang et al introduced system POP that enables cloud servers to give privacy-preserving photo sharing and searching service to mobile device users who intend to outsource photo management while protecting their privacy in photos. Given system not only protects the outsourced photos so that no unauthorized users can access them, but also enables users to encode their image search so that the search can also be outsourced to an un-trusted cloud server obliviously without leakage on the query contents or results.

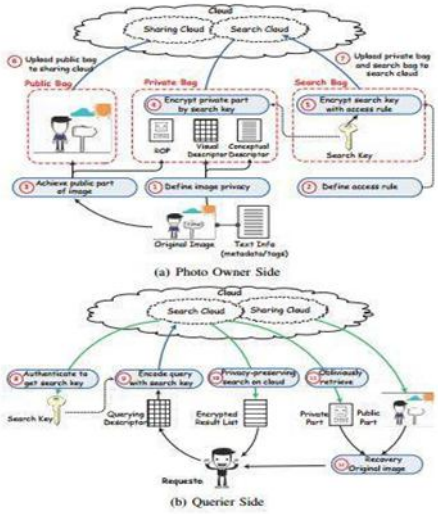


Fig. 10: POP System Overview

In paper [14] L. Zhang et al have given a system known PIC towards privacy preserving content-based search on large-scale outsourced images. With our careful design, the majority of the computationally intensive image matching jobs are outsourced to the cloud in a non-interactive way, but the image and query privacy is preserved.

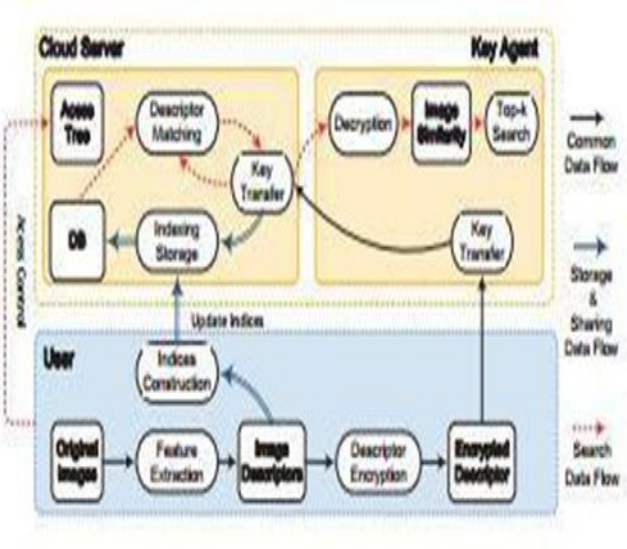


Fig.11 System Architecture [14]

In paper [15] C.-Y. Hsu et al given a homomorphic encryption-based privacy-preserving SIFT (PPSIFT) method to solve with the privacy-preserving issue present in a cloud computing environment, where the server can finish the tasks of SIFT based applications without learning anything to breach the user's privacy. In PPSIFT, the most challenging problem, i.e., homomorphic comparison has been solved in this paper. Authors also demonstrated that the implemented Paillier cryptosystem-based PPSIFT systems achieve provable security depending on DLP and RSA.

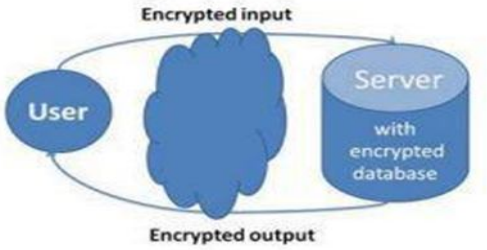


Fig.12 System Architecture [15]

III. PROPOSE SYSTEM

In recent most of the data owners interested in outsourcing their huge amount of personal multimedia data onto the cloud as it is the cost efficient and flexible solution. Such data is used by most of the service providers or any other applications for various purpose such as learning, searching or for behavioral advertising. In such cases sometimes this outsourced multimedia data may disclose the data owner's private information.

So in this paper authors will use the protocol of privacy preserving computation over outsourced multimedia data when Scale-Invariant Feature Transform(SIFT) feature extraction method apply on encrypted image data. In this paper, next they makes use of these extracted feature descriptors in content based searching by third party users with high level of security over encrypted image data. To test the performance of system, they use Breast Cancer Image dataset and analyze our proposed system.

Experimental results will prove that the proposed solution is very efficient and effective for image search over encrypted image data and achieves high level privacy preservation with SIFT feature descriptors.

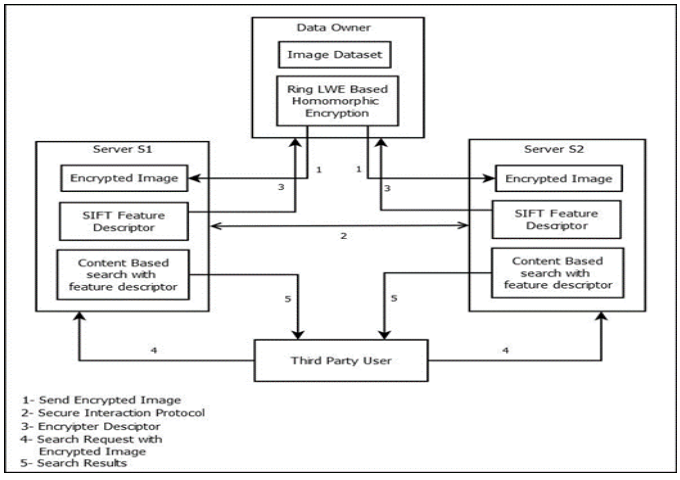


Fig.13: System Architecture for proposed system

IV. IMPLEMENTATION WORK

A. Browse Dataset

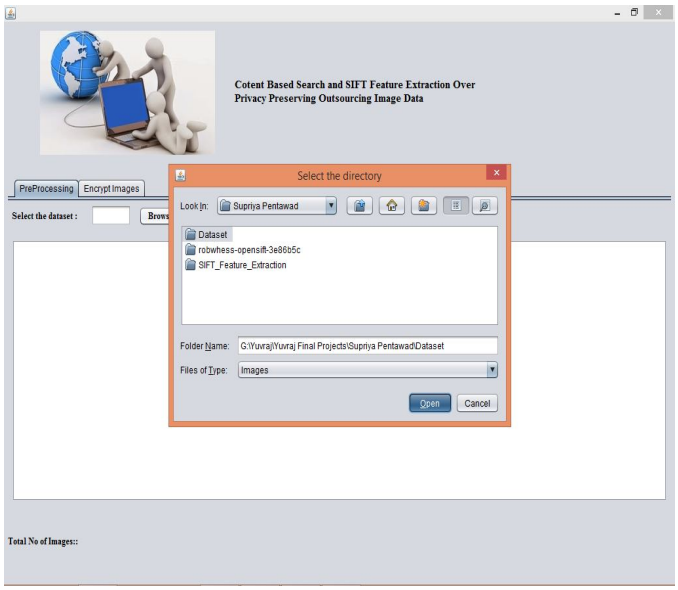


Fig.14: Browse Dataset

Fig. 14 shows the dataset browsing process where dataset is browse for preprocessing the data.

B. Display Image

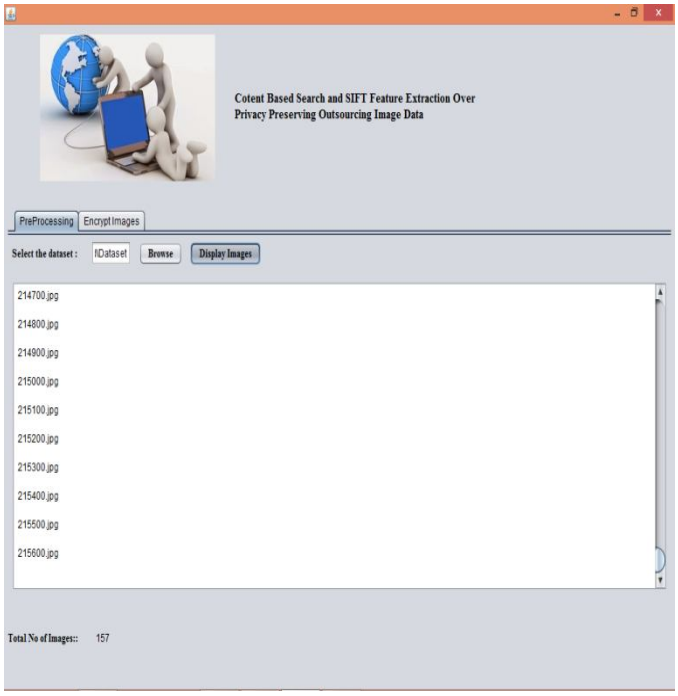


Fig.15: Display Images

Fig. 15 displays the browse jpg images.

C.Encrypt Images

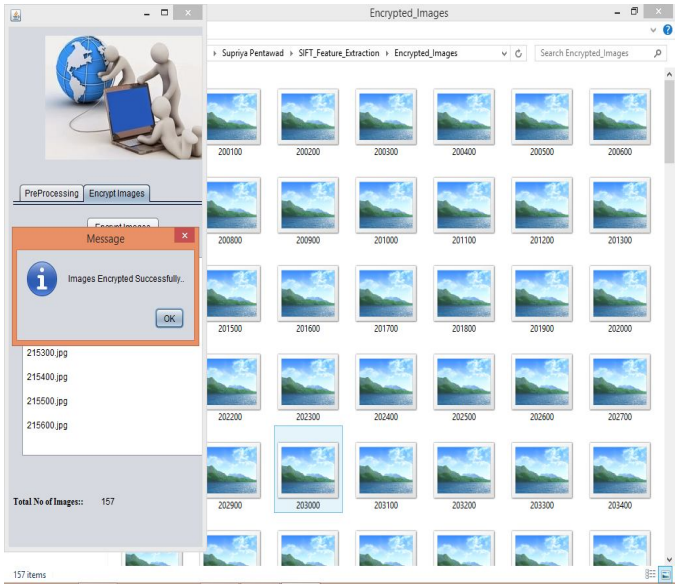


Fig.16: Encrypted Images

Fig. 16 displays the encrypted images. For encryption system used encryption algorithm. It is used to provide security to the images.

V. DISCUSSION

By studying various systems related to the topic in this paper list some disadvantage of the present system for Feature Extraction Techniques. To overcome this problem this paper introduces new technique which has several advantages and disadvantages which are listed below:

BENEFITS:

1. Privacy preserving outsourcing
2. Secure content based search
3. Time efficient search over encrypted image data
4. Secure and effective system design
5. Secure interaction protocol

LIMITATIONS:

1. Aggregator descriptor method is not utilized
2. Only working on image dataset

V. CONCLUSION

This paper presents a secure framework for the privacy-preserving outsourced storage, their search, and retrieval in those large-scale outsourced image repositories. Such repositories are dynamically updated. This survey shows some recent techniques has been developed for supporting theefficient and secure feature extraction over outsourced multimedia data. Also presents the limitations of all techniques that will be further useful for new improvements in same area.

REFERENCES

[1] Hu S, Wang Q, Wang J, Qin Z, Ren K. SecSIFT: Privacy-preserving Outsourcing Computation of Feature Extractions over Encrypted Image Data," in IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411-3425, July 2016.

[2] Q. Wang, S. Hu, K. Ren, J. Wang, Z. Wang, and M. Du,"Catch me in the dark: Effective privacy-preserving outsourcing of feature extractions over image data," in Proc. of INFOCOM'16, Accepted to appear, 2016.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no.1, pp. 69–73, 2012.

[4] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel and Distributed Systems, 2015, DOI: 10.1109/TPDS.2015.2506573

[5] 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 andDistributed Systems, vol. 27, no. 2, pp. 340–352, 2015.

[6] S. Salinas, C. Luo, X. Chen, and P. Li, "Efficient secure outsourcing of large-scale linear systems of equations," in Proc. of INFOCOM'15.IEEE, 2015, pp. 1035–1043.

[7] L. Weng, L. Amsaleg, A. Morton, and S. Marchand Maillet, "A privacy-preserving framework for large-scale content-based information retrieval," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 152–167, 2015.

[8] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving sift," IEEE Transactions on Image Processing, vol. 21, no. 11, pp. 4593–4607, 2012.

[9] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in Proc. Of CRYPTO'11.Springer, 2011, pp. 505–524

[10] Z. Ren, L. Wang, Q. Wang and M. Xu, "Dynamic proofs of retrievability for coded cloud storage systems", IEEE Trans. Services Computing, vol. PP, no. 99, pp. 1, Sep. 2015.

[11] Y. Elmehdwi, B. K. Samanthula and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments", Proc. IEEE ICDE, pp. 664-675.

[12] M. Osadchy, B. Pinkas, A. Jarrous and B. Moskovich, "SCiFI—A system for secure face identification", Proc. IEEE S&P, pp. 239-254.
[13] 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", Proc. IEEE ICDCS, pp. 308-317.
[14] L. Zhang, T. Jung, P. Feng, K. Liu, X.-Y. Li and Y. Liu, "PIC: Enable large-scale privacy preserving content-based image search on cloud", Proc. IEEE ICPP, pp. 949-958.
[15] C.-Y. Hsu, C.-S. Lu and S. Pei, "Image feature extractionin encrypted domain with privacy-reserving