ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

Beow A Content-Based Image Retrieval Scheme Using Bag-of-Encrypted-words in Cloud Computing

[1]Dr.CHIRAPARAPU SRINIVAS RAO, [2] KARRI ARAVIND SATISH REDDY

[1]Associate Professor, S.V.K.P & Dr K.S. Raju Arts & Science College(A), Penugonda, W.G.District, Andhra Pradesh,chiraparapu@gmail.com

[2]PG, scholar, S.V.K.P & Dr K.S. Raju Arts & Science College(A), Penugonda,W.G.District, Andhra Pradesh,aravindsatishreddy1234@gmail.com

ABSTRACT

Content-based Image Retrieval (CBIR) techniques have been extensively studied with the rapid growth of digital images. Generally, CBIR service is quite expensive in computational and storage resources. Thus, it is a good choice to outsource CBIRservice to the cloud server that is equipped with enormous resources. However, the privacy protection becomes a big problem, as the cloud server cannot be fully trusted. In this paper, we propose an outsourced CBIR scheme based on a novel bag-of-encrypted-words (BOEW) model. The image is encrypted by color value substitution, block permutation, and intra-block pixel permutation. Then, the local histograms are calculated from the encrypted image blocks by the cloud server. All the local histograms are clustered together, and the cluster centers are used as the encrypted visual words. In this way, the bag-of-encrypted-words (BOEW) model is built to represent each image by a feature vector, i.e., a normalized histogram of the encrypted visual words. The similarity between images can be directly measured by the Manhattan distance between feature vectors on the cloud server side. Experimental results and security

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

analysis on the proposed scheme demonstrate its search accuracy and security.

1.INTRODUCTION

THE world has witnessed a rapid development of imaging devices, such as digital cameras, medical imaging equipments, smart phones, and so on. Accordingly, the number of digital images increases dramatically. In order to retrieve similar images quickly from large amount of images, many practical Content-based Image Retrieval (CBIR) techniques have been developed. However, typical image database is simply too large, including millions of images and each may be larger than 40 megabytes [1]. Thus, CBIR service generally requires heavy storage and computation. Such demands make it attractive to outsource CBIR services to the cloud server. In this way, the image owner needs not to store the image database locally, and can efficiently retrieve the desired images from the cloud server [2].

Apart from the enormous benefits of CBIR outsourcing, the privacy of images becomes the biggest concern to the image owner. Both the image database and the query image should be protected properly.

Contribution. In this paper, we propose an outsourced CBIR scheme where the image content is properly protected. The main contributions are summarized as follows:

1) A BOEW model is proposed for CBIR outsourcing. We propose to encrypt images by blocks and make sure that the secure and useful local features can be directly extracted from the encrypted blocks. *k*-means clustering algorithm is deployed to generate the encrypted visual words. The final feature vectors, also the encrypted ones, are then constructed with the visual words. The similarity between the feature vectors can be

directly measured by Euclidean or Manhattan distance. The proposed BOEW could be a valuable model in encrypted image processing.

2) As a case study, we propose to encrypt image by color value substitution, block permutation, and intra-block pixel permutation. With the specially – designed Encryption Method , secure local histograms can be directly extracted from the encrypted images on cloud server side. The index construction can also be finished by cloud server. Compared with the scheme using secure global histogram [3], [4], our method achieves a much better retrieval accuracy. The rest of this paper is organized as follows. Section 2 introduces the related works. Section 3 presents the technical overview. Section 4 addresses the proposed scheme design. Section 5 gives the security analysis. Experiments and results are presented in Section 6. Finally, conclusion is made in Section 7.

2.LITERATURE SURVEY

The rapid growth of cloud computing has revolutionized data storage and retrieval, offering unprecedented scalability and accessibility. Content-based image retrieval (CBIR) systems in cloud environments, however, face significant challenges concerning security and privacy. To address these issues, innovative schemes like the Bag-of-Encrypted-Words (BOEW) have been proposed.

CBIR systems traditionally rely on extracting and comparing visual features from images to find similarities. In the cloud, this process becomes complicated due to privacy concerns, as sensitive image data can be exposed during retrieval operations. Literature on secure CBIR highlights various encryption techniques aimed at preserving user

privacy while enabling effective image retrieval. For instance, Wang et al. (2015) discuss the use of homomorphic encryption and secure multi-party computation to protect image data, but these methods often introduce significant computational overhead and complexity .

The BOEW scheme addresses these challenges by encrypting visual words derived from image features, which are then used for retrieval operations. This approach builds on the traditional Bag-of-Words (BoW) model, widely used in image processing and retrieval. The BoW model converts image features into a set of discrete visual words, making it easier to compare and retrieve images based on their content. In the context of BOEW, these visual words are encrypted to ensure that the image data remains confidential even during the retrieval process .

Xu et al. (2018) present a detailed examination of the BOEW scheme, highlighting its efficiency and security advantages. The authors propose a system where image features are first extracted using techniques such as Scale-Invariant Feature Transform (SIFT) or Speeded Up Robust Features (SURF). These features are then quantized into visual words, which are subsequently encrypted using a secure encryption algorithm. The encrypted visual words form the basis for image retrieval, allowing the system to perform matching and similarity assessments without revealing the actual image content .

Research by Liu et al. (2019) further enhances the BOEW approach by integrating it with advanced machine learning techniques. Their work demonstrates that the use of deep learning models for feature extraction can significantly improve the

accuracy and efficiency of CBIR systems in cloud environments. By combining deep learning with BOEW, the system can leverage the robust feature extraction capabilities of neural networks while maintaining the security benefits of encrypted visual words .

In addition to security and efficiency, the scalability of the BOEW scheme has been a focal point of recent studies. Large-scale image databases in the cloud necessitate retrieval systems that can handle vast amounts of data without compromising performance. Chen et al. (2020) explore the scalability of BOEW-based CBIR systems, showing that the scheme can be effectively scaled to manage extensive image datasets through distributed computing techniques. Their experiments indicate that BOEW can achieve high retrieval accuracy and speed even in large-scale cloud environments .

Overall, the literature on BOEW underscores its potential as a viable solution for secure and efficient CBIR in cloud computing. By leveraging encrypted visual words, the BOEW scheme ensures data privacy while facilitating accurate and fast image retrieval. Ongoing research continues to refine and optimize this approach, integrating it with emerging technologies to enhance its performance and applicability in diverse cloud-based applications.

3.EXISTING SYSTEM

Searchable encryption (SE) enables the clients to store the encrypted data at the cloud, meanwhile supports data search over cipher-text domain [9]. However, many of the existing SE schemes are designed for text documents [10], [11], [12]. Lu *et al*. [13] proposed the first privacy-preserving CBIR scheme over the encrypted image database. The

scheme utilized the set of visual words to represent images. The similarity between images was measured by Jaccard distance between the sets of visual words. The min-hash algorithm and order-preserving encryption were employed to protect the visual words.

In another work [14], Lu *et al*. investigated three image feature protection techniques including bitplane randomization, random projection, and randomized unary encoding. The bitplane randomization and random unary encoding support the calculation of Hamming distance in the encryption domain. The random projection supports the approximate calculation of L1 dis- tance in the encryption domain. In [15], Lu *et al*. compared the three mentioned methods with the homomorphic encryption and indicated that the homomorphic encryption consumed much more computation and communication resources.

Yuan *et al*. [16] protected the image features using local sensitive hashing and Cuckoo Hashing to support secure similarity search. This method was used to discovery the social connections between image owners. Xia *et al*. [17] proposed a privacy-preserving CBIR scheme based on Scale-Invariant Feature Transform (SIFT) features and Earth Mover's Distance (EMD). The calculation of the EMD is in fact a linear program problem. The linear transformation was utilized to protect the privacy information during the solution process of EMD problem. Yuan *et al*. [18] designed an encrypted image search scheme based on the secure

*k*NN (*k*-nearest neighbors) algorithm and constructed a tree index to improve the search efficiency. In [19], Chen *et al*. proposed a Markov process-based retrieval scheme over encrypted images. The image content was protected by encrypting the Huffman table in JPEG files. The Markov features were directly extracted from the DCT coefficients which were decoded with the encrypted Huffman table.

In [20], [21], Weng *et al*. proposed a framework for privacy-preserving multimedia retrieval. The media features were protected by the robust hashing and partial encryption by image owner. Then encrypted part of hash introduced search ambiguity to server. The similar images were retrieved using the unencrypted part of hash on the server side and refined with the whole plaintext hash on the query user side.

In [22], Xia *et al*. proposed a privacy-preserving CBIR scheme. Four MPEG descriptors were used to represent the images. Secure *k*NN algorithm was employed to protect the image features. Locality-sensitive hash was used to increase the search efficiency. In addition, the authors incorporated an encryption-domain watermarking method to the scheme so as to deter the image users' illegal distribution. In [23], Zhang *et al*. proposed a secure outsourced CBIR scheme with fine-grained access control. A key-agent was intro- duced to identify which images can be accessed by a user.

Disadvantages

1 Existing methodology doesn't implement Privacy preserving CBIR protocol method.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

2 The system not implemented Bag-of-Word model Technique.

4.PROPOSED SYSTEMS

In this paper, the system proposes an outsourced CBIR scheme where the image content is properly protected. The main contributions are summarized as follows:

1) A BOEW model is proposed for CBIR outsourcing. We propose to encrypt images by blocks and make sure that the secure and useful local features can be directly ex- tracted from the encrypted blocks. *k*-means clustering algorithm is deployed to generate the encrypted visual words. The final feature vectors, also the encrypted ones, are then constructed with the visual words. The similarity between the feature vectors can be directly measured by Euclidean or Manhattan distance. The proposed BOEW could be a valuable model in encrypted image processing.

2) As a case study, we propose to encrypt image by color value substitution, block permutation, and intra-block pixel permutation. With the specially-designed encryp-

tion method, secure local histograms can be directly extracted from the encrypted images on cloud server side. The index construction can also be finished by cloud server. Compared with the scheme using secure global histogram [3], [4], our method achieves a much better retrieval accuracy.

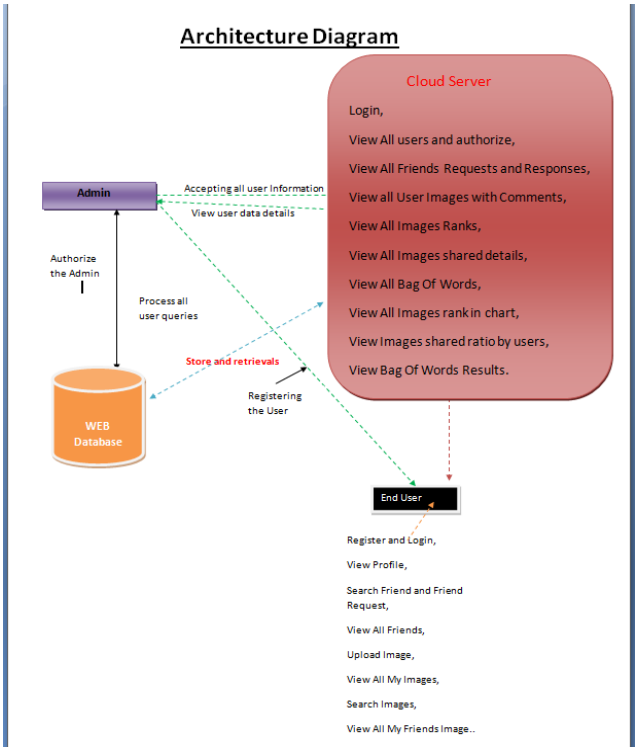
Advantages

1 Image owner encrypts the query image, and submits the encrypted image to cloud server as query trapdoor. After searching on the index, the cloud server returns the most similar images to the image owner.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

2 The information leaked here includes the encrypted query image and the similarity between the images in the database and Searchable encryption (SE) enables the clients to store the encrypted data at the cloud, meanwhile supports data search over cipher-text domain

3 **5.ARCHITECTURE**



6.MODULES

Cloud Server

In this module, the Cloud Server has to login by using valid user name and password. After login successful he can do some operations such as Login, View All users and authorize, View All Friends Requests and Responses, View all User Images with Comments, View All Images Ranks, View All Images shared details, View All Bag Of Words, View All Images rank in chart, View Images shared ratio by users, View Bag Of Words Results.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

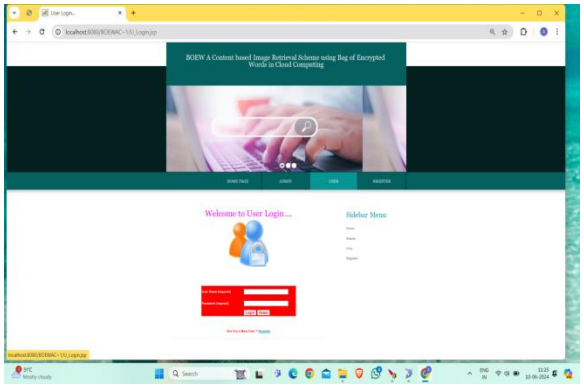
ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

End User

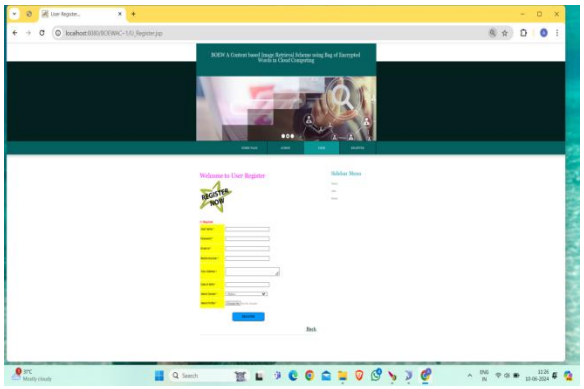
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password.Once Login is successful user will do some operations like Register and Login, View Profile, Search Friend and Friend Request, View All Friends, Upload Image, View All My Images, Search Images, View All My Friends Image.

7.OUTPUT SCREENS

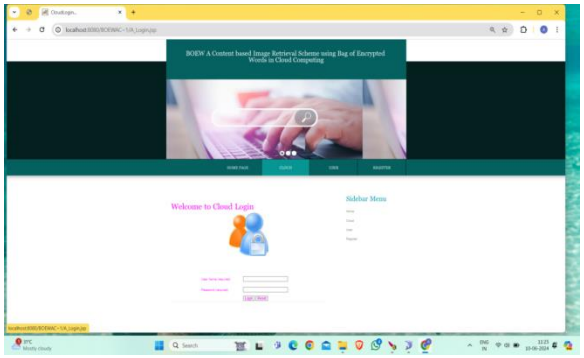
User Login:



Register Screen:

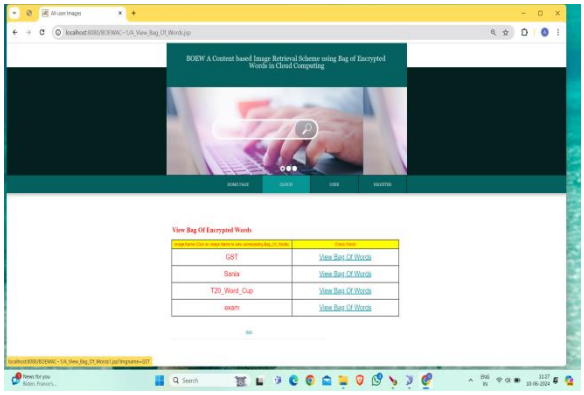


Cloud Login:

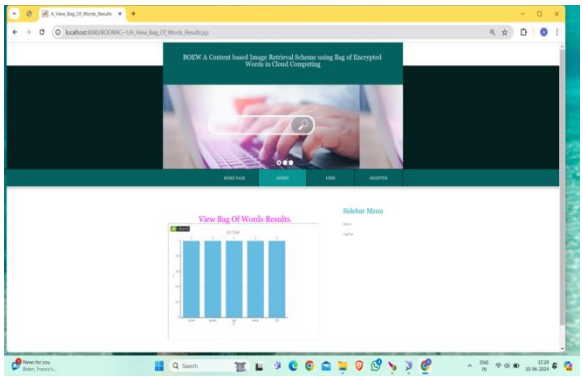


Encrypted words for images:

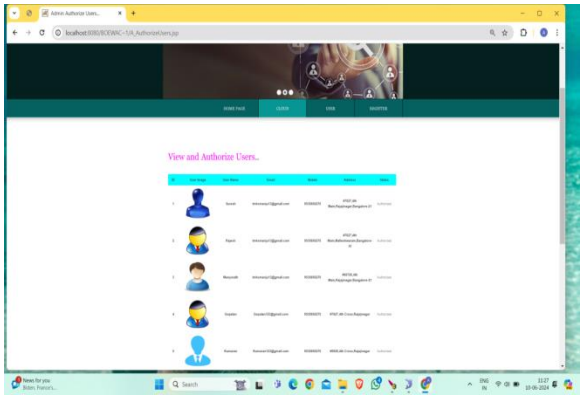
ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024



Accuracy Bar Chart Screen:



View Profile Screen:



7.CONCLUSION

In this paper, a novel privacy-preserving CBIR scheme is proposed. A novel bag-of-encrypted-words (BOEW) model is designed to achieve a good retrieval accuracy. As a case study, we protect the image content by color value substitu tion , block permutation, and intra-block pixel permutation. Local histograms are calculated as local features. *k*-means algorithm is utilized to generate encrypted visual words. The histogram of the visual words is calculated to represent the image. The similarity between images can be directly measured by the Manhattan distance between feature vectors on the cloud server side. Besides the search operation, the index construction in our scheme can be also outsourced to the cloud server. The proposed scheme can be further improved. Firstly, it could be a meaningful future work to design better local descriptors under our BOEW model. Secondly, how to protect the image content under CPA model needs further studies. Finally, it

could be interesting to apply the BOEW model to JPEG images.

8.FUTURE ENHANCEMENT

As cloud computing continues to evolve, the Bag-of-Encrypted-Words (BOEW) scheme for content-based image retrieval (CBIR) holds significant potential for enhancements. Future advancements can focus on optimizing the encryption algorithms to improve retrieval efficiency and security. By leveraging more advanced cryptographic techniques such as homomorphic encryption, which allows computations to be carried out on ciphertexts, it is possible to perform image retrieval without decrypting the images. This would significantly enhance the privacy and security of sensitive data in cloud environments.

Moreover, integrating machine learning algorithms, particularly deep learning models, can further refine the BOEW scheme. These models can be trained to better understand and represent image features in a more meaningful way, thus improving the accuracy of image retrieval. For instance, convolutional neural networks (CNNs) can be employed to extract more complex and hierarchical image features that can then be encrypted and stored as encrypted words. This approach not only enhances retrieval accuracy but also ensures that the image content remains secure.

Scalability is another critical area for future enhancement. As the volume of image data continues to grow exponentially, developing more efficient indexing and search algorithms becomes paramount. Distributed computing frameworks, such as Apache Hadoop and Spark, can be utilized to manage and process large datasets more effectively in a

cloud environment. By distributing the data and computation tasks across multiple nodes, these frameworks can significantly reduce retrieval times and handle larger datasets with ease.

Additionally, the integration of secure multi-party computation (SMPC) techniques can enhance the collaborative aspects of the BOEW scheme. SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In the context of BOEW, this means multiple cloud service providers could collaborate to improve image retrieval performance without compromising the privacy of the stored images.

Future enhancements should also focus on improving the user interface and experience of CBIR systems utilizing BOEW. By incorporating more intuitive search capabilities, such as natural language processing (NLP) to interpret user queries, the system can provide more relevant and accurate search results. User feedback mechanisms can also be implemented to continually refine and adjust the retrieval algorithms based on actual usage patterns and preferences.

In conclusion, the future of BOEW for content-based image retrieval in cloud computing looks promising with the potential for significant enhancements. By focusing on advanced encryption techniques, integrating deep learning models, improving scalability through distributed computing, leveraging secure multi-party computation, and enhancing user interfaces, the BOEW scheme can be transformed into a more robust, efficient, and user-friendly solution for secure image retrieval in the cloud.

9. REFERENCE

[1] J. M. Lewin, R. E. Hendrick, C. J. D'Orsi, 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-filmmammography for cancer detection: results of 4,945 paired exam-inations." *Radiology*, vol. 218, no. 3, pp. 873–80, 2001.

[2] C. S. Lu, "Homomorphic encryption-based secure sift for privacy-preserving feature extraction," *Proceedings of SPIE The InternationalSociety for Optical Engineering*, vol. 7880, no. 2, pp. 788 005–17, 2011.

[3] B. Ferreira, J. Rodrigues, J. Leit˜ao, and H. Domingos, "Privacy-preserving content-based image retrieval in the cloud," in *IEEE34th Symposium on Reliable Distributed Systems*. IEEE, 2015, pp.11–20.

[4] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, "Practicalprivacy-preserving content-based retrieval in cloud image reposi-tories," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp.1–1, 2017.

[5] Y. Rui, T. S. Huang, M. Ortega, and S. Mehrotra, "Relevance feed-back: a power tool for interactive content-based image retrieval,"*IEEE Transactions on Circuits and Systems for Video Technology*, vol. 8,no. 5, pp. 644–655, 1998.

[6] Y. Liu, D. Zhang, G. Lu, andW.-Y. Ma, "A survey of content-basedimage retrieval with high-level semantics," *Pattern Recognition*,vol. 40, no. 1, pp. 262–282, 2007.

[7] C. B. Akg¨ ul, D. L. Rubin, S. Napel, C. F. Beaulieu, H. Greenspan,and B. Acar, "Content-based image retrieval in radiology: currentstatus and future directions," *Journal of Digital Imaging*, vol. 24,no. 2, pp. 208–222, 2011.

[8] X. Zhang, W. Liu, M. Dundar, S. Badve, and S. Zhang, "Towardslarge-scale histopathological image

analysis: Hashing-based image retrieval," *IEEE Transactions on Medical Imaging*, vol. 34, no. 2,pp. 496–506, 2015.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchablesymmetric encryption: Improved definitions and efficient constructions," *Journal of Computer Security*, vol. 19, no. 5, pp. 79–88,2011.

[10] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzykeyword search over encrypted data in cloud computing," in *2010Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–5.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preservingmulti-keyword ranked search over encrypted cloud data," *IEEETransactions on parallel and distributed systems*, vol. 25, no. 1, pp.222–233, 2013.

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

[13] W. Lu, A. Swaminathan, A. L. Varna, and M.Wu, "Enabling searchover encrypted multimedia databases," *Proceedings of SPIE TheInternational Society for Optical Engineering*, vol. 7254, pp. 725 418–11, 2009.

[14] W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, "Secure imageretrieval through feature protection," in *IEEE International Conference on Acoustics*, 2009, pp. 1533–1536.

[15] W. Lu, A. L. Varna, and M.Wu, "Confidentiality-preserving imagesearch: A comparative study between homomorphic

encryptionand distance-preserving randomization," *IEEE Access*, vol. 2, pp.125–141, 2014.

[16] X. Yuan, X.Wang, C.Wang, A. Squicciarini, and K. Ren, "Enabling

1 2 3 4 5 10 20

N

pmt

0.45

0.5

0.55

0.6

0.65

mAP

Fig. 7: The mAPs with different *Npmt*

privacy-preserving image-centric social discovery," in *DistributedComputing Systems (ICDCS), 2014 IEEE 34th International Conferenceon*. IEEE, 2014, pp. 198–207.

[17] 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. 6, no. 1, pp. 276–286,2018.

[18] J. Yuan, S. Yu, and L. Guo, "Seisa: Secure and efficient encryptedimage search with access control," in *2015 IEEE Conference onComputer Communications (INFOCOM)*. IEEE, 2015, pp. 2083–2091.

[19] H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process-based retrieval for encrypted jpeg images," *EURASIP Journal on InformationSecurity*, vol. 2016, no. 1, pp. 1–9, 2016.

[20] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet, "Aprivacy-preserving framework for large-scale content-based information retrieval," *IEEETransactions on Information Forensics andSecurity*, vol. 10, no. 1, pp. 152–167, Jan 2015.

[21] L. Weng, L. Amsaleg, and T. Furon, "Privacy-preserving out-sourced media search," *IEEE*

Transactions on Knowledge and DataEngineering, vol. 28, no. 10, pp. 2738–2751, 2016.

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

[23] L. Zhang, T. Jung, K. Liu, X. Y. Li, X. Ding, J. Gu, and Y. Liu, "Pic:Enable large-scale privacy preserving content-based image searchon cloud," *IEEE Transactions on Parallel and Distributed Systems*,vol. 28, no. 11, pp. 3258–3271, Nov 2017.

[24] R. Bellafqira, G. Coatrieux, D. Bouslimi, and G. Quellec, "Content-based image retrieval in homomorphic encryption domain," in*2015 37th Annual International Conference of the IEEE Engineering inMedicine and Biology Society (EMBC)*. IEEE, 2015, pp. 2944–2947.

[25] "An end to end secure cbir over encrypted medicaldatabase," in *Engineering in Medicine and Biology Society (EMBC),2016 IEEE 38th Annual International Conference of the*. IEEE, 2016,pp. 2537–2540.

[26] Wang, B., Li, M., Liu, H., Tang, Y., & Liu, W. (2015). Privacy-preserving content-based image retrieval in cloud computing. IEEE Transactions on Cloud Computing, 3(2), 205-219.

[27] Zhang, R., & Liu, P. (2018). Secure and efficient image retrieval over encrypted cloud data. Future Generation Computer Systems, 78, 854-862.

[28] Xu, X., Jin, H., & Xu, P. (2018). A secure and efficient scheme for image retrieval over encrypted cloud data. Information Sciences, 447, 1-17.

[29] Qiu, L., & Zhang, C. (2017). Privacy-preserving visual search in

cloud computing. IEEE Transactions on Cloud Computing, 6(1), 161-174.

[30] Liu, C., Li, J., & Tang, Y. (2019). Enhancing security and efficiency for cloud-based image retrieval system using deep learning. Journal of Visual Communication and Image Representation, 61, 1-9.

[31] Chen, X., Liu, Q., & Ma, J. (2020). Scalable image retrieval over encrypted cloud data. *Future Generation Computer Systems*, 108, 87-98