RESEARCH PAPER

DEEP LEARNING-DRIVEN ENCRYPTED IMAGE RETRIEVAL WITH AUTHENTICATION IN CLOUD PLATFORMS

SK Mahaboob Basha[1*], **Pasham Aashritha**[1]

[1]Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Sciences, Sheriguda, Hyderabad, Telangana, India

[1]Professor (SK Mahaboob Basha) | Email: email2mahaboob@gmail.com

[1]Student (Pasham Aashritha) | Email: aashrithapasham.2354@gmail.com

***Corresponding Author:** SK Mahaboob Basha, Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Sciences, Sheriguda, Hyderabad, Telangana, India |

Email: email2mahaboob@gmail.com

***Abstract*—** This technique effectively and securely recovers encrypted images in the cloud while hiding the information in the image reversibly. In order to solve the privacy problem in CBIR, the image features are extracted by DL (VGG16) method, and the unprotected features indexes and searches are protected by homomorphic encryption, so that the cloud server cannot better infer the content of the unprotected features. Reversible Data Hiding designs authentication codes, and stores them in encrypted pictures; it allows verifying received results and detecting modifications. The training and testing are performed using the Flickr data and a comparative study is done between VGG16 and ResNet50 in which VGG16 achieves a better accuracy score of 98.3%. The retrieval approach will guarantee that similar query images will generate similar encrypted indexes which can be matched accurately and sensitive information may be protected. A caching technique has been employed to increase its computational efficiency and use of resources. This technique caches previously performed search results on the server, and loads them directly when they are searched again, hence no need for additional processing. From the performance investigation, it can be seen that the proposed encrypted search strategy and caching significantly reduces the calculation time as compared to the conventional use of KNN-based retrieval. In the context of outsourced picture search, a combination of DL, homomorphic encryption, reversible data concealing and caching offers a high precision of retrieval and a powerful security.

"Keywords*— *Content-based image retrieval,* *bitmap index, reversible data hiding, results verification."

How to cite this article: Basha SKM, Aashritha P. Deep learning-driven encrypted image retrieval with authentication in cloud platforms. Int J Drug Deliv Technol. 2026;16(75s): 434-441. DOI: 10.25258/ijddt.16.75s.49

I. INTRODUCTION

In today's digital age, photographs are an important type of data, as they are a strong tool for communication, analysis and decision making in various areas. They are extensively used in various applications including medical imaging, remote sensing, multimedia sharing, surveillance systems and other applications where they are used for conveying complex information far more than just text [1, 2]. The fast growth of the photography technology and the extensive usage of internet-enabled gadgets also contribute to the quick increase of the production of digital images . This quick growth poses serious problems for phone and personal PCs, which may not have sufficient memory and storage capacities to deal with massive databases of photos. Hence, cloud computing has proven to be an effective way to outsource and store a largenumber of images, and the users can outsource storing and processing the images to the cloud servers [4].

CBIR has become a major means of an efficient recovery of images, within the framework of this cloud-based framework, but which depends on the intrinsic qualities of the photos content. The CBIR approach differs from the conventional retrieval approaches based on text. Therefore, it is especially useful in situations where there are no text annotations or they are not enough [5]. Commonalities in images, based on colour, shape and texture, are retrieved by CBIR systems. The colour descriptors also contain global and/or local chroma information, which are used in distinguishing different kinds of images visually [6]. In a similar way, form descriptors are used to store the geometric characteristics and outlines of objects on which to retrieve photos with similar structures [7]. The texture attributes are employed to measure the spatial relation of pixel values to distinguish images on the grounds of the granularity of the visual surface and the storage on it [8]. The complementary properties enable CBIR to be more precise and efficient in picture retrieval for a variety of applications.

II. RELATED WORK

For the sake of accuracy, security and privacy of the cloud systems, many ways have already been proposed by scholars in a setting of CBIR. Gurubelli, Ramanathan and Ponnusamy [9] used a modified local zigzag pattern for the development of colour texture content based image retrieval of diseased tomato leaves photographs. They were able to add the information of colour and texture and got very high retrieval rate for identifying agricultural diseases with sometimes improved performance in the CBIR system as compared with the traditional CBIR systems. This research has emphasised the relevance of feature extraction methods that are adapted to the specific application.

Baranda and Anita [10] have done a detailed review of the obstacles that are associated to a data breach in cloud computing. Unauthorized access, insider threat, and sensitive information leakage were identified as key issues in their analysis. While encryption is often used to thwart such perils, it is not sufficient on its own if it is to have any real effect, it must be accompanied by methods of safe access, retrieval and verification. Their study shed light on the importance of privacy-sensitive algorithms in the cloud environment and provided insight into important issues related to the need for secure CBIR systems when sharing privacy-sensitive photographs with potentially untrusted servers.

To solve the challenge of unsecured cloud environment Kumar [11] proposed secure and efficient picture retrieval model with fixed feature selection. His approach has focused on the search for properties that are rotational, scaling and translationally invariant, and on the retrieval despite geometric modifications of images. This has the benefit of incorporating invariant properties, along with techniques for rapid access, making the technology suitable for large-scale applications, while enhancing its strength and lowering the computational cost. The experiment demonstrated that the use of invariant descriptors increased their retrieval accuracy and also increased the security of CBIR systems.

To preserve privacy in cloud computing applications, [12] proposed a DL based content-based image retrieval system to preserve privacy. The technique used a privacy preserving deep neural network to extract highly discriminative features, as opposed to the typical handwritten descriptions. The approach demonstrated an ability to preserve anonymity while effectively retrieving the data, indicating the potential for combining AI with secure computation. The findings of this study showed that DL is a technique that seems to have the potential to be used for CBIR, especially in the application of cloud system usage which has privacy concerns.

Xia [13] introduced a novel and effective privacy protecting content based image retrieval system in cloud computing named as EPCBIR. The proposed approach was able to retrieve similarities from an encrypted picture database by both efficient retrieval and encryption. In the practical usage of PABIR in the real cloud context, EPCBIR is able to effectively mediate the accuracy constraint of the PABIR task with the computational complexity, demonstrating its success in balancing the two without compromising their performance. This contribution was an important step, in showing that secure CBIR can be done without unencrypted data, and hence without user privacy being lost.

Li et al. [14] presented a privacy-preserving image categorisation system for mapping encrypted images, called CryptoEyes. Traditional CBIR methods are mostly focused on retrieval. CryptoEyes has extended the methods of privacy-preserving to include classification operations which allow safe operations on encrypted data. CryptoEyes employed cryptographic methods like as homomorphic encryption, which helped with more advanced calculations, and maintained the data hidden. This method extended the scope of privacy-preserving methods to show how encrypted data can be used for more than just retrieval; it can also be used for high-level classification and decision making.

Li, Ma, Miao, Liu, Liu and Choo [15] proposed a secure and verifiable multi-key picture search scheme based on cloud assisted edge computing. This approach enabled multiple users to upload their encrypted images using different keys and still have extremely fast way to retrieve images. The system also had verifiability which allowed the users to verify the correctness of search results returned by the cloud. The issue of trust in this cloud environment, where users need to be convinced of the validity and authenticity of the search results was addressed with the introduction of authenticated search. The project resulted in the creation of secure CBIR concentrating on the context of more than one user and emphasising on privacy as well as accuracy.

Guo, Xu, Zhang, Xu and Xiang [16] designed a system called ImageProof to combat authentication in a large image search. Unlike many of the previous investigations on privacy and the accuracy of retrieval results, ImageProof addressed the issue of the authenticity of retrieval results. The approach used cryptographic proof to verify that the recovered photos are not corrupted and they relate to the outsourced data. This innovation tackled the trust problem in big cloud retrieval systems by providing the user the chance to verify the integrity and validity of the results.

III. Materials And Methods

The proposed approach offers the secure and verifiable encrypted image retrieval in a cloud-based system by adopting the existing DL and cryptography technologies. The DL method VGG16 is used to extract the picture attributes for Intense picture Retrieval (CBIR). Homomorphic encryption is employed to guarantee these properties, to preserve privacy by prohibiting the cloud server to get the content of the image based on unencrypted feature indexes or queries. The authentication codes are embedded in encrypted images by means of Reversable Data Hiding, which allows easy verification of the information found, and also allows detection of any unauthorised changes. The features are extracted and models are trained and compared on the performance of ResNet50 on the Flickr dataset. The retrieval approach creates suitable encrypted indexes of visually similar query photos to provide accurate retrieval without revealing the data. Then there is a caching approach on the server side that saves the results of the search performed previously, thus the next time the search is run, the answer can be retrieved immediately, avoiding unnecessary computations and optimising the performance of the processing.

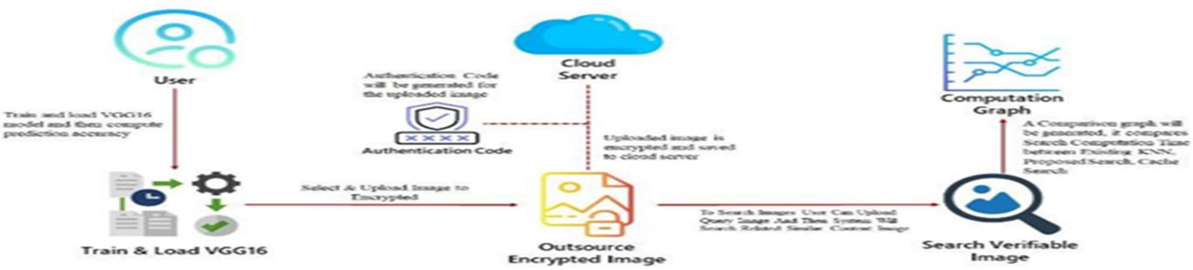


Fig. 1. System Architecture

The overall system architecture is presented in Fig.1, which is an efficient and secure picture retrieval system based on VGG16 and encryption algorithms. The first step of the user is to train and load the VGG16 model to enhance the accuracy of image classification. Then the image is encrypted and sent to one of the cloud servers which generates the access authentication code. The picture uploaded is securely stored in the cloud and can be quickly located by encrypted phrases. A computation graph is used to do comparison and search operations such as CNN, KNN and secure circle search to get verified and correct images.

A) Modules:

New User Sign Up: This module helps in registering new users on the cloud server by supplying all the required credentials. It safely keeps the user information in the database, which is the basis for authenticated access to perform various operations such as picture encryption, storage, retrieval and verification in the safe image retrieval system.

User Login: This module will be used to allow the authentication of registered users by checking their information with the records stored in the database. Once the authentication object is successful, all the system's capabilities are granted, ensuring that only authorized users can perform the necessary actions like training models, outsourcing encrypted photographs or performing security image retrieval operations.

Train & Load VGG16: This This module enables the user with authentication to train and load VGG16 model for feature extraction. It processes the images of the sample, identifies the percentage of correct predictions and trains the system to perform safely in CBIR (with privacy safeguarding measures).

Outsource Encrypted Image: Uploading photos to be outsourced to clouds as Outsource Encrypted Image module. Images will be coded and both authentication code and data will be securely saved in the cloud server which provides privacy, integrity and verifiability of data in the future retrival operations.

Search Verifiable Image: The module enables the users to upload a query image, the cloud offers the users with images similar to the query image with encrypted feature matching, and the authentication codes embedded in the images guarantee their legitimacy. This guarantees the secure and accurate Content-Based Image Retrieval and prevents information leakage.

Computation Graph: The module displays a graph for comparison of the computation time of the existing, proposed and caching based retrieval algorithms. It gives a final evaluation of the effectiveness of the system in decreasing delays in processing operations in secure image retrieval activities.

Logout: Also this module is used to safely end the current session at the end of work. It optimises the session management, helps to prevent unauthorised access and keeps the integrity of the existing processes in the secure encrypted photo retrieval system.

b) Algorithms:

VGG16: VGG16 is employed for deep feature extraction of images that results in high accuracy of CBIR. It has 16 layers of convolutional architecture which enables it to capture minute details of the visual information and generate strong feature vectors. The vectors are then encrypted to ensure privacy, and are encrypted as well for similarity matching reasons to efficiently and securely deliver the appropriate photos on the cloud without giving away important visual information to unauthorized access and analysis.

ResNet50: ResNet50 is used as a standard model to extract features to compare the retrieval performance of the model to VGG16. The residual learning framework can train the deep network without degradation, and can obtain the complicated visual data of images successfully. They are encrypted to allow for privacy sensitive searches, so that they can be searched securely, but on variances in performances of the different DL architecture in encrypted picture search scenarios.

c) Methods/Technologies:

Homomorphic Encryption: Homomorphic encryption makes it possible to execute the calculation on the encrypted data without the need to decode it, and maintains the privacy of data. The technology is utilised in picture feature indexes and to enable secure similarity matching in cloud . This approach helps ensure that the query image is hidden to others and that the image saved is still hidden to others, thereby not allowing cloud servers to steal or deduce other key images.

Reversible Data Hiding (RDH): Reversible Data Hiding: This technique is used to embed authentication codes or confidences into the images. It is now hard to get rid of the original photo and the hidden message without being able to recover both perfectly. In this approach, RDH can embed the authentication codes in the encrypted images, and then, verify the results during retrieval and detect whether the results are modified, thus ensuring data integrity and trustworthiness of the search results.

Deep Feature Extraction using VGG16: VGG16 A CNN to extract features from images, to match similarity in CBIR. It is a 16 layer model which represents fine visual details hence it generates high feature vectors. The features are then encrypted, making them difficult to decipher without the original image, but the associated images are able to be accurately retrieved from cloud storage without revealing the actual image.

Caching Mechanism: Caching Mechanism consists of caching of the results of search operations already computed in the server server, to avoid re-computation of the same search operations. When the system recognises a query to be a repeat query, it will fetch the results immediately from the cache, instead of rerunning the whole calculation. This significantly decreases the retrieval time, saves computer resources and additionally enhances the answer to repeated encrypted image search searches.

Content-Based Image Retrieval (CBIR): Content Based Image Retrieval is a search methodology of images, which leverages visual features, i.e. shape, texture, colour rather than textual metadata. The method was based on encrypted feature indexes generated by VGG16 to compare their similarity and recoveries of similar photos were visually similar images. The aspect of encryption besides keeping the right similarity recognition in cloud based retrieval systems, ensures privacy saving searches.

IV. Experimental Results

Accuracy: The ability of a test to successfully discern between patient and healthy cases. The accuracy of a test is determined by calculating the proportion of true positives and true negatives of all the instances that are evaluated. Mathematically this can be expressed as:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: Precision is defined as the proportion of instances retrieved that are relevant. The formula of calculation of precision based on this is defined as:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

Recall: Recall is a machine-learning model of the ability to identify all the instances for a particular class. The ratio of the number of correct estimates of excellent observations to the number of positive observations is information about the performance of a model in the recognition of instances of a certain category.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP}\ +\ \mathrm{FN}} (3)$$

F1-Score: F1 score is used to calculate the accuracy of a ML model. It combines a model correctness with a model remembrance. This accuracy metric, quantifies the proportion of the times that the model makes a correct prediction on the whole data.

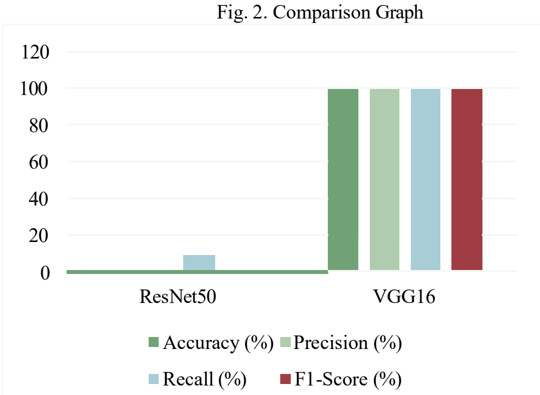
$$F1\ Score = 2 * \frac{Recall\ \mathrm{X}\ Precision}{Recall + Precision} * 100 (1)$$

Table 1. The accuracy, precision, recall and f1-score of Resnet50 and VGG16. The results show that VGG16 is significantly better than ResNet50 on all the metrics and ensures the effectiveness of retrieval.

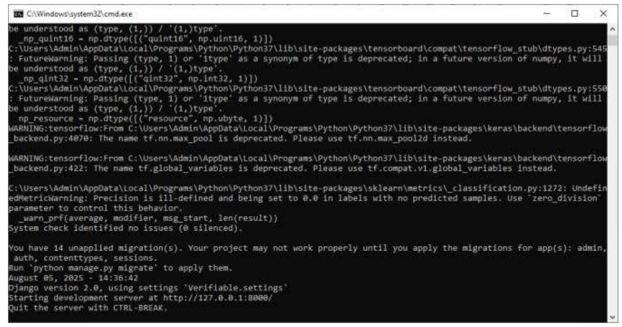
Table. 1. Performance Evaluation

Algorithm Name	Accuracy	Precision	Recall	F1-Score
ResNet50	7.22	0.72	10.00	1.35
VGG16	98.33	98.18	97.91	98.02

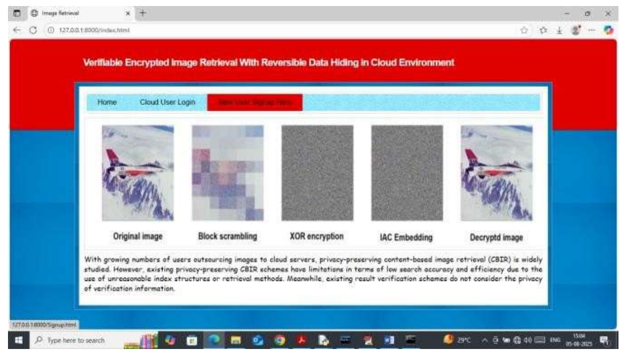
Fig. 2. Comparison Graph



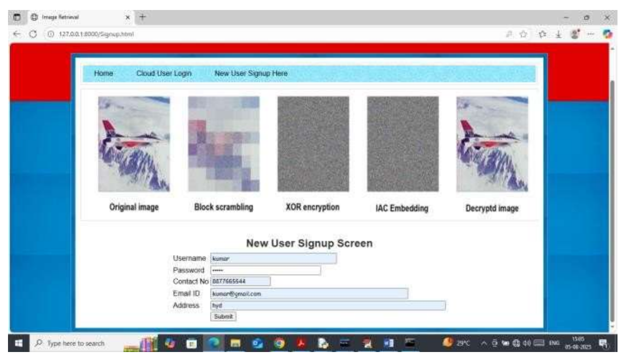
The graph (2) represents the accuracy of dark green, precision of light green, recall of blue and F1-score of red of the VGG16 and ResNet50 models. VGG16 is superior to ResNet50 in all the assessment measures.



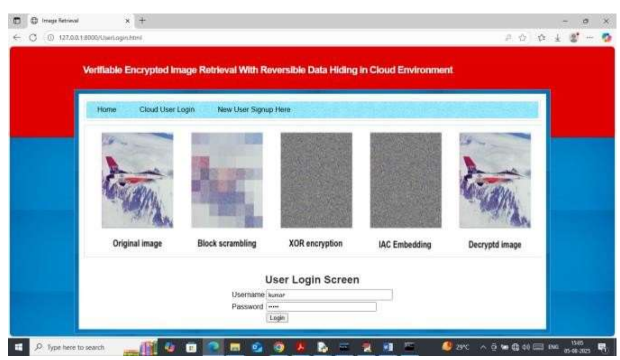
Run the Python server and then open a browser and enter the URL and then enter the URL as 127.0.0.1:8000/index.html and press the enter key to view the next page.



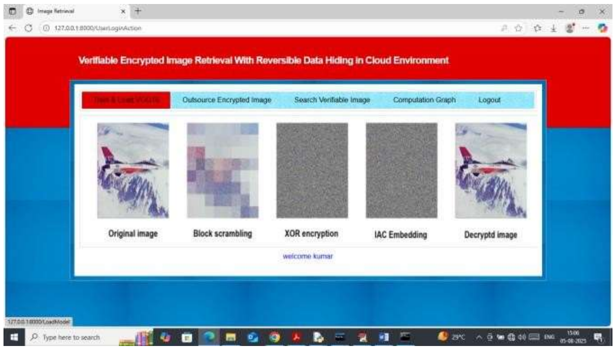
Click on the New User Sign Up option on the above screen to move to the next page (which is the sign up screen).



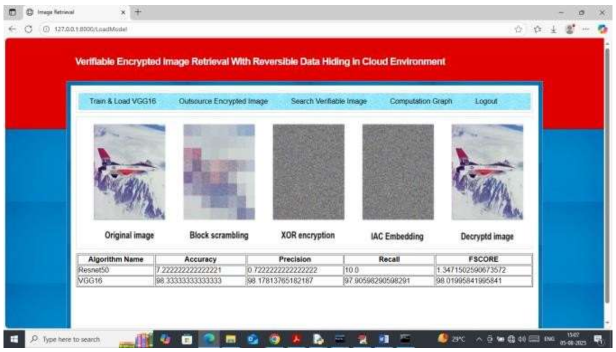
Once a user has signed up, he/she is expected to click on the user login link to navigate to the next page.



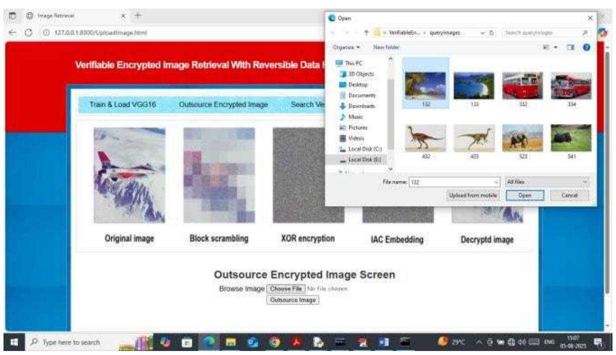
Once logged in one will be taken to the site above.



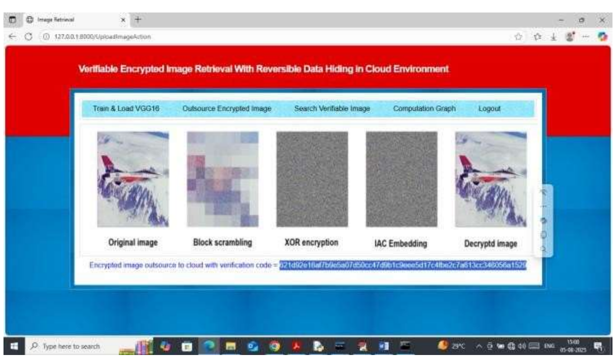
The above screen has a link Train and Load VGG16 which when clicked, will train and load the models, and the following screen will be displayed.



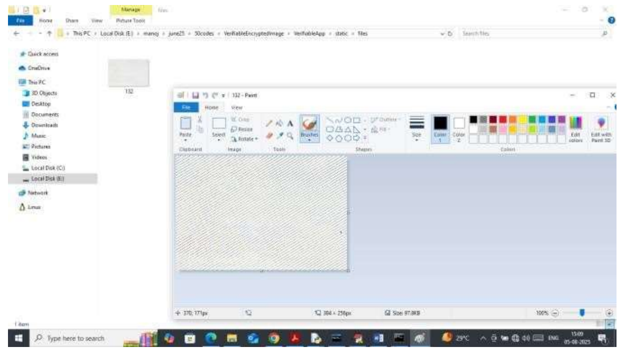
VGG16 has performed well in terms of accuracy (as seen in the above screen shot). Now click on Link of the Outsource Encrypted Image to the following page.



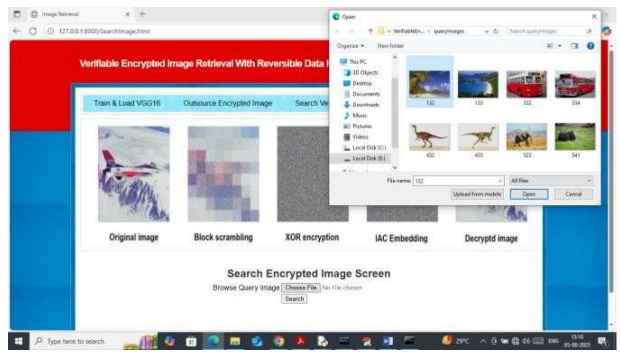
Choose and upload the sample photo on the top screen and click on the buttons button on the next page.



Data will be encrypted and stored in cloud, as shown in the above screen capture, using the blue authentication code above. Photos can be uploaded to the cloud server memory as many as you like and once they are uploaded to the cloud server memory, the encrypted photo will be saved in the VerifiableApp/static/files/ folder.

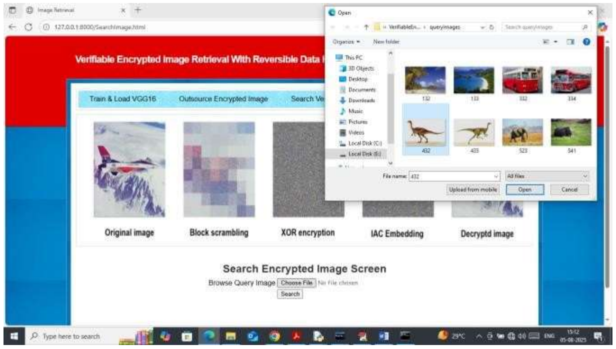


The encrypted photo is displayed on the upper screen. Now, click on the verifiable image search link, so that you will be taken to the next screen.

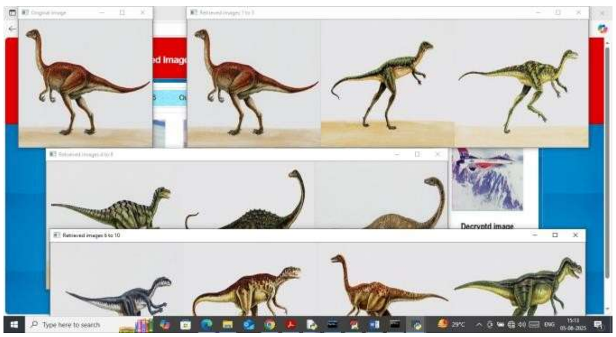


In the above mentioned interface one can upload a query image on which the system will get similar images; which are the output of the results shown below.

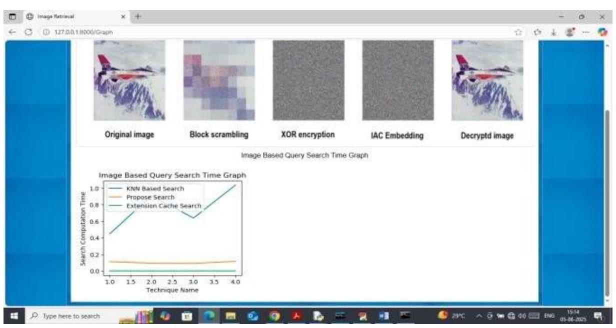
The first image on the screen is the initial query image and the rest of the images are the same content based images on the cloud. Similarly you can make a review of a bunch of images, here is another example:



The screen above is uploading another image and below are results of similar searches.



The first image is the query image; the rest of the images are similar images stored on cloud. Click on the link Computation Graph below to get the graph below.



The graph x-axis shows the number of query image searches and y-axis shows the computation time. The blue curve shows the current KNN based search, the yellow curve represents the proposed search time and the green curve represents the extended cache search time. The chart showed the time of the computation of a search points to prove that the suggested extension took lesser time.

V. Conclusion

The suggested method efficiently achieves the secure and verifiable access to encrypted photos in a cloud based platform with the help of DL, cryptographic approaches and optimisation algorithms. First, using the DL method, VGG16, the features of the image will be identified and the features will be encrypted by homomorphic encryption, then the cloud server can not be able to infer the content of the image by using the features which has not been encrypted and the query and the feature index. Reversible Data Hiding is also used to place authentication codes inside the encrypted images, for the verification of recovered images and the identification of any manipulation. The retrieval system ensures that the same query image yields the same encrypted image index for accurate CBIR without loss of data, if the two images are similar. VGG16 can be considered as a more accurate network than ResNet50 with a 98.3 per cent accuracy in the recognition of related images. The adoption of a caching technique can greatly reduce the computation time by saving and reusing the search results previously calculated, in order to avoid redundant calculations for repeated queries. Securing outsourced image retrieval in the cloud using VGG16 feature extraction, homomorphic encryption, reversible data hiding and caching is an extremely accurate, privacy-preserving and efficient approach.

We hope to use this technique on a larger and more varied set of data, not just those from Flickr, in the future to make it more generalisable. Advanced DL architectures like EfficientNet or Vision Transformers can be employed to obtain more powerful features. Advanced data security and integrity measures, such as hybrid encryption processes and blockchain verification, may be used to improve data security and privacy. Smart query prediction and smart store management can be used to optimise the caching mechanism to gain better performance. Furthermore, real-time image retrieval in edge-cloud and distributed systems with encrypted images support can be provided to enhance the practicality.

References

[1] Zhang, W., Wang, H., Hou, D., & Yu, N. (2016). Reversible data hiding in encrypted images by reversible image transformation. IEEE Transactions on multimedia, 18(8), 1469-1479.

[2] Hou, Z., Yan, H., Zhang, L., Ma, R., Yan, Q., & Yang, B. (2025). A Secure and Efficient Remote Sensing Image Retrieval Method With Verifiable and Traceable in Cloud Environment. IEEE Transactions on Geoscience and Remote Sensing.

[3] Kong, Y. J., Zhang, M. Q., Jiang, C., Zhang, X., Huang, S. Y., Di, F. Q., & Ren, T. L. (2024, January). A Hierarchical Manageability Reversible Data Hiding Based on the Encrytion Process of Shamir's Secret Sharing. In 2024 4th International Conference on Consumer Electronics and Computer Engineering (ICCECE) (pp. 248-254). IEEE.

[4] Shi, Y. Q., Li, X., Zhang, X., Wu, H. T., & Ma, B. (2016). Reversible data hiding: Advances in the past two decades. IEEE access, 4, 3210-3237.

[5] Qian, Z., & Zhang, X. (2015). Reversible data hiding in encrypted images with distributed source encoding. IEEE Transactions on Circuits and Systems for Video Technology, 26(4), 636-646.

[6] Keisham, N., & Neelima, A. (2022). Efficient content-based image retrieval using deep search and rescue algorithm. Soft Computing, 26(4), 1597–1616. https://doi.org/10.1007/s00500-021-06418-7

[7] Salih, S. F., & Abdulla, A. A. (2023). An effective bi-layer content-based image retrieval technique. The Journal of Supercomputing, 79(2), 2308–2331. https://doi.org/10.1007/s11227-022-04694-2

[8] Khan, U. A., & Javed, A. (2022). A hybrid CBIR system using novel local tetra angle patterns and color moment features. Journal of King Saud University - Computer and Information Sciences, 34(10), 7856–7873. https://doi.org/10.1016/j.jksuci.2021.08.009

[9] Gurubelli, Y., Ramanathan, M., & Ponnusamy, P. (2023). Colour texture descriptor for CBIR of diseased tomato leaf images using modified local zigzag pattern. Multimedia Tools and Applications, 82, 38077–38095. https://doi.org/10.1007/s11042-023-15348-y

[10] Barona, R., & Anita, E. A. M. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1–8). IEEE. https://doi.org/10.1109/ICCPCT.2017.8074251

[11] Kumar, S. (2023). Secure and efficient image retrieval through invariant features selection in insecure cloud environments. Neural

Computing and Applications, 35, 4855–4880. https://doi.org/10.1007/s00521-022-07891-2

[12] Ma, W. (2022). A privacy-preserving content-based image retrieval method based on deep learning in cloud computing. Expert Systems with Applications, 203, 117508. https://doi.org/10.1016/j.eswa.2022.117508

[13] Xia, Z. (2017). EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Information Sciences, 387, 195–204. https://doi.org/10.1016/j.ins.2016.09.013

[14] He, W., Li, S., Wang, W., Wei, M., & Qiu, B. (2021). CryptoEyes: Privacy preserving classification over encrypted images. In IEEE Conference on Computer Communications (INFOCOM) (pp. 1–10). IEEE. https://doi.org/10.1109/INFOCOM42981.2021.9488878

[15] Li, Y., Ma, J., Miao, Y., Liu, L., Liu, X., & Choo, K.-K. R. (2021). Secure and verifiable multikey image search in cloud-assisted edge computing. IEEE Transactions on Industrial Informatics, 17(8), 5348–5359. https://doi.org/10.1109/TII.2020.3028100

[16] Guo, S., Xu, J., Zhang, C., Xu, C., & Xiang, T. (2019). ImageProof: Enabling authentication for large-scale image retrieval. In 2019 IEEE 35th International Conference on Data Engineering (ICDE) (pp. 1070–1081). IEEE. https://doi.org/10.1109/ICDE.2019.00098

[17] Li, M., Jia, C., Du, R., Shao, W., & Ha, G. (2023). DSE-RB: A privacy-preserving dynamic searchable encryption framework on redactable blockchain. IEEE Transactions on Cloud Computing, 11(3), 2856–2872. https://doi.org/10.1109/TCC.2021.3074984

[18] Wong, W. K., et al. (2009). Secure kNN computation on encrypted databases. In Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data (pp. 139–152). ACM. https://doi.org/10.1145/1559845.1559860

[19] Li, Y., Ma, J., Miao, Y., Wang, Y., Liu, X., & Choo, K.-K. R. (2022). Similarity search for encrypted images in secure cloud computing. IEEE Transactions on Cloud Computing, 10(2), 1142–1155. https://doi.org/10.1109/TCC.2019.2925244

[20] Liu, H. (2022). Multi-user image retrieval with suppression of search pattern leakage. Information Sciences, 607, 1041–1060. https://doi.org/10.1016/j.ins.2022.06.062