Review on encryption of images onto cloud

Komal Pratap Ghorpade[1], Dr.G.A.Patil[2]
[1,2]DYPCET, Kolhapur Maharashtra, India

***Abstract*— Multimedia data, such as photographs, are becoming increasingly significant in medical, education, advertising, entertainment, and other media industries due to the expeditious development of imaging sensors and mobile electronic devices. Outsourcing images to the public cloud can bringup worries about privacy. To make image searches work wellin real-life situations, we must find ways to make the search faster and more efficient. To solve these issues, there is a need to create a system that can update index keys in real-time, handle multiple owners and offer verification support. Our solution is to provide an encrypted image retrieval-based system. This system will not only let users easily and accurately find similar images, but it will also keep the image owner's and user's privacy safe from the cloud server.**

Keywords*— Fuzzy logic, Artificial Neural Network, Convolutional Neural Network, Fog Computing, Cardio-diabetic Diseases.

I. INTRODUCTION

There is an urgent need for more storage capacity than before due to the rapid expansion of digital image applications. Because of digital image applications popularity and ability to manage enormous amounts of data compared to hardware upgrades and infrastructure reorganization, cost is significantly cheaper. Currently, image related data is increasing essentially in numerous applications, including the identification of faces, detection of diseases and recognition of objects where II.typically requires more than text related data storage. Cloud services reduce the storage burden on local hardware by shifting enormous picture libraries to the cloud server, as well as employ the cloud's computing capacity for image processing applications. Images must be protected before they are sent to the cloud to protectthe sensitive data contained inside them. Storing images on the cloud in encrypted form is crucial to safeguard sensitive data and maintain privacy. Encryption ensures that only authorized users with the decryption key can access and view the images, protecting against unauthorized access and potential data breaches. It helps organizations comply with data protection regulations and industry standards, mitigating legal and reputational risks.By encrypting images, businesses can confidently leverage cloud storage without compromising the securityand confidentiality of their valuable visual assets. Users will query the cloud server for the encrypted image data after putting it in the target picture and will search the image. Nevertheless, most of the time, Content-Based Image Retrieval (CBIR) solutions are ineffective. Consequently, this study attempts to find a solution to the issue of searching encrypted image data. Cloud service providers make unstructured data hosting simple and economical. Cloud services, on second thought, are third-party solutions that do not provide consumers with access to or control over their data. This has exacerbated security and privacy concerns for many businesses (users) who rely on cloud-based solutions to store sensitive data. User-side encryption may be able to alleviate these concerns by focusing on the user and providing the user authority over their data. User-side encryption, on the other hand, limits how Cloud-encrypted data can be accessed. processed (for example, searched). To provide real-time, user-centered search capabilities, our system employs the locality feature via edge computing.

II.DIFFERENT TECHNIQUES USED FOR ENCRYPTION OF IMAGES ONTO CLOUD

Because of the expeditious expansion of cloud services and the demand for individual privacy, Secure cloud storage and search over encoded datasets have risen in popularity.Images of identity cards and driver's licenses that have lately surfaced have sparked widespread interest. As part of the push towards secure computation, Homomorphic Encryption (HE) and Asymmetric-

Scalar-Product- Preserving Encryption (ASPE) [1] have attracted a lot of attention. Although ASPE may effectively encrypt and compare ciphertexts, it is not a viable technology due to its reliance on the notion that users can be entirely trusted in the real world and potential key leakage difficulties. Unlike ASPE, HE can perform addition and multiplication in the encrypted domain and overcome the key leaking issue. J. -S. Li etal [1]. have developed a novel with a confidentiality content-based image retrieval approach that includes a critical confidentiality component to defend against assaults from data owners, servers in the cloud, and users. A sophisticated and realistic threat framework was usedto construct the privacy-preserving picture retrieval approach. The system protects both the private nature of the search information as well as the security of the keyto the encryption at the same time. A rapid verification mechanism to confirm the system's reliability or correctness should also be provided. It is the initial publication of its type to examine these issues in this context.

In cloud computing, encrypted image retrieval is a vital technology for realizing huge pics of preservation, management, and image safety [2]. The research done by J. Qin et al proposes a novel extraction of features technique for accessing encrypted pictures. The revised Harris approach is used to get the image features initially. The concept of the Bag of Words framework and itsSpeeded-Up Robust Features technique are then applied to each image to generate feature vectors. The Local Sensitivity Hash method is then used to the feature vectors to generate a searchable index. The chaos encryption algorithm safeguards images and indexes. Thecloud server will then conduct a secure similarity search. The experimental results show that, when compared to existing encrypted retrieval systems like Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Blowfish. Their proposed retrieval scheme not only uses less time but an efficient index generation ability to encrypt images.

Because of the constant requirement to protect data privacy, secrecy, and integrity, Content-Based Image Retrieval (CBIR) [3] on encrypted domains has become highly crucial with the introduction of the cloud. CBIR on outsourced encrypted images can be accomplished by extraction characteristics from uncompressed photos and creating an accessible encrypted database based on those attributes. In similarity searches, visual descriptors such as color, form, and texture descriptors are used. An attempt was made in this work to incorporate visual descriptions because they are significant in obtaining the most similar findings. The impact of combining different visual descriptors on retrieval precision is investigated by J. Anju and R. Shreelekshmi [3] safe CBIR system. According to experimental data, combining visual descriptors can significantly improve the system performance.

D. X. Song et al [6]. have presented security proofs for the associated cryptographic systems and outlined cryptographic solutions to the challenge of finding data that was encrypted.it has methods that provide numerous major advantages. The techniques they present in this research offered strong security features. These include keeping searches isolated, so the server cannot learn more about the data thannecessary, ensuring encryption secrecy, and controlling searches to prevent unauthorized access. The algorithms used for encryption and search are efficient, making them simple to understand, easy to implement, and practical forimmediate use. Content-Based Image Retrieval (CBIR) research has become significant due to the increasing importance of images in our daily lives.

CBIR technologies in the plaintext domain are rendered ineffective. L. Zhang et al. have proposed a method for implementing Content-Based Image Retrieval (CBIR) [7] over encrypted pictures without providing a private data to the cloud server.

Feature vectors are initially extracted to represent the associated photographs. To improve search efficiency, pre-filter tables are generated using locality-sensitive hashing. Furthermore, the feature vectors are encrypted using a conventional stream cipher, and the image pixels are safeguarded by the secret K-Near Neural based Network (KNN) approach. They also recommend using a watermark to prevent such unauthorized distributions. Furthermore, Z. Xia, X. Wang et al [7] have proposed a watermark-based solution to preventing such unauthorized releases, considering the likelihood that permitted query users will illegally copy and distribute recovered photographs to others. In the watermark-based protocol, the cloud server directly places a distinguishing watermark on the encrypted images before transferring them to the query user. As a result, if an image copy is discovered, the watermark extraction can be used to track out the illegal query user who provided the image. The testing and security evaluations show that the technique presented by Z. Xia and X. Wang et al is efficient and secure which prevents unauthorized releases. Many image protection techniques have previously been proposed. Encryption is the most used method for securing photos.

In particular, the edge system delivers insightful forecasts. The multi-source big data search space is trimmed based on the user's search patterns to speed up the search process. The pruning algorithm efficiently samples the cloud-based clustered massive dataset. The pruning algorithm dynamically samples the proper number of phrases for each cluster based on the user's search patterns to ensure that it is optimally represented. C.-K. Chu et al. have developed and tested a user-centric [4] search system prototype using multiple datasets. According to the results of the experiments, both search accuracy and pruning quality have improved by 27%.

In the research by J. Li et al [5] developed a system to handle encrypted big data from multiple organizations (sources) without revealing it to the cloud service provider, especially during searching processes. Due to Searchable Symmetric Encryption (SSE), a private dataset can be transferred to a cloud server while still being searchable [5]. SSE techniques now in use improve search and safety performance in a variety of ways. However, nearly none of the SSE systems now in use take data dispersion into account. Researchers show that when a dataset is not distributed equally, standard search approaches suffer in terms of search quality. As a result, present SSE techniques cannot ensure high search quality when dealing with non-uniform datasets. Furthermore, the bulk of available SSE algorithms are incapable of concealing the query set's distribution.

Using a secret key and an encryption technique, the plain image is turned into an encrypted image in the method proposed by V. Himthani et al. The encrypted image appears chaotic, which is likely to attract the attention of the attacker. Sensitive information may be revealed if an image is recorded and stacked. In this regard, the VisuallyMeaningful Encrypted Image (VMEI) [8] technology, which encrypts the original image before disguising it in a reference image, is being developed. The encrypted image produced by the VMEI approach looks just like a conventional image. As a result, the VMEI methodology is more secure than existing picture encryption methods. The resulting encrypted image retains its natural appearance while providing enhanced security.

As more complicated architecture designs for DNN models are produced, the demand for cloud servers for training Deep Neural Network (DNN) models grows. Cloud servers are still viewed as reliable. Previous study presented the concept of learnable photo encryption, with an emphasis on medical diagnostic privacy issues using a DNN. Even though various ways for partially attacking previous encryption algorithms have been revealed, there is still room for advancement. Q. -X. Huang et al [9] presented an enhanced learnable image encryption method that may be used to train an outstanding DNN model while keeping the training images private. Having evaluated this method using publicly available medical datasets, and the results back it up. The suggested system investigates advanced perturbation techniques. The suggested system by Q. -X. Huang et al. Sun studies cutting-edge perturbation approaches based on unique chaotic maps. To address the shortcomings of current chaos-based confusion and diffusion designs, the author advocated perturbation-based data encryption be used in both rounds of confusion and diffusion.

The way this method works depends on two main things:

(i) the new mapping settings and chaotic sequences, and

(ii) the properties that control how pixels are shuffled andsubstituted. To see if the system behaves in a chaotic manner, various tools like the bifurcation diagram, Lyapunov exponents, and tests like NIST and DIEHARD

[10] are used. These tools help assess how the system

behaves and ensure its effectiveness. Furthermore, testingthe proposed cryptosystem on a range of test photos indicated that it is rapid, extremely efficient, robust in securing medical images, and well-documented. The goal of research presented by I. Yasser et al [10] was to offer a self-adaptive encryption system that protects quantum images while taking up little storage space.

A system proposed by R. Ismail Abdelfatah which has a newly constructed Pseudorandom Number Generator (PRNG) is utilized, which encrypts data twice using two separate pseudorandom number sequences. This PRNG is divided into two sections [11]. The first half is based on a recently devised chaotic-based concurrent keyless hashed operate, which in turn serves as the second half's controller. In the second section, the Tent of Chaos, and these chaos maps (TCM) are multiplied. Because of the significant rise in the number of control parameters and beginning values, the hash function and chaotic maps generate a scheme with a very large key space and high unpredictability of the hash function output.

III.LIMITATIONS

Encrypting images onto the cloud has several drawbacks. Firstly, it introduces increased processing overhead due to encryption and decryption operations, leading to longer upload and download times. Secondly, search complexity is amplified as the cloud server cannot directly process encrypted image features, making content-based image retrieval more challenging. Thirdly, proper management of encryption keys becomes crucial to avoid data loss andunauthorized access, posing a challenge in large-scale cloud environments. Fourthly, encrypted image search is limited in flexibility and functionality compared to plaintext searches, hindering complex queries and advanced filters. Additionally, encryption may interfere with image processing tasks like compression and optimization, impacting storage requirements. There is also a risk of security vulnerabilities and dependence on the strength of chosen encryption algorithms. Furthermore, encrypted images may still leak metadata, potentially revealing sensitive information. Lastly, securely distributing encryption keys when multiple usersor organizations require access to encrypted images can be complex. This paper primarily examines various approaches used to encrypt images on the cloud. It explores different methods, including Searchable Symmetric Encryption (SSE), Content-Based Image Retrieval (CBIR), Asymmetric Scalar-Product-Preserving Encryption (ASPE), and the Harris method. The study analyzes these techniques and draws conclusions based on their effectiveness in ensuring image security on the cloud.

Content-Based Image Retrieval required extra interaction between image owner and user. Content-BasedImage Many issues remain in retrieval, such as low searchaccuracy, low search efficiency, key leakage, and so on. Outsourcing photos directly to the public cloud invariably creates privacy concerns. Improving search performance is critical for supporting large-scale picture search in real-world applications.

IV.CONCLUSION

Multimedia data, such as photos, are becoming more and more essential in the fields of medicine, advertising, education, entertainment, and other industries. This is because Imaging sensors and mobile electronic gadgets are rapidly evolving. The main outsourcing options for picture storage and image search is cloud computing, which offers consumers on-demand, paid processing, and storage services. An important technique in cloud computing for huge image storage & management and image security is encrypted image retrieval.

We propose to provide a solution for implementing an encrypted picture recovery system that will not only help an image user to search for similar photos accurately and efficiently, but also safeguard the image owner's and image user's privacy from the cloud server.

REFERENCE

1. J. -S. Li, I. -H. Liu, C. -J. Tsai, Z. -Y. Su, C. -F. Li and C. -G. Liu, "Secure Content-Based Image Retrieval in the Cloud with Key Confidentiality," in IEEE Access, vol. 8, pp. 114940-114952, 2020, Doi: 10.1109/ACCESS.2020.3003928.
2. J. Qin et al., "An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing," in IEEE Access,

vol. 7, pp. 24626-24633, 2019, Doi: 10.1109/ACCESS.2019. 2894673..

3. J. Anju and R. Shreelekshmi, "Modified Feature Descriptors to enhance Secure Content-based ImageRetrieval in Cloud," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 2019, pp. 674-680, Doi: 10.1109/ICICICT46008.2019.8993195.
4. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R.
H. Deng, "Key aggregate cryptosystem for scalable data sharing in cloud storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 468– 477, 2014.
5. J. Li, R. Ma, and H. Guan, "Tees: An efficient searchscheme over encrypted data on mobile cloud," IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 126–139, 2017.
6. 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, pp. 44–55, IEEE, 2000
7. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp.2594–2608, 2016.
8. V. Himthani, V. S. Dhaka, M. Kaur, D. Singh, and H.-N. Lee, "Systematic Survey on Visually MeaningfulImage Encryption Techniques," in IEEE Access, vol.10, pp. 98360-98373, 2022, Doi:10.1109/ACCESS.2022.3203173.
9. Q. -X. Huang, W. L. Yap, M. -Y. Chiu and H. -M. Sun, "Privacy-Preserving Deep Learning with Learnable Image Encryption on Medical Images," inIEEE Access, vol. 10, pp. 66345-66355, 2022, Doi: 10.1109/ACCESS.2022.3185206.
10. I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra and F. Khalifa, "A Robust Chaos-Based Technique for Medical Image Encryption," in IEEE Access, vol.10, pp. 244-257, 2022, Doi: 10.1109/ACCESS.2021.3138718.
11. R. Ismail Abdelfatah, "Quantum Image Encryption Using a Self-Adaptive Hash Function-Controlled Chaotic Map (SAHF-CCM)," in IEEE Access, vol.10, pp. 107152-107169, 2022, Doi: 10.1109/ACCESS.2022.3212899.