JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing With Double Protection

[1] J.Sheeba Selvapattu, [2] Dr Suchithra R Nair,

[1]Assistant Proffessor, [2] Principal,
[1] Bangalore School of Design and Technology, India,
[2]Presidency College,India,

Abstract : Many content-based picture retrieval techniques have been widely adopted in our daily lives as a result of the exponential development in the number of images. In terms of computing and storage, image retrieval services are typically highly expensive. Thus, picture owners should consider outsourcing services to a cloud server. Yet, because the cloud server can only be partially trusted, privacy protection can become a significant problem for image owners. In this paper, we propose a novel image retrieval scheme. Initially the images are blurred to secure the image data. And encrypting the data.The histogram of encrypted data and original image data is constructed to determine the The similarity between images. Experiments and analysis prove the effect of the scheme**.**

IndexTerms **– Double Protection, Encryption, Content-Based Image Retrieval.**

I. INTRODUCTION

Visual data now accounts for one of the largest shares of global Internet traffic in both corporate and personal use scenarios. Every day, more images, graphics, and photos are created and shared. Many image collections have been created by institutions in the educational, industrial, medical, social, and other spheres of life. Every day, there are more and more creations and exchanges of images, graphics, and photos. In the internet-based world, it becomes vital to store a lot of data. Consumers are encouraged to upload their photos to cloud services because of the quick expansion of image data and the potential loss of local capacity on devices. The storage requirements for such large amounts of data have been a driving factor for data outsourcing services such as those that use Cloud Storage and Computing solutions. Big data processing and storing are made possible by cloud computing systems, which are becoming more crucial. In the internet-based world, it becomes vital to store a lot of data. The image owners can conveniently retrieve the desired images from the cloud via the Internet in this manner, eliminating the need for them to maintain the image collection locally. The owners of the photographs, however, lose ownership of them once they are transferred to the cloud. The primary issue with outsourcing is image privacy. For starters, hackers are constantly interested in attacking cloud servers. A well-known example is the 2014 iCloud breach, which exposed approximately 500 celebrity private photos. The cloud server cannot be completely trusted because they may be interested in the contents of the images as well. Because of the growing popularity of cloud-based information retrieval, image owner are encouraged to store their massive amounts of potentially sensitive data files and computationally expensive tasks on remote cloud servers. Thought the cloud facilitatess the user to storage and resource sharing for better computation. The fact that the data owner and the cloud belong to distinct trust domains also creates serious security and privacy issues [1], [2], [3].

Popular social network companies, like Facebook and Flickr, in particular, frequently have outsourced the user image data to perform a analytics for better user experience with general user data. This are done by extraction features from the image data as a input to the models developed to analysis the data. The private information of the data owner, and also the financial profiles, will unavoidably be made public if original image data is exposed to a semi-trusted cloud service provider. Encrypting sensitive multimedia data locally before outsourcing is a straightforward way to secure the privacy of sensitive data. Privacy-preserving data search in the ciphertext domain has only recently been extended to content-based multimedia retrieval [4], face recognition [5], and fingerprint identification [6]. [7], [8] investigated how to enable secure image search in the data outsourcing environment. In this paper, we propose an efficient double protection approach that ensures the privacy of the user's data.

The following are the main contributions of this work:

1. We propose a method to blur the image using image filter algorithm that can prevent from unauthorized users to extraction feature from the existing image.
2. We propose a image encryption algorithm to secure and efficient searching over encrypted images. The proposed encryption approach is more secure.

3. The histogram of the blur images and encrypted images are done for better analysis of the encryption algorithm and the retrieval accuracy.

The rest of the paper is organized as follows: Section 2 explains the relevant literature .Section 3 defined the proposed approach. Section 4 presents security analysis and section 5 discuss experimental results. Finally, the conclusion is summarized in Section 6

II. Related work

Searchable encryption techniques enable the user to look for specific information within a collection of encrypted data. The majority of existing searchable encryption techniques are used to extract textual information. In earlier stages, basic cryptographic schemes were used to search for the query term in the encrypted text document, with extra care taken to prevent the server from learning anything from outsourced data [9]. Following that, a large number of methods in various thread models were proposed in the literature to achieve various search functionalities, such as multi-keyword top - ranking search [10], similarity search [11], and dynamic search [12]. Many of these schemes, however, are reliable and simple to implement for secure image retrieval tasks. A private content-based picture retrieval method was proposed by Shashank et al. [13] in which the query image is encrypted before being sent to the cloud but the image database is left unencrypted on the server. Other researchers, like [14], kept their subjects' privacy while outsourcing feature extraction, a computationally intensive operation. Running cloud-based queries in a way that protects privacy is the main tactic used in CBIR outsourcing.

Furthermore, homomorphic-based techniques necessitate a large amount of computation power, making them unsuitable for smartphone devices. The first privacy-preserving CBIR technique over encrypted photos was put out by Lu et al. [15], in which images are represented by visual characteristics kept on a cloud server. In order to accomplish similarity matching between the two corresponding images, Jaccard similarity between the visual features of the query image and those in the features database is determined. The min-hash technique and orderpreserving encryption are used to protect the feature vectors of the image. Three feature protection techniques were explored by Lu et al. [16] who compared the security, retrieval efficiency, and computational complexity of each. The authors gave examples of how Bitplane Randomization and Randomised Unary Encoding can be used to easily calculate Hamming distance for feature vectors. But, in the encryption domain, L1 distance can be calculated using features encrypted with a random projection algorithm. Using the previously stated bitplane randomization and randomised unary encoding, Cheng et al. [17] developed a secure CBIR system. A brand-new cryptographic method specifically created for privacy-preserving image indexing and retrieval in sizable image repositories was introduced by Ferreira et al. [18]. In their work, they separated texture from the colour component and encrypted each component using several encryption techniques. The texture component was encrypted using a probabilistic cryptosystem, but the colour component was encrypted using a deterministic cryptosystem, to execute CBIR utilising the colour property. An image retrieval method for encrypted stream cypher images was put out by Cheng et al. [19]. Using support vector machines, our method extracts Markov characteristics from encrypted images and categorises them [20]..

III. Proposed Framework

The proposed framework safeguards user data privacy. The proposed scheme is made up of two parts: the image owner and the cloud server. The two entities each have their own set of responsibilities. The image owner is in charge of blur the image, key generation and image encryption. The proposed model secure the data with double protection to preserve the image data. First stage the images are blurred and in the second stage these blurred images are encrypted by the encryption algorithm by the image owner. The secret key is created using the key generation process and saved to the image owner. the image owner first uses the image encryption algorithm to encrypt the image database. After receiving the encrypted image database, the cloud server builds the index using an index building technique. These encrypted images are saved in the database. The index generation and search are handled by the cloud server. the retrieval trapdoors are generated using the trapdoor creation technique, the owner sends a query request to the cloud server. The cloud server uses the search algorithm to locate related images, which are then returned as search results to the owner of the original image. After receiving the search results, the owner of the image uses the decryption technique and decrypt the image

Finally, the image owner is in charge of image decryption and reblur the image. By using an energy-efficient encryption technique to encrypt photos, our framework safeguards user data as shown in Fig 1

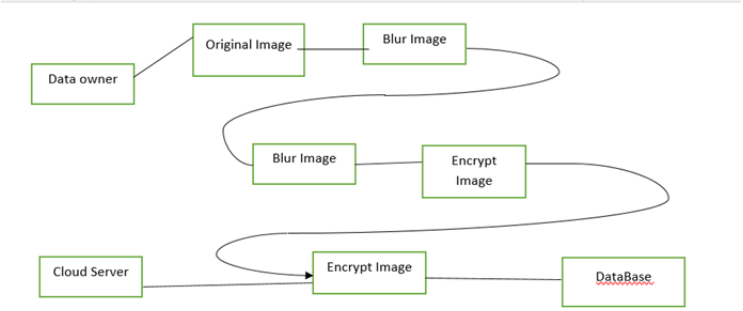
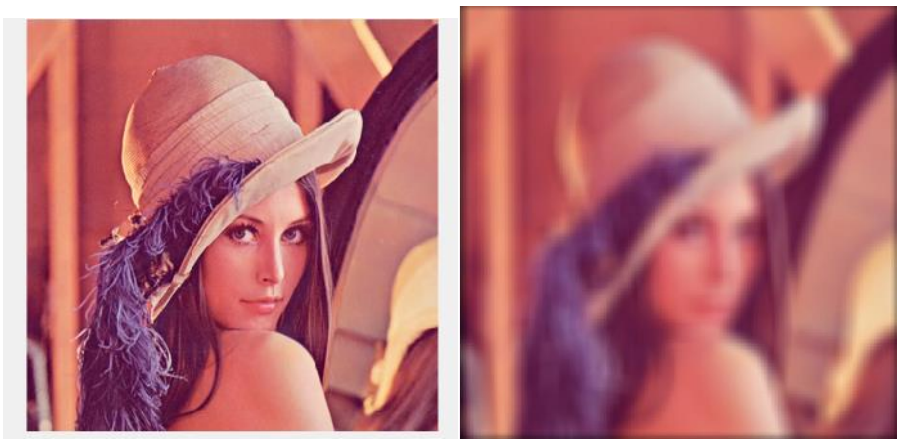


Fig 1: Proposed System

3.1 Image Filter

The framework of the project is to enforce the owner's image. In the proposed method the first stage to filter the image. Since there is a security concern with the third party provider or the cloud service provider. The images are filtered by the image owner as a result the images are blurred using filtering technique for prevention of image data from being lost as shown in fig 2.



Original image (a) (b) filtered image

Fig 2 Image filter

3.2 Image Encryption

Image encryption methods try to transform one image into another that is difficult to read in order to keep an image secret between users, or to put it another way, it is essential that no one could learn the content without a key for decryption.

Image Encryption Algorithm

Image Owner

• The secret keys are produced by the key generation algorithm using the security settings.

• The image encryption algorithm receives as inputs the identity set ID, the block size Bblksize, the image database I, the secret keys K, and the encrypted image database.

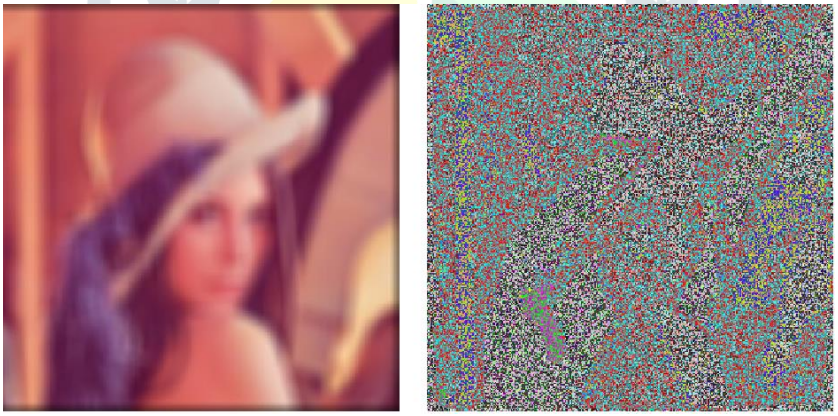
• The query image, the block size, and the secret keys K are all inputs to the trapdoor generating process, which outputs the trapdoor.

• The comparable encrypted picture set, the block size Bblksize, and the secret keys K are all inputs to the image decryption algorithm, which outputs the decrypted image set.

Cloud Server

•The encrypted image database C and the block size Bblksize are the two inputs used by the algorithm that creates the index.

• The search algorithm retrieves encrypted similar images by using the encrypted database C, the index, the trapdoor, and the block size Bblksize as inputs.



(a) Query Image (b) encrypted image

Fig 3 Image Encryption

3.2 Search Operation

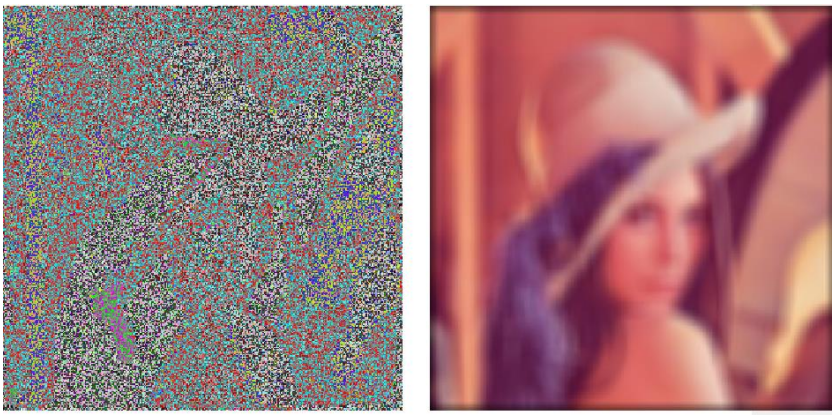
Manhattan measures the degree of similarity between the query feature vector and the feature vector of an image from the dataset.

$$d(q,f) = \sum_{i}^{k} |q_i - f_i|$$

where q and f stand for the feature vector of the dataset picture and the query image, respectively. The search results are then limited to the pictures that are closest to each other.

3.2 Image Decryption

After getting encrypted photos, the owner must decode these files. The process of decryption is very different from that of encryption.



(c) encrypted image (d) decrypted image

Fig 3 Image decryption

IV. Security Analysis

In this section, we will examine the security of our proposed scheme. The original photos are filtered using a common filtering technique to ensure the security of the data stored on the cloud server. The typical encryption mechanism used to encrypt these filtered photos in our system is semantically secure. The cloud server shouldn't be able to deduce the original image data as long as the secret key is maintained a secret. As a result, the privacy of the original photos is appropriately preserved. Sicne the proposed system focus on double protection. There is a chances durimg communication between the cloud server and the users, the cloud server may generate an access pattern and a search pattern. While search pattern clearly provides information defining which queries have similar picture attributes, access pattern explicitly includes the search results corresponding to the query trapdoors but a search pattern will explicitly state which queries include similar image features. As a result, our scheme should ensure that no information other than the access pattern and the search pattern is leaked to the attackers. Since our proposed model uses double protection if there is chances of data leakage only the encrypted images can be leaked since imaged are blurred attacker cannot understand the blurred data.

4.1 Security of Image Feature

In the proposed work, in first stage the orginal image is blurred using filtering technique hence the feature cannot be extracted by the service provider fig shows the Histogram of original image and filtered image. Next stage these query images are encrypted using a efficient encryption algorithm these images are stored in the vloud database. the cloud server's capacity to decrypt photos using the appropriate secret key and extract features for image search is restricted. In other words, the cloud server cannot provide helpful features without owner-encrypted images.

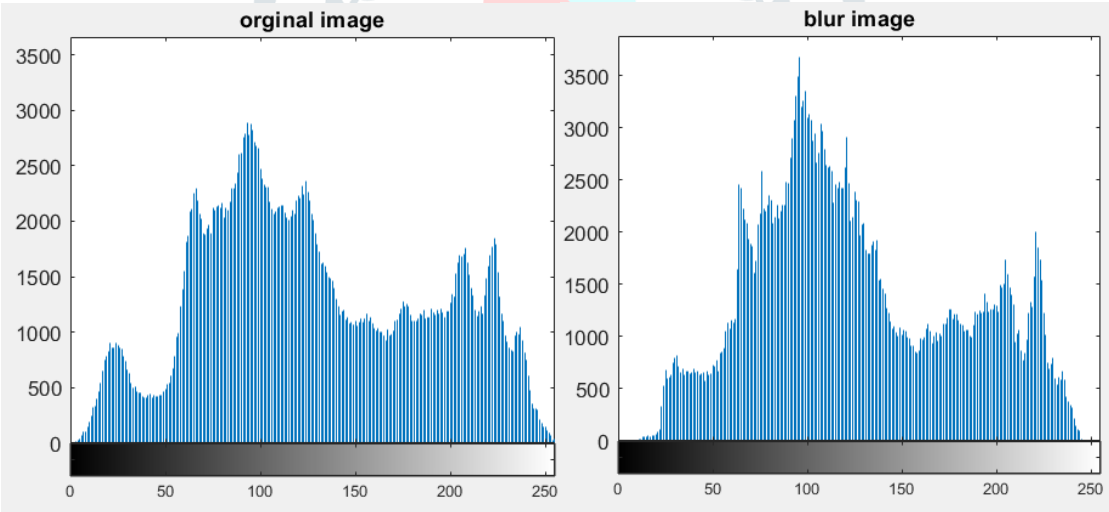


Fig 5 Histogram of orginal image and blur image

V. EXPERIMENTAL RESULTS

The effectiveness of the suggested system is evaluated in this section. This project is done in Matlab 2022a is used to create a prototype system that runs on a Windows 10 machine with an Intel Core i5 and 6 GB of RAM. Here, the experimental database is the Inria Holidays database.

5.1 Effectiveness of Encryption

The proposed approach encrypts images using encryption technique that can offer excellent security. A nature image's content is disturbed, as seen in Figure 3.The encrypted image will not reveal any shape information, as the image content is blurred, as seen in Figure 3. The encryption can effectively safeguard the images

5.2 Retrieval Accuracy

The results of the studies indicate that the suggested approach is successfully to retrieve similar photos. As illustrated in the Fig 6. The histogram of the orginalBlurred image and encryptedBlurred images and decrypted Blurred. This shows that decryptedBlurred and orginalBlurred shows the Same frequency, hence the retrieval rate is high compared to the other existing model

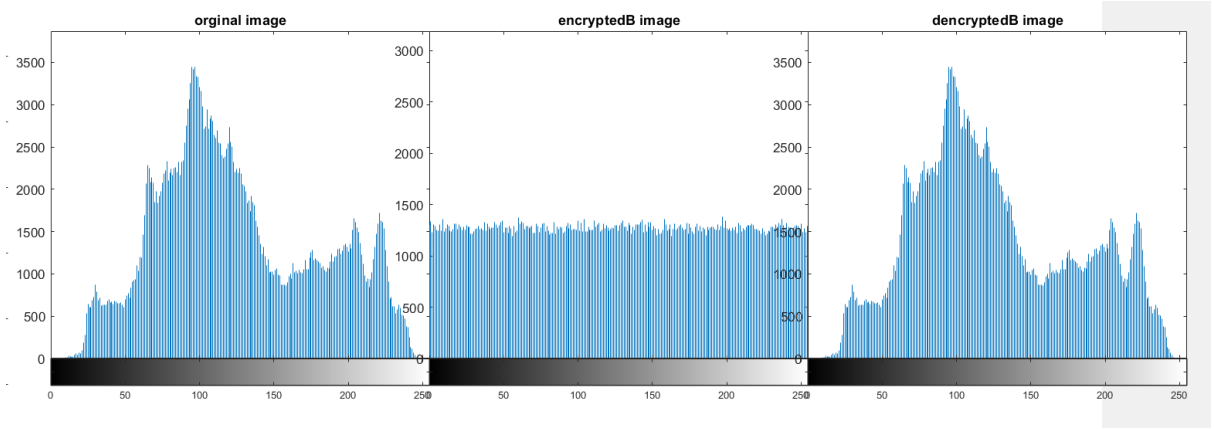


Fig 6 Histogram of the orginalB image and encryptedB images and decryptedB

VI CONCLUSION

This paper proposed a privacy-preserving content-based image retrieval method in this research that enables the data owner to outsource the images to an untrustworthy cloud without disclosing the privacy of the images. the proposed model use double protection to To increase security. First stage the images are filtered using filtered technique. In the secong stage the filtered images are encrypted with the efficient encryption algorithm. These encrypted images are saved in the database. After receiving the encrypted image database, the cloud server builds the index using an index building technique. the accuracy of the retrieval image and that proves the frequency are similar. Hence the proposed method can be more secured when compared to existing methods. In Future the encryption algorithm can extract more accurate local characteristics from the images. And better filtering techniques can be used to preserve the features of the image data.

REFERENCES

[1] J. Ahmad, K. Muhammad, S. Bakshi, and S. W. Baik, "Object-oriented convolutional features for fine-grained image retrieval in large surveillance datasets," Future Generation Computer Systems, vol. 81, pp. 314-330, 2018.
[2] J. Ahmad, M. Sajjad, I. Mehmood, and S. W. Baik, "SiNC: Saliency-injected neural codes for representation and efficient retrieval of medical radiographs," PloS one, vol. 12, p. e0181707, 2017.
[3] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," Computer vision and image understanding, vol. 110, pp. 346-359, 2008
[4] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, "Verifiable private multi-party computation: ranging and ranking," in INFOCOM, 2013 Proceedings IEEE, 2013, pp. 605-609.
[5] Wang, J., Liu, W., Kumar, S., & Chang, S. F. (2015). Learning to hash for indexing big data—A survey. Proceedings of the IEEE, 104(1), 34-57.
[6] Gionis, A., Indyk, P., & Motwani, R. (1999, September). Similarity search in high dimensions via hashing. In Vldb (Vol. 99, No. 6, pp. 518-529).
[7] Datar, M., Immorlica, N., Indyk, P., & Mirrokni, V. S. (2004, June). Locality-sensitive hashing scheme based on p-stable distributions. In Proceedings of the twentieth annual symposium on Computational geometry (pp. 253-262).
[8] Yu, X., Zhang, S., Liu, B., Zhong, L., & Metaxas, D. (2013). Large scale medical image search via unsupervised PCA hashing. In Proceedings of the IEEE conference on computer vision and pattern recognition workshops (pp. 393-398).
[9] Song, D. X., Wagner, D., & Perrig, A. (2000, May). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE symposium on security and privacy. S&P 2000 (pp. 44-55). IEEE.
[10] Fu, Z., Sun, X., Liu, Q., Zhou, L., & Shu, J. (2015). Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Transactions on Communications, 98(1), 190-200.
[11] Wang, C., Ren, K., Yu, S., & Urs, K. M. R. (2012, March). Achieving usable and privacy-assured similarity search over outsourced cloud data. In 2012 Proceedings IEEE INFOCOM (pp. 451-459). IEEE.
[12] Xia, Z., Wang, X., Sun, X., & Wang, Q. (2015). A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE transactions on parallel and distributed systems, 27(2), 340-352.
[13] Shashank, J., Kowshik, P., Srinathan, K., & Jawahar, C. V. (2008, June). Private content based image retrieval. In 2008 IEEE Conference on Computer Vision and Pattern Recognition (pp. 1-8). IEEE.
[14] Qin, Z., Yan, J., Ren, K., Chen, C. W., & Wang, C. (2014, November). Towards efficient privacy-preserving image feature extraction in cloud computing. In Proceedings of the 22nd ACM international conference on multimedia (pp. 497-506).
[15] Wang, Q., Wang, J., Hu, S., Zou, Q., & Ren, K. (2016, May). SecHOG: Privacy-preserving outsourcing computation of histogram of oriented gradients in the cloud. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (pp. 257-268).
[16] Lu, W., Varna, A. L., Swaminathan, A., & Wu, M. (2009, April). Secure image retrieval through feature protection. In 2009 IEEE International Conference on Acoustics, Speech and Signal Processing (pp. 1533-1536). IEEE.
[17] Hsu, C. Y., Lu, C. S., & Pei, S. C. (2009, October). Secure and robust SIFT. In Proceedings of the 17th ACM international conference on Multimedia (pp. 637-640).
[18] Ferreira, B., Rodrigues, J., Leitão, J., & Domingos, H. (2015). Towards an image encryption scheme with content-based image retrieval properties. In Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance: 9th International

Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014. Revised Selected Papers (pp. 311-318). Springer International Publishing.
[19] Cheng, H., Zhang, X., Yu, J., & Li, F. (2016). Markov process-based retrieval for encrypted JPEG images. EURASIP Journal on Information Security, 2016, 1-9.
[20] Gu, B., Sheng, V. S., Tay, K. Y., Romano, W., & Li, S. (2014). Incremental support vector learning for ordinal regression. IEEE Transactions on Neural networks and learning systems, 26(7), 1403-1416.