Securing the Privacy on content based retrieval image in cloud

Prof Pokharkar.S.T [1], Prof Tupe Kapil .A[2], Prof Shete Ajit. J [3], Prof Wadnere Umesh.P [4]

[1] Prof satish tukaram pokharkar, SCSCOE Rahuri factory maharshtara, India
[2] Prof Tupe Kapil .A, SCSCOE Rahuri factory Maharashtra, India
[3] Prof Shete Ajit. J, SCSCOE Rahuri factory Maharashtra, India
[4] Prof Wadnere Umesh.P, SCSCOE Rahuri factory Maharashtra, India

ABSTRACT

Capacity prerequisites for visual information have been expanding as of late, after the rise of some exceptionally Intuitive sight and sound administrations and applications for cell phones in both individual and corporate situations. This has been a key driving component for the selection of cloud-based information outsourcing arrangements. Nonetheless, outsourcing information stockpiling to the Cloud additionally prompts new security challenges that must be painstakingly tended to, particularly with respect to protection. In this paper we propose a safe structure for outsourced security protecting capacity and recovery in substantial shared picture stores. Our proposition depends on IES-CBIR, a novel Picture Encryption Scheme that shows Content-Based Image Retrieval properties. The system empowers both scrambled stockpiling furthermore, looking utilizing Content-Based Image Retrieval inquiries while protecting security against legitimate however inquisitive cloud executives. We have assembled a model of the proposed system, formally broke down and demonstrated its security properties, and tentatively assessed its execution and recovery exactness. Our outcomes demonstrate that IES-CBIR is provably secure, permits more efficient operations than existing proposition, both as far as time and space many-sided quality, and makes ready for new down to earth application situations.

Keyword - *Data and Computation Outsourcing; Encrypted Data Processing; Searchable Encryption; Content-Based Image Retrieval*

1 INTRODUCTION

These days visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corporate and individual utilize situations [1]. The measure of pictures, illustrations, and photographs being created and shared regular, particularly through cell phones, is developing at an ever expanding rate. The capacity requirements for such vast sums of information in asset obliged cell phones has been a driving element for information outsourcing administrations, for example, the ones utilizing Cloud Storage and Computing arrangements. Such administrations (e.g. Instagram and Flickr) have been accounted for to be among the biggest developing web administrations [2]. Expansion partner, the accessibility of a lot of pictures in broad daylight what's more, private archives additionally prompts the requirement for content- based inquiry and recovery arrangements (CBIR) [3]. In spite of the way that information outsourcing, particularly to cloud registering foundations, appears a characteristic answer for sup- port extensive scale picture stockpiling and recovery frameworks, it moreover brings new difficulties up as far as information security control. This is a result of outsourcing information, which typically infers discharging control (and a few times even compelling proprietorship) over it [4]. Late episodes have given clear proof that security ought not be required to be protected by cloud suppliers [5], [6]. Besides, noxious or just indiscreet framework chairmen working for the suppliers have full access to information on the facilitating cloud machines [7], [8]. At long last, outer programmers can abuse programming vulnerable- ities to increase unapproved access to servers [9]. The current episode with the iCloud picture stockpiling administration and superstar N OWADAYS visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corpo- rate and individual utilize situations [1]. The measure of pictures, illustrations, and photographs being produced and shared ordinary, particularly through cell phones, is developing at an ever expanding rate. The capacity requirements for such substantial sums of information in asset compelled cell phones has been a driving component for information outsourcing administrations, for example, the ones utilizing Cloud Storage and Computing arrangements. Such administrations (e.g. Instagram and Flickr) have been accounted for to be among the biggest developing web administrations [2]. Expansion partner, the accessibility of a lot of pictures in broad daylight what's more, private archives additionally prompts the requirement for content- based inquiry and recovery arrangements (CBIR) [3]. In spite of the way that information outsourcing, particularly to cloud registering foundations, appears a characteristic answer for sup- port huge scale picture stockpiling and recovery frameworks, it too brings new difficulties up regarding information protection control. This is a result of outsourcing information, which normally suggests discharging control (and a few times even successful possession) over it [4]. Late occurrences have given clear confirmation protection ought not be required to be saved by cloud suppliers [5], [6]. Moreover, malevolent or basically reckless framework executives working for the suppliers have full access to information on the facilitating cloud machines [7], [8]. At last, outside programmers can misuse programming vulnerable- ities to increase unapproved access to servers [9]. The current episode with the iCloud picture stockpiling administration and celebrity OWADAYS visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corpo- rate and individual utilize situations [1]. The measure of pictures, illustrations, and photographs being produced and shared ordinary, particularly through cell phones, is developing at an ever expanding rate. The capacity requirements for such expansive sums of information in asset obliged cell phones has been a driving variable for information outsourcing administrations, for example, the ones utilizing Cloud Storage and Computing arrangements. Such administrations (e.g. Instagram and Flickr) have been accounted for to be among the biggest developing web administrations [2]. Expansion partner, the accessibility of a lot of pictures in broad daylight what's more, private vaults likewise prompts the requirement for content- based pursuit and recovery arrangements (CBIR) [3].Notwithstanding the way that information outsourcing, particularly to cloud figuring foundations, appears a characteristic answer for sup- port expansive scale picture stockpiling and recovery frameworks, it moreover brings new difficulties up as far as information security control. This is an outcome of outsourcing information, which typically suggests discharging control (and a few times even powerful possession) over it [4]. Late episodes have given clear confirmation that security ought not be relied upon to be saved by cloud suppliers [5], [6]. Besides, malignant or essentially indiscreet framework directors working for the suppliers have full access to information on the facilitating cloud machines [7], [8]. At long last, outside programmers can abuse programming vulnerable- ities to increase unapproved access to servers [9]. The current occurrence with the iCloud picture stockpiling administration and superstar (uplink). Due to the compact design, test subjects can wear the system nodes without impeding their body movements. The measurements enable the evaluation of the RF-EMFs incident on the body and allow a comparison with international radiation regulation such as those of the International Commission on Non-Ionizing Radiation Protection (ICNIRP) [2]. In addition to the dissymmetric measurement, two inertial sensors were integrated into the system, in order to quantify activity parameters of the test subject [3]. A tri-axial accelerometer and tri-axial gyroscope measure the accelerations and angular speeds of the measurement nodes. This paper presents the validation of the proposed system for two orthogonal polarizations in the 2.4 GHz ISM band in an anechoic and reverberation chamber, as well as in an indoor office space. The main focus in the proposed experiments into demonstrate feasibility and merits of a distributed PDE with integrated inertial sensing to acquire high quality data that takes the presence and motion of the human body into account during-EMF exposure assessments

2. RELATED WORK

These days visual information is in charge of one of the biggest offers of worldwide Internet traffic in both corporate and individual utilize situations [1]. The measure of pictures, designs, and photographs being created and shared ordinary, particularly through cell phones, is developing at an ever expanding rate. The capacity requirements for such expansive sums of information in asset obliged cell phones has been a driving element for information outsourcing administrations, for example, the ones utilizing Cloud Storage and Computing arrangements. Such administrations (e.g. Instagram and Flickr) have been accounted for to be among the biggest developing web administrations [2]. Expansion partner, the accessibility of a lot of pictures out in the open what's more, private stores likewise prompts the requirement for content- based inquiry and recovery arrangements (CBIR) [3]. In spite of the way that information outsourcing, particularly to cloud registering frameworks, appears a characteristic answer for sup- port huge scale picture stockpiling and recovery frameworks, it too brings new difficulties up as far as information security control. This is an outcome of outsourcing information, which generally suggests discharging control (and a few times even compelling possession) over it [4]. Late episodes have given clear confirmation that security ought not to be relied upon to be safeguarded by cloud suppliers [5], [6]. Besides, noxious or basically imprudent framework heads working for the suppliers Past proposition for supporting outsourced stockpiling, hunt, and recovery of pictures in the scrambled area can be comprehensively separated in two classes: those in view of Searchable Symmetric Encryption (SSE) procedures and those based on Public-Key halfway Homomorphism Encryption (PKHE). SSE has been generally utilized as a part of the past by the exploration group, particularly for content information [23], [24], [25]. In the picture area, despite the fact that not distinguished as SSE plans, various frameworks utilize the same (or comparative) strategies for picture look/recovery [17], [18], [19], [26]. For effortlessness, we allude to these as SSE-based arrangements. In SSE-based arrangements, customers process their information before scrambling and outsourcing it to the Cloud. From this handling, a file is made, scrambled, and put away in the outsourced foundation, which enables customers to look through their information effectively what's more, secure. Information is normally encoded with probabilistic symmetric-key encryption plans, while the record is secured through a blend of probabilistic and deterministic (or even request safeguarding [27]) encryption. Sadly, SSE-based methodologies by and large offer the following impediments:

(I) Clients either require a trusted intermediary [18] or need to file their pictures (and encode that list) locally [17], [26], which involves the utilization of extra computational power on their side and restricts the common sense of such answers for asset compelled cell phones. This impact is further exacerbated while considering dynamic situations, where pictures are always being included, refreshed, and expelled. In such unique situations, SSE arrangements typically require various rounds of correspondence for refreshing picture stores and their records. For example, a past approach by Lu et al. [17] utilizes archive wide insights (e.g. backwards archive frequencies), which change as the storehouses are refreshed and hence drive the re-development and re-encryption of the record, expecting customers to download what's more, decode the full substance of the store. Furthermore record esteems are encoded with a request safeguarding encryption conspire that relies upon plaintext space conveyance. With various updates this circulation changes, once more require the re-development and re-encryption of the file. This is an imperative issue from a security perspective. Other comes closer from the writing require various rounds of correspondence for performing such operations [18], [24], [26];

(ii) Clients need to exchange extra information to the cloud, rather than simply transferring pictures, they additionally need to recover what's more, re-transfer their scrambled list with every vault refresh. This prompts extra data transfer capacity use, contrarily affecting the inertness of capacity operations as saw by clients and being a specific issue for cloud backed organizations;

(iii) As SSE works utilize deterministic tokens to give their usefulness with functional execution. Deterministic Tokens incorporate special record identifiers and deterministic encryptions of watchwords. Thusly they spill what are known as pursuit, access, comparability, and refresh designs [18], [23], [24], [25], i.e. they uncover individually: if an inquiry has been submitted earlier; which pictures are returned for each question; which pictures are like a given query image (in the event of comparability/positioned hunt); and which pictures (beforehand sought) are like another picture being embedded. These spillage designs bring about uncovering as much data as a completely deterministic encryption conspire, though with significantly higher computational overhead. This is exhibited in [28] and is especially apparent in seemingly perpetual framework with many questions being executed simultaneously and all list passages being gotten to. In any case, the peruser should take note of that deterministic plans (and SSE-based plans with the alluded spillages) can in any case be provably-secure, as long as the larger amount applications utilizing them control the measure of foundation data spilled to foes (counting plaintext circulation learning) [28].

3. TECHNICAL OVERVIEW

To beat the restrictions of the condition of workmanship, we propose a structure for protection safeguarding outsourced capacity, inquiry, and recovery of pictures in substantial scale, progressively refreshed vaults. Our system is made out of two principle parts: a picture encryption segment, executed on customer gadgets; and a capacity, ordering, and looking part (in the scrambled space), executed in the outsourcing server (e.g. a cloud supplier). We base this system on another encryption plot particularly intended for pictures, called IES-CBIR, which enables us to configuration outsourced picture store frameworks that help content-based picture recovery (CBIR) in

View of shading highlights, while ensuring the protection of both picture proprietors also, different clients issuing inquiries. Concerning condition of-craftsmanship, IES-CBIR indicates tantamount recovery exactness and higher Computational execution than past methodologies as seen by customers, since it safely moves ordering calculations to the cloud supplier's framework and evades open key and homomorphism cryptography. IES-CBIR too limits cipher text development and thusly transmission capacity and outsourced space prerequisites, fortifying the positive effect on client saw inertness. These advantages are additionally delineated in our trial work exhibited in Segment 5, where the execution of an IES-CBIR framework is looked at against the condition of-workmanship SSE [17] and PKHE [15] based methodologies. For the rest of the paper we utilize the accompanying wording: an archive is an accumulation of pictures which is put away in the framework of a cloud supplier; the cloud server, or simply cloud, is the outsourcing framework that goes about as a server both for capacity and calculation over pictures; clients are the customers of our framework, potentially utilizing lightweight cell phones, where every client gets to one or more archives to inquiry, include, and refresh pictures at any time; archive keys are mystery cryptographic keys that are used to inquiry, include, and refresh pictures in the vaults (every store has its own vault key); picture keys are mystery keys utilized for encoding and unscrambling pictures in the vaults, in conjunction with the individual store keys. In the accompanying subsections we introduce the framework demonstrate for our proposed structure (Sections 3.1), took after by its foe model and security suppositions (Sections 3.2) and by some important utilize cases we imagine for the use of our proposition.

3.1 System Model and Architecture

We now portray the framework model and engineering imagined for utilizing our system and IES-CBIR. In this Demonstrate, we consider two fundamental substances: the cloud and (various) clients (Figure 1). Pictures are outsourced to stores that live in the cloud. Every archive is utilized by products Clients, where they can both include their own particular pictures or potentially look utilizing an inquiry picture. Clients can likewise ask for get to to put away pictures from their makers/proprietors. Our target is to guarantee the security of clients, subsequently all information sent to the cloud is encoded. Every vault is made by a solitary client.

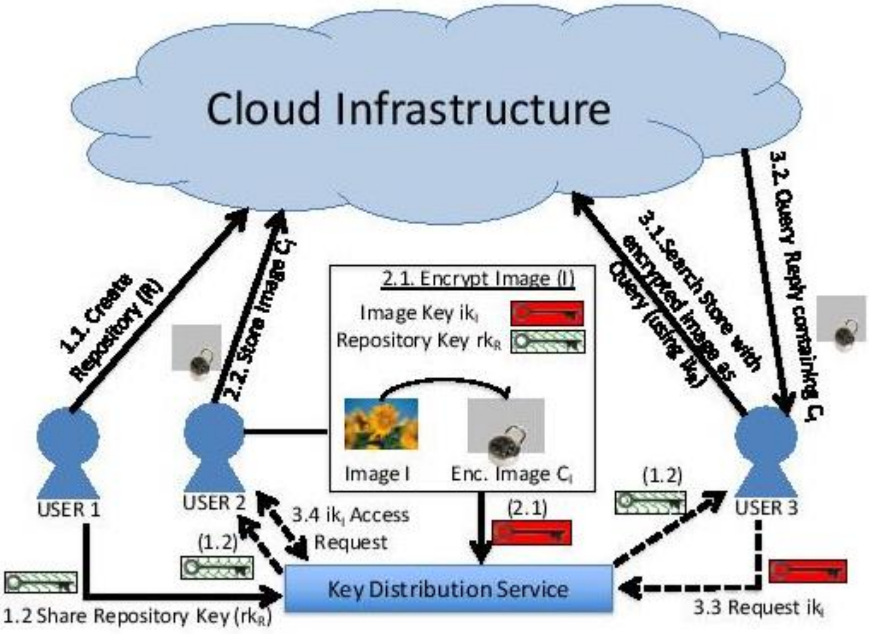

Fig. 1: System model overview of the proposed framework.

3.2 Adversary Model

In this work we center at ensuring the security of clients' pictures and questions. The fundamental enemy we consider is the cloud chairman, who works the cloud's foundation also, servers. Like numerous past works found in the writing [17], [18], [23], [24], [25], [27], we accept a honest but-inquisitive foe [4], implying that the cloud is viewed as a latent foe that is required to accurately perform operations when asked (i.e. satisfy its agreement understandings), be that as it may, may listen in and divulgence clients' information. We expect that a pernicious cloud executive approaches all information put away on circle or in RAM on any gadget situated at the cloud foundation, and going through the system from or to the cloud. In Section 4.4, we formally demonstrate the security of our system against such an enemy. A more grounded foe that ought to likewise be considered is the malevolent client, i.e. a client of the framework who goes astray from his normal conduct. Pernicious clients are an open issue for any multi-client application, as they might be offered access to numerous vault and picture keys some time recently being found, and would more be able to effectively listen in on other clients' pictures. In this work we concentrate on ensuring our proposition and demonstrating their security against the legit but curious cloud director, and leave the vindictive clients challenge as a future research heading. In any case, we recognize that diverse orthogonal systems can be sent to relieve the difficulties presented by malevolent clients, including access control strategies, storehouse get to denial, and intermittent key refreshment [23]. Moreover, we don't consider honesty or accessibility dangers, as these can be taken care of by various systems that are orthogonal to our commitments.

4. IES-CBIR Design and Implementation

The main component on the users' side leverages a novel cryptographic scheme specifically designed for images and Privacy preserving CBIR, dubbed IES-CBIR. Before describing IES-CBIR in detail, we give a definition of image privacy that underlines our work .An Image Encryption Scheme with CBIR properties is a tuple (GENRK, GENIK, ENC, DEC, TRPGEN) of five polynomial-time algorithms run by a user, where:

* GENRK (sprk): is a probabilistic algorithm that takes as input the security parameter sprk 2 N and generates a repository key rk;

* GENIK (spik): is a probabilistic algorithm that takes as input the security parameter spik 2 N and generates an image key ik;

* ENC (I; rk; ik): takes as input an image I and the cryptographic keys frk; ikg, returning an encrypted image CI ;

*DEC (CI; rk; ik): takes as input an encrypted image Cardkeys frk; ikg, returning the decrypted image I ;

* TRPGEN (Q; rk): takes as input a query image Q and repository key rk, returning a searching trapdoor CQ

4.1.1 Key Generation

IES-CBIR works with two distinct sorts of cryptographic keys, storehouse keys (rk) and picture keys (ik), which are created by the GENRK and GENIK calculations separately. Repository keys deterministically map a pixel's color value in a color channel to some new random value4. To prevent images from increasing in size after encryption (i.e. prevent cipher text expansion), encrypted pixels should be in the same range of values as their original plaintexts (usually 8 bitsper color channel). As such, we build repository keys in IESCBIR by performing random permutations of all possible pixel color values in each color channel. Leveraging the HSVcolor space ((H) hue, (S) saturation, (V) value/brightness),we perform three independent random permutations of thevalues in range [0::100]. This range represents all possible color values in the HSV color space, and each permutationis used for a different color channel, resulting in 3 repository sub-keys: rkH ; rkS; rkV. Permutations are performed bya Pseudo-Random Generator (PRG) [21] G parameterized.

4.1.2 Encryption

Picture encryption in IES-CBIR is accomplished through two primary advances and a last (discretionary) advance: i) pixel color values encryption, ii) pixel positions permutation, and iii) image compression. The goal of the first step is to protect image color features, through the application of a Pseudo-Random Permutation (PRP) [21] P on all pixel color values. Although we could use a standard PRP construction to instantiate (such as an AES-based PRP [21]), we chose to conceive specific color-domain PRP, allowing us to preserve the format of encrypted images. Our construction encrypts pixel color values by deterministically replacing them, in each color channel, using repository key rk = frkH ; rkS; rkVg.Equation 2 represents this operation, where Prk (pz) is the encryption of pixel p in color component z through P and key rkz, and cpzis the resulting cipher text

4.1.3 Decryption

The decryption algorithm applies the different steps of encryption in the inverse order, or more formally, through the ordered application of the transformations) is the encryption of pixel p in color component z through P and Key rkz and cpzis the resulting cipher text.

4.2 Framework Protocols

```
Algorithm 1 Operation Create New Repository
procedure USER (IDU).CREATEREPOSITORY (ID R, sprk, spik, n, m, fID Ii; Iigdi=0)
    rkR   IES-CBIR.GenRK (sprk)
    for all fID Ii; Iigdi=0do
        ikIiIES-CBIR.GenIK(spik)
        CIiIES-CBIR.Enc(Ii; rkR; ikIi)
    end for
    CLOUD.CreateRepository (ID R; n; m; IDU; fID Ii; CIigdi=0)
    return frkR; fikIigdi=0g
end procedure.
```

```
procedure CLOUD.C REATEREPOSITORY (ID R, n, m, IDU, fID Ii; CIigdi=0)
    RepR= fID Ii; fCIi; IDUigg   i=0InitiateRepository ()
    Idx R = fID vwi; fID Ij; f reqIjvwig   j=0gni=0InitiateIndex (n)
    for all fCIigdi=0do
        f vCIi= fhistH; histS; histV g   Extract Features (CIi)
    end for
    CBR   ClusterFeaturesIntoCodebook (n; m; ff vCIigdi=0)
    for all fID Ii; CIi; f vCIigdi=0do
        vwCI= fID vwj; f reqCIivwjgjvwCIijj=0CBR.Stem (f vCIi)
        for all fID vwj; f reqCIivwjgjvwCIijj=0do
            Idx R[ID vwj].add(fID Ii; f reqCIivwg)
        end for
        RepR [ID Ii]   fCIi; IDUg
    end for
end procedure
```

Algorithm 2 Operation Store/Update Image.

```
procedure USER (IDU).UPDATEI MAGE (ID R; rkR; ID I; I; spik)
    ikI   IES-CBIR.GenIK(spik)
    CI   IES-CBIR.Enc (I; rkR; ikI )
    cloud.StoreImage (ID R; ID I ; CI ; IDU)
    return fikIg
end procedure.
procedure CLOUD.U PDATEI MAGE (ID R; ID I ; CI ; IDU)
    if RepR.contains (ID I ) then
        cloud.Remove (ID R; ID I )
    end if
    f vCI= fhistH; histS; histV g   Extract Features (CI )
    vwCI= fID vwi; f reqCIvwigjvwCIji=0CBIDR.Stem (f vCI)
    for all fID vwi; f reqCIvwigjvwCIji=0do
        Idx R[ID vwi].add (fID I ; f reqCIvwig)
    end for
    RepR [ID I ]   {fCI ; IDUg}
end procedure
```

Algorithm 3 Operation Search with Image as Query

```
procedure USER (IDU).SEARCH (ID R; Q; rkR; k)
    CQ   IES-CBIR.GenTrp (Q; rkR)
    rankedImgDistances   cloud. Search (ID R; CQ; k)
    return rankedImgDistances
end procedure.
procedure CLOUD.S EARCH (ID R; CQ; k)
    qr   InitiateQueryResults ()
    f vCQ= fhistH; histS; histV g   Extract Features (CQ)
    vwCQ= fID vwi; f reqCQvwigjvwCQji=0CBR.Stem (f vCQ)
    for all fID vwi; f reqCQvwigjvwCQji=0do
        PLvwi= fID Ij; f reqCIjvwigjPLvwijj=0Idx R[ID vwi]
        for all fID Ij; f reqCIjvwigjPLvwijj=0do
            scoreQIjScaledTfIdf (f reqCQvwi, f reqCIjvwi, jRepIDRj,jPLvwij)
            fCIj; IDUjg   RepR [ID Ij]
            qr[ID Ij]   fCIj; qr[ID Ij]:score + scoreQIj; IDUjg)
        end for
    end for
    return resize(k, Sort(qr))
end procedure
```

Algorithm 4 Operation Access Image

```
procedure USER (IDU).ACCESS (CI; rkR; ikI )
    I   IES-CBIR.Enc (CI; rkR; ikI)
    return I
end procedure
```

Algorithm 5 Operations Remove Image

```
procedure CLOUD. REMOVE (ID R; ID I )
    RepR [ID I ] = fg
    for all PLvw 2 Idx R do
        PLvw.Remove (ID I )
    end for
end procedure
```

5. CONCLUSIONS

In this paper we have proposed another protected system for the security safeguarding outsourced capacity, look, and recovery of vast scale, powerfully refreshed picture archives, where the diminishment of customer overheads is a focal angle. In the premise of our system is a novel cryptographic plan, particularly intended for pictures, named IES-CBIR. Key to its plan is the perception that in pictures, shading data can be isolated from surface data, empowering the utilization of various encryption strategies with various properties for everyone, and permitting privacy preserving Content-Based Image Retrieval to be performed by outsider, untrusted cloud servers. We formally investigated the security of our proposition, and extra test assessment of executed models uncovered that Our approach accomplishes a fascinating exchange off amongst accuracy and review in CBIR, while showing elite What's more, versatility when contrasted and elective arrangements. A fascinating future work course is to explore the materialness of our philosophy - i.e. the partition of data settings when preparing information (shading and surface in this commitment) - in different spaces past picture information

6. REFERENCES

[1]. Reference 1 Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories Bernardo Ferreira, Student Member, IEEE, Jo ˜ ao Rodrigues, Jo ˜ ao Leit ˜ ao, Member, IEEE,and Henrique Domingos, Member, IEEE

[2]. Reference 2 Global Web Index, "Instagram tops the list of social network growth," http://tinyurl.com/hnwwlzm, 2013

[3] C. D. Manning, P. Raghavan, and H. Sch ¨ utze, An Introduction to Information Retrieval. Cambridge University Press, 2009, vol. 1.

[4] R. Chow, P. Golle, M. Jacobson, E. Shi, J. Staddon, R. Masuoka,and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in CCSW'09, 2009.

[5] D. Rushe, "Google: don't expect privacy when sending to Gmail,"http://tinyurl.com/kjga34x, 2013.

[6] G. Greenwald and E. Mac skill, "NSA Prism programtaps in to user data of Apple, Google and others," http://tinyurl.com/oea3g8t, 2013.

[7] A. Chen, "GCreep: Google Engineer Stalked Teens, Spied on Chats," http://gawker.com/5637234, 2010.

[8] J. Halderman and S. Schoen, "Lest we remember: cold-boot attack son encryption keys," in Commun. ACM, vol. 52, no. 5, 2009.

[9] National Vulnerability Database, "CVE Statistics,"http://web.nvd.nist.gov/view/vuln/statistics, 2014.

[10] D. Lewis, "iCloud Data Breach: Hacking And Celebrity Photos,"https://tinyurl.com/nohznmr, 2014.

[11] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, andM. Walfish, "Depot: Cloud Storage with Minimal Trust," ACMTrans. Comput. Syst., vol. 29, no. 4, pp. 1–38, dec 2011.

[12] C. Gentry, S. Halevi, and N. P. Smart, "Monomorphic evaluation of the AES circuit," in CRYPTO'12. Springer, 2012, pp. 850–867.

[13] P. Parlier, "Public-key cryptosystems based on composite degreeresiduosity classes," in EUROCRYPT'99, 1999, pp. 223–238.

[14] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Adv. Cryptol. Springer, 1985.

[15] 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.

[16] P. Zheng and J. Huang, "An efficient image monomorphic encryption scheme with small cipher text expansion," in MM'13, 2013.

[17] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, “Enabling Search over Encrypted Multimedia Databases,” in IS&T/SPIE Electron. Imaging, feb 2009, pp. 725 418–725 418–11.
[18] X. Yuan, X. Wang, C. Wang, A. Squicciarini, and K. Ren, “Enabling Privacy-preserving Image-centric Social Discovery,” in ICDCS’14.IEEE, 2014.
[19] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-maillet, “A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval,” TIFS, vol. 10, no. 1, pp. 152–167, 2015.
[20] J. Z. Wang, J. Li, and G. Wiederhold, “Simplicity: Semantics sensitive Integrated Matching for Picture Libraries,” IEEE Trans.Pattern Anal. Mach. Intell., vol. 23, no. 9, pp. 947–963, 2001.
[21] J. Katz and Y. Lindell, Introduction to Modern Cryptography. CRCPRESS, 2007.
[22] B. Ferreira, J. Rodrigues, J. Leit ˜ ao, and H. Domingos, “Privacy Preserving Content-Based Image Retrieval in the Cloud,” inSRDS’15. IEEE, 2015
[23] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Dentitions and Efcient Constructions,” in CCS’06, 2006, pp. 79–88.
[24] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient Similarity Search over Encrypted Data,” in ICDE’12, 2012, pp. 1156–1167.
[25] F. Hahn and F. Kerschbaum, “Searchable Encryption with Secureand Efficient Updates,” in CCS’14. ACM, 2014, pp. 310–320.
[26] 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, 2015.
[27] R. A. Popa, F. H. Li, and N. Zeldovich, “An Ideal-Security Protocol for Order-Preserving Encoding,” S&P’13, may 2013