A NOVEL APPROACH

FOR PRIVACY PRESERVING SYSTEM WITH CONTENT BASED IMAGE RETRIEVAL IN CLOUD COMPUTING

[1*]K ANJANEYULU, K RAM MOHAN GOUD[2]

[12]Assistant professor ,DEPT OF CSE , Sri Indu College of Engineering & Technology(autonomous), Sheriguda Ibrahimpatnam, Rangareddy, , Telangana ,INDIA

Abstract—

Keeping in mind the true objective to enhance the capacity need of visual information, investigate concentrate on outsourcing the information to the cloud. This paper gives an examination of the present techniques of the security safeguarding content based picture recuperation. Significant late creations are incorporated into this diagram covering distinctive parts of the examination around there, including, differing strategies, for example, and watermarking calculation, encryption calculation to enhance security while outsourcing information to the cloud. Content-based image retrieval (CBIR) applications have been rapidly created along with the increase in the quantity, availability, and importance of images in our daily life. Nonetheless, the wide sending of CBIR plot has been restricted by it's the serious computation and storage prerequisite. In this paper, we propose privacy-preserving content-based image retrieval conspire, which allows the data proprietor to redistribute the image database and CBIR administration to the cloud, without revealing the actual content of the database to the cloud server. Local features are used to speak to the images, and earth mover's distance EMD) is utilized to evaluate the similarity of images. The EMD computation is essentially a linear programming (LP) issue. The proposed plan transforms the EMD issue so that the cloud server can fathom it without learning the touchy information. In addition, local touchy hash (LSH) is used to enhance the search productivity. The security analysis and trials demonstrate the security and productivity of the proposed plan.

Index Terms—Cloud computing, searchable encryption, image retrieval, local feature, earth mover's distance, Feature extraction, Image encryption, Searchable encryption.

I. INTRODUCTION:

Cloud computing is the conveyance of figuring administrations over the Internet. Cloud administrations enable individuals and organizations to use programming and gear that are managed by outcasts at remote areas. Cases of cloud administrations incorporate online record stockpiling, long range informal communication locales, webmail, and online business applications. The cloud computing model enables access to data and PC assets from anyplace that a system association is accessible. Cloud computing gives a mutual pool of assets, including information storage room, systems, PC preparing power, and concentrated corporate and customer applications. The qualities of cloud computing incorporate on-ask for self-administration, expansive system get to, asset pooling, fast adaptability, and estimated advantage. On-ask for self-administration infer those customers (typically associations) can ask for and deal with their own particular processing assets. The expansive system gets to enables administrations to be offered over the Internet or private systems. In remote server farms, customers have the choice to draw the assets from a pool of processing assets. The quantity of administrations can be pretty much nothing or vast, and utilization of an administration is estimated and customers are charged as necessities be.

The administration models of cloud computing can be delegated: Software as a Service i.e. SaaS, Platform as a Service i.e. PaaS and Infrastructure as a Service i.e. IaaS. In Software as a Service demonstrates, a pre-made application, alongside any required programming, working framework, hardware, and system are given. In PaaS, a working framework, gear, and system are given, and the customer introduces or develops its own particular programming and applications. The IaaS display gives just the hardware and system; the customer

introduces or develops its own particular working frameworks, programming and applications. While there are benefits, there are insurance and security worries as well. Information is going over the Internet and is secured in remote areas. Also, cloud providers regularly serve distinctive customers at the same time. The greater part of this may raise the measure of presentation to conceivable breaks, both incidental and contemplate. Concerns have been raised by various that cloud computing may incite "capacity crawl" work of information by cloud providers that were not expected when the data was initially gathered and for which assent has regularly not been acquired. Given that it is so economical to keep information, there is a minimal motivating force to remove the data from the cloud and more motivations to find distinctive activities with it.

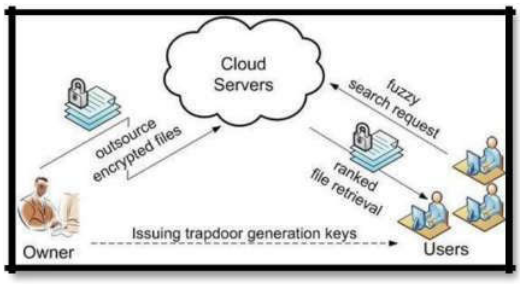

Figure 1: Framework of encrypted cloud data to retrieve the files based on similar search

The need to isolate information while managing providers that serve various customers, potential auxiliary jobs of the information—these are locales that associations ought to recollect while thinking about a cloud provider and while arranging contracts or inspecting terms of administration with a cloud provider. Given that the association exchanging this data to the provider is eventually in charge of its insurance, it needs to guarantee that the individual data is fitting taken care of.

An authorized data client can question the cloud for CBIR benefit without interacting with the data proprietor. Regardless of the colossal advantages, privacy turns into the greatest worry about CBIR outsourcing. For example, the patients won't want to uncover their medical images. In fact, the Health Insurance Portability and Accountability Act (HIPAA) set legal necessities to secure patients' privacy.

II. Related Work

Piva, An., and De Rosa, A., (2010), Watermarking in Client-Side implanting frameworks have proposed as the conceivable answer for copyright insurance in substantial content of the scale scattering conditions. The proposed approach licenses to successfully consolidate the security of client-side install ding with the quality of educated implanting procedures. Since this approach licenses to viably consolidate the safe implanting of fingerprints at the client agree with the predominant heartiness of educated installing systems, giving another intense apparatus to the ensured scattering of brilliant interactive media sub-stance. In any case, the security isn't upgraded and when the server appropriates encoded image it cannot be ideally compressed. Open issues in the proposed structure to be watched out for later on inquire about concern the necessity for higher security and the weight overhead.

Rial, A., and Preneel, B., (2010), proposed security definitions for visually impaired and intelligible watermarking plans and for obscure BSW traditions. Ongoing BSW traditions are not outfitted with the formal investigation of their security of properties. In this paper, they simply center on security properties. They didn't extend to various properties. So the future work ought to be coordinated to adjust or extend definitions to traditions that offer extra properties. For instance, attractive property for online business traditions is exchange fairness and consequently characterizing and outlining insurance safeguarding reasonable BSW traditions is an intriguing goal.

Chen, B. and Wornell, G.W., (2001)they displayed new classes of installing strategies, named quantization list regulation (QIM) and mutilation repaid
QIM (DC-QIM), and create accommodating acknowledge as what we allude to as dither adjustment.QIM strategies are in all likelihood better than added substance spread range and summed up LBM against

constrained annoyance and free assaults and are close ideal for Gaussian channels, for which DC-QIM is optimal. Future work is required around there to enable 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 turned around record is delivered utilizing visual articulations of pictures and after that scrambled dually by randomized twofold encoding and a key-based Gaussian arbitrary lattice separately, creating a secured document. The proposed strategy can give secure, fruitful and exact recuperation execution for customers without decoding, and accomplish practically identical recuperation execution to the traditional tremendous scale picture recuperation without uncovering data about picture substance and customers' insurance.

Manjunath, B.S and Ohm, J.R.,(2001)the shading and surface descriptors that are portrayed in this paper have encountered broad assessment and enhancement. All of these descriptors has been altogether attempted and assessed following the MPEG-7 Core Experiment methods to guarantee their viability and adequacy in a wide assortment of employment in perspective of sight and sound substance portrayal. For engineered pictures or for to a great degree particular spaces, for example, bio-therapeutic imagery, refinements of existing descriptors or potentially extra descriptors may be required.

Wang, C., and Lou, W., (2012) proposed a plan utilized for encryption is ranked searchable encryption conspire. This plan overcomes the disadvantages in another plan that cloud server needs to specifically navigate the whole document of the considerable number of reports for each inquiry ask for, while this is successful as SSE plans which is existing one with simply reliable chase cash on the server. The disadvantage of this is the ebb and flow implementation of secure ranked catchphrase search isn't completely enhanced. Future work is an expansion of experimental outcomes will make this work more effective.

Hsu, C.Y., and Pei, S.C., (2012) proposed an approach used is this, insurance safeguarding feature extraction 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-content/unscrambled space. The weakness of this plan accomplishes better results how-ever the computational many-sided quality ought to be expanded. In Future work, they demonstrate that the proposed Paillier cryptosystem-based Privacy Preserving scale-invariant component change Privacy Preserving scale-invariant feature transform (PPSIFT) plot accomplishes provable security in light of Data Loss Prevention Data Loss Prevention (DLP) and Rivest Shamir AdlemanRivest Shamir Adleman(RSA), anyway the computational intricacy ought to be additionally diminished.

Lu, C.S. and Liao, H.Y., (2001)proposed two integral watermarks are inserted utilizing blended drink watermarking and they can be indiscriminately expelled without access to the host picture. The execution of their multipurpose watermarking plan is to make sure eminent as far as energy and delicacy. Future work will consider joining delicate watermarking and fingerprinting together. Overall, the recently referenced instrument is as yet an open issue and requires to be additionally investigated.

Lu, C.S. and Huang, S.K., (2000) novel picture security plot called "blended drink watermarking" is proposed in this paper. Blended drink watermarking plan is strikingly incredible in opposing diverse assaults, including consolidated ones. The need of various bits as a payload containing data about the proprietor or dealer of a given picture in a copyright assurance framework is in like manner required.

Lu, C.S. and Liao, H.Y., (2003) proposed another structural digital signature (SDS) plot has been proposed for image authentication. Their plan is to a great degree hearty to content-saving controls and delicate to content-evolving twists. Their future work will think about geometric twists, for example, unrest and interpretation, which can't go ahead without genuine results in this paper in light of the fact that the basic modernized signature worked in the wavelet space is the variation to turn and interpretation.

Lin, C.Y. and Chang, S.F., (2001) have proposed an image validation technique that perceives the JPEG lossy standard weight from various malignant controls. Their proposed technique can be changed to suit various requirements and acknowledge "alluring" control.

Lin, C.Y. and Wu, M.,(2001)proposed a watermarking calculation that is energetic to RST twists. The results moreover display the shortcoming of this strategy to trimming, an assault against which no means have been taken in the plan. Future work will concentrate on more fruitful installing and RST solid watermarking intended to endure editing and weight.

Fuh, C.S. and Cho, S.W.,(2000)proposed joining a shading division with the creation of a dynamic relationship tree and the utilization of the comparing tree coordinating strategy is actualized. Their approach has great recuperation capability when the locale associations of

inquiry objects are marginally unpredictable. The disservice is that the recuperation strategy relies upon right tree coordinating.

Lai, C.C. and Chen, Y.C.(2011) a customer situated instrument for CBIR method in perspective of an intuitive hereditary calculation (IGA) are proposed. The aftereffects of the proposed approach have demonstrated the critical change in recuperation execution. Additionally, work considering even more low-level picture descriptors or abnormal state semantics in the proposed approach is in advance.

Mukherjee, D.and Chae, J.J.(2000) displayed a source and channel coding structure for information stowing away, permitting any tradeoff between the permeability of distortions introduced, the measure of information installed, and the dimension of capacity to clamor. The present work isn't enthusiastic to changes, for example, upset and segment. Changes or features of an image that are invariant to such changes should be examined to review this disadvantage.

Tiakas, E. and Rafailidis, D.(2013)a novel estimated ordering plan for profitable substance based picture interest and recuperation is introduced, called Multi-Sort Indexing (MSIDX). The proposed plot underpins the desired functionalities of present-day applications since it is prepared for performing exact substance based recuperation in low inquiry time and handles the dynamic operations of

inclusions and cancellations continuously.

Khelifi, F. and Jiang, J., (2010)another perceptual picture hashing strategy has been proposed. The proposed hashing technique has been appeared to pass on better execution as far as power at a lower computational cost when contrasted with related strategies.

Cannons, J. and Moulin, P. (2004)proposed a greatest probability watermark indicator in light of a factual picture demonstrate. The joint hashing/watermarking plan beats the customary "hash less" watermarking system. All things considered, further enhancements can be acquired by considering the plan of the watermark finder.

III. PROPOSED SYSTEM:

3.1 System architecture

As appeared in Fig. 2, the proposed plan involves three kinds of elements: a data proprietor, data clients and cloud server. The data proprietor holds a large-scale image database M={m1,...,mn} to be re-appropriated, where n is the image number of the database. The data proprietor generates a searchable index for the image database M. For privacy-preserving, the data proprietor needs to scramble the image database and the search index and then re-appropriates the encoded image database and index to the cloud. Since it is normal that the cloud can furnish the CBIR benefit without interacting with the data proprietor once the database is re-appropriated, we have to build a special searchable encryption plot that bolsters CBIR over encoded data. During the CBIR question phase, the authorized client presents a scrambled inquiry trapdoor to the cloud server. At that point, the cloud server compares the similarities between the inquiry image and the images in the database and returns the encoded similar images to the data client. Finally, the authorized client unscrambles the got images.

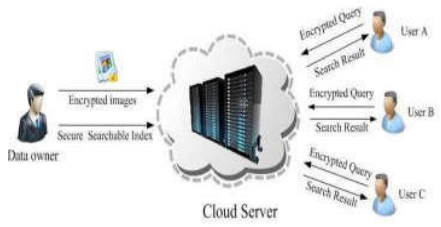

Fig. 2: Architecture of proposed scheme

3.2 SECURITY MODEL

In this paper, we consider the semi-legitimate (also known as fair yet inquisitive) cloud server, who will effectively pursue the designated convention specification, yet keep and analyze the communication history, trying to determine touchy information. The data proprietor and authorized clients are always trusted. The plan is intended to keep the cloud server from knowing the content of the image database and clients' inquiries. Similar to a searchable encryption conspire, we don't consider the information leakage because of access pattern. For instance, if images mi and mj are returned as the search consequences of the same inquiry, it is easy to reason that images mi and mj are similar to each other. In fact, this issue can be viably tackled by applying an existing ORAM plot, e.g. [26].

3.3Earth mover's distance

The earth mover's distance can be applied to evaluate the similarity between the dispersions [24], [25]. Given two circulations, the appropriation with a smaller total of weights can be seen as a mass of earth which properly spread in space, and the dispersion with a larger whole of weights can be seen as an array of gaps in the same space. The EMD measures the minimal expense of moving all the earth into the gaps. A unit of work will be tallied when a unit of the earth is transported for a unit of distance. The EMD trans-forms the matching issue to
the transportation issue. Two

appropriations have the least transportation cost can be seen as the most similar ones. Given two image Two distributions have the least transportation cost can be viewed as the most similar ones. Given two image signatures $st = \{(c1$

, $w1\ ), \ldots, (ci\ , wi\ ), \ldots, (ckt\ , wkt\ )\}$, for t

= 1, 2, the EMD is defined in terms of an optimal flow $F=\{fi;j\ \}$, which minimizes the work required to move earth from one signature to another, denoted as $W(s1, s2, F) = \sum k\ i=1\ 1\ \sum k\ j=1\ 2\ fi;jdi:j$, where $di;j = d(c(1)\ i\ , c(2)\ j\ )$ is the distance between $c(1)\ i$ and $c(2)\ j$, e.g. the Euclidean distance in Rd. Meanwhile, the flow $fi;j$ must satisfy the following constraints:

Meanwhile, the flow $fi;j$ must satisfy the following constraints:

- $f_{i,j} \geq 0, 1 \leq i \leq k_1, 1 \leq j \leq k_2;$
- $\sum_{i=1}^{k_1} f_{i,j} \leq w_j^{(2)}, 1 \leq j \leq k_2;$
- $\sum_{j=1}^{k_2} f_{i,j} \leq w_i^{(1)}, 1 \leq i \leq k_1;$
- $\sum_{i=1}^{k_1} \sum_{j=1}^{k_2} f_{i,j} = \min(\sum_{i=1}^{k_1} w_i^{(1)}, \sum_{j=1}^{k_2} w_j^{(2)})$.

Once the optimal flow $fi;j^*$ is found, the EMD between s_1 and s_2 is defined as

$$EMD(s_1, s_2) = \frac{\sum_{i=1}^{k_1} \sum_{j=1}^{k_2} f_{i,j}^* d_{i,j}}{\sum_{i=1}^{k_1} \sum_{j=1}^{k_2} f_{i,j}^*}, \qquad (2)$$

where the numerator is the minimal transportation cost and the denominator
is the total development. The signatures can always be changed over to legitimate probability conveyances by normalizing the weights to add up to 1 [32]. Consequently, we can streamline the constraints to:The EMD distance can be converted to an LP optimiza-tion problem as follows:

$$\begin{aligned} &minimize && \sum_{i=1}^{k_1}\sum_{j=1}^{k_2} f_{i,j}d_{i,j}, \\ &subject\ to && f_{i,j} \geq 0, 1 \leq i \leq k_1, 1 \leq j \leq k_2, \\ & && \sum_{i=1}^{k_1} f_{i,j} = w_j^{(2)}, 1 \leq j \leq k_2, \\ & && \sum_{j=1}^{k_2} f_{i,j} = w_i^{(1)}, 1 \leq i \leq k_1, \\ & && \sum_{i=1}^{k_1}\sum_{j=1}^{k_2} f_{i,j} = 1. \end{aligned} \tag{3}$$

we portray the plan of our privacy-preserving CBIR conspire. Initially, we introduce the framework of the proposed plan. Next, we introduce two advances which will be utilized in index development. Finally, we present the details of the entire plan.

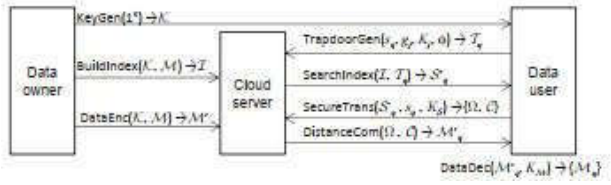

Fig. 3: Flow chart of the proposed scheme

3.4 The framework of the scheme

the proposed scheme consists of a tuples of probabilistic polynomial time algorithms Γ=*{*KeyGen,BuildIndex,DataEnc, TrapdoorGen, SearchIndex, SecureTrans, DistanceCom, DataDec*}*.The flow chart of the proposed scheme is illustrated in Fig. 2.

In the initiation phase, given an image database *M*, the data owner runs KeyGen (1*κ*), BuildIndex (*K, M*) and DataEnc (*K, M*) to generate *K*, *I* and *M′*. Then the data owner server and sends the *K* to the authorized data users. In the image retrieval phase, an

authenticated data user runs TrapdoorGen (*sq, go, Kj, ϕ*) to generate trapdoor *Tq*, and then submits *Tq* to the cloud server. The cloud server runs SearchIndex (*I, Tq*) to obtain a set of encrypted signature *S′ q*. This means that the corresponding set of images *Mq ⊆ M* is a subset of images that may be similar to the query image *mq*. The cloud server then sends *Sq′* to the data user. Upon receiving *Sq′,* the data user runs SecureTrans (*Sq′, sq, KS*) to construct the set of encrypted EMD problem **Ω**, and then sends **Ω** to cloud server. Upon receiving the set of encrypted EMD problem **Ω**, the cloud server runs DistanceCom (**Ω**) to find the most similar images to the query image, and then sends the set of encrypted image set *M′ q* to the data user. Finally, the data user runs DataDec(*M′ q, KM*) to get the set of similar images *Mq*.

3.5 Local sensitive hash on signature centroid

The calculation of EMD issue between the question image and the images in the database will cause a period multifaceted nature linear to the cardinality of the image set. It will be unusable in a real world application with countless. In this manner, we require a strategy to sift through the dissimilar images rapidly, and then just calculate the EMD issues with the remaining images. In this paper, the local delicate hash calculated with signature centroid is utilized to sift through the dissimilar images rapidly. **Centroid of the signature**. A lower bound of EMD between two signatures is the Euclidean distance between their centroid [24]. The centroid of the signature *st* is defined a EMD between the signature of st and sq can be defined as

$$\xi_t = \sum_{i=1}^{k_t} c_i^{(t)} w_i^{(t)}. \qquad (4)$$

$$EMD(s_t, s_q) = \sum_{i=1}^{k_t} \sum_{j=1}^{k_q} f_{i,j}^* d_{i,j}$$
$$\geq \| \sum_{i=1}^{k_t} c_i^{(t)} w_i^{(t)} - \sum_{j=1}^{k_q} c_j^{(q)} w_j^{(q)} \|_2 .$$

Algorithm 1. BuildIndex

Input: the centroid database Ξ, the set of hash functions $\{g_j\}_{j=1}^{L}$, the set of keys for hash value $\{K_j\}_{j=1}^{L}$, the one way hash function ϕ.
Output: secure index $\mathcal{I}$.
1. For each $j = 1, \cdots, L$, data owner builds the j-th hash table by applying function g_j over all the elements in centroid database Ξ. One example is shown in Tab. 1.
2. For each $j = 1, \cdots, L$, data owner picks a random key K_j and replaces each LSH hash digest $B_{j,i}, i = 1, \cdots, N_j$ in the j-th hash table with $\phi(K_j, B_{j,i})$.
3. For each $j = 1, \cdots, L$, data owner further fills the j-th hash tables with identifiers of corresponding images $ID(m_i)$.
Return: Index $\mathcal{I}$ consists of L secure hash tables.

Algorithm 2. Secure Transformation

Input: Original problem $\Psi = \{c, U, \tau, V, E\}$ and secure key $K_T = \{G, \Lambda, r, \gamma\}$
Output: Transformed problem $\Omega = \{c', U', \tau', V', E'\}$
1: Pick a non-singular $k_t k_q \times k_t k_q$ matrix Λ and $k_t k_q \times 1$ vector r to perform the transformation as Formula(6);
2: Pick an $(k_t + k_q) \times (k_t + k_q)$ generalized permutation matrix G and multiple it to the constraints as Formula (7);
Return: The transformed problem Ω as shown in Formula (8).

In this subsection, we argue that the encoded database, secure searchable index, and scrambled inquiry won't reveal extra information to the cloud. Most importantly, it is easy to see that the image database is very much ensured if the encryption plot is CPA-secure. The watchwords in hash tables are encoded by the restricted hash work. For each j = 1, ..., L, data proprietor picks a random key Kj and scrambles each watchword Bj;i, I = 1, ..., Nj in the j-th hash table as ϕ(kj, Bj;i).Since the catchphrases in the same hash table are novel and each hash table is encoded with an alternate key, the same catchphrases are never scrambled with the same key twice. Hence, the
encoded watchwords are indistinguishable from random. Similar to the safe searchable index, the encoded question is also very much ensured.

CONCLUSION

In this paper, we propose a privacy-preserving content-based image retrieval conspire, which allows the data proprietor to redistribute image database and the CBIR administration to the cloud without revealing the actual content of the database. Local features are used to speak to the images, and earth mover's distance (EMD) is utilized to evaluate the similarity of images. We transform the EMD issue so the cloud server can take care of the issue without learning delicate information. In request to enhance the search effectiveness, we plan a two-stage structure with LSH. In the primary stage, dissimilar images are sifted through by pre-channel tables to shrink the search scope. In the second stage, the remaining images are compared under EMD metric one by one for refined search results. The security analysis and tests demonstrate the security and effectiveness of the

proposed plan. Later on, we will think about how to re-appropriate the feature extraction to the cloud server in order to additionally alleviate the weight of data proprietor and data client.

REFERENCES

[1]C. Pavlopoulou, A. C. Kak, and C. E. Brodley, "Content-based image retrieval for medical imagery," in Medical Imaging 2003. International Society for Optics and Photonics, 2003, pp. 85–96.
[2]A. K. Jain, J.-E. Lee, R. Jin, and N. Gregg, "Content-based image retrieval: An application to tattoo images," in Image Processing (ICIP), 2009 16th IEEE International Conference on. IEEE, 2009,pp2745–2748.
[3]J. M. Lewin, R. E. Hendrick, C. J.
DOrsi, P. K. Isaacs, L. J. Moss, A. Karellas, G. A. Sisney, C. C. Kuni, and G. R. Cutter, "Comparison of full-field digital
mammography with screen-film mammography for cancer detection: Results of 4,945 paired exam-inations 1," Radiology, vol. 218, no. 3, pp. 873–880, 2001.
[4]D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[5]E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
[6]R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient con-structions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.
[7]M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156– 1167.
[8]C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451– 459.
[9]Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," Journal of Cloud Computing, vol. 3, no. 1, pp. 1–11, 2014.
[10]W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud sup-porting similarity-based ranking," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013, pp. 71–82.
[11]N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.
[12]Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. PP, no. 99,p.1, 2015.
[13]S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security. Springer, 2013, pp. 258–274.
[14]D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation," in Proc. of NDSS, vol. 14, 2014.
[15]J. Shashank, P. Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on. IEEE, 2008,pp.
[16]C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Secure and robust SIFT," in Proceedings of the 17th ACM international conference on Multimedia. ACM, 2009, pp. 637–640. [17]"Image feature extraction in encrypted domain with privacy-preserving SIFT," Image Processing, IEEE Transactions on, vol. 21, no. 11, pp. 4593–4607, 2012.
[18]P. Zheng and J. Huang, "An efficient image homomorphic encryp-tion scheme with small ciphertext expansion," in Proceedings of the 21st ACM international conference on Multimedia. ACM, 2013, pp. 803–812.
[19]Z. Qin, J. Yan, K. Ren, C. W. Chen, and C. Wang, "Towards efficient privacy-preserving image feature extraction in cloud computing," in Proceedings of the ACM International Conference on Multimedia.ACM, 2014, pp. 497–506.
[20]W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in
IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2009,pp.725 418–725 418.
[21]W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, "Secure image retrieval through feature protection," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, 2009, pp. 1533– 1536.
[22]B. Cheng, L. Zhuo, Y. Bai, Y. Peng, and J. Zhang, "Secure index construction for privacy-preserving large-scale image retrieval," in Big Data and Cloud Computing (BdCloud), 2014 IEEE Fourth International Conference on. IEEE, 2014, pp. 116–120.