

# **Two Months Internship Report**

*on*

## ***“JPEG Image Retrieval Scheme in Cloud Computing”***

*submitted by*

**Mr. Aditya Narsale**

*from*

**Department of Computer Engineering**

**Vishwakarma Institute of Technology (VIT)**

*under the*

*Supervision of*

**Dr. Kaushlendra Sharma**

**Assistant Professor**

**Department of Computer Science &  
Engineering**



**भारतीय सूचना प्रौद्योगिकी संस्थान, नागपुर**  
**Indian Institute of Information Technology, Nagpur**

*(An Institution of National Importance by an Act of Parliament)*

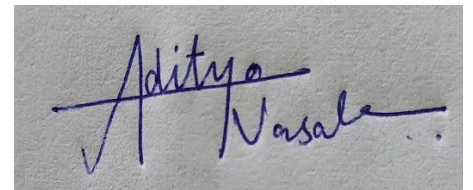
**Nagpur– 441108, India**

## DECLARATION

I, **Mr. Aditya Narsale** hereby declare that the Internship report entitled “**JPEG Image Retrieval Scheme in Cloud Computing**” is an original work conducted and prepared by me. This document is submitted in partial fulfillment of the requirements for the Internship Program at **Indian Institute of Information Technology**.

I affirm that this report is a result of my efforts and contributions. Any reference to existing research, direct quotations, or paraphrasing has been properly acknowledged.

I understand the importance of this declaration and hereby certify that the information presented in this report is true and accurate to the best of my knowledge and belief.



**Date: 27/09/2024**

**Name: Mr. Aditya Narsale**

**Place: Pune**

## **CERTIFICATE**

This is to certify that the **Mr. Aditya Narsale** student of **Vishwakarma Institute of Technology (VIT)** has completed his Two Months Internship and submitted Internship Report on the topic: “**JPEG Image Retrieval Scheme in Cloud Computing**” under my supervision during **8/7/2024 to 8/9/2024** in the **Department of Computer Science & Engineering at Indian Institute of Information Technology, Nagpur**

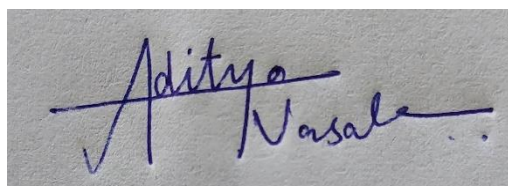
**Supervisor Name & Signature**

## ACKNOWLEDGEMENT

The two Internship opportunity I had with **Indian Institute of Information Technology, Nagpur** was a great chance for learning and professional development. I would like to express my deepest thanks and great sense gratitude towards **Dr. Kaushlendra Sharma** for his valuable guidance, time by help and constant encouragement during my internship of two months on the topic “**JPEG Image Retrieval Scheme in Cloud Computing.**”

I extend my heartfelt thanks to all members of IIIT, Nagpur for providing me resources essentials for carrying out this internship.

I perceive this opportunity as a big milestone in my career development. I will strive to use gained professional skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives.

A handwritten signature in blue ink on a light-colored background. The signature is written in a cursive style, with the first name 'Aditya' and the last name 'Narsale' clearly visible. There is a checkmark-like mark to the left of the first name.

**Name: Mr. Aditya Narsale**

## **ABSTRACT**

In the era of rapid digitalization, the volume of images stored on cloud platforms has grown significantly, raising concerns about privacy and security. To address these issues, this project proposes a Privacy-Preserving JPEG Image Retrieval Scheme that integrates Local Markov Features and the Bag-of-Words (BoW) Model. The primary goal is to enable secure, content-based image retrieval (CBIR) in a cloud environment, where images are encrypted to ensure privacy.

The scheme allows the cloud server to perform similarity-based image retrieval without decrypting the images, thereby maintaining data confidentiality. The process involves encrypting specific components of JPEG images, such as the VLI binary code, quantization table, and big-block permutation, while leaving essential structural elements accessible for feature extraction. The Local Markov Features are derived from encrypted DCT coefficients, capturing intra-block, inter-block, and inter-component dependencies. These features are then represented using a Bag-of-Words model, which facilitates efficient similarity search and image retrieval.

The project has successfully implemented the image search and retrieval functionality, achieving privacy-preserving results without compromising retrieval accuracy. Future work will focus on optimizing retrieval efficiency and enhancing the security framework to better balance privacy and performance.

## **LEARNING OBJECTIVE OF INTERNSHIP**

### Understanding Privacy-Preserving Techniques:

Gain in-depth knowledge of privacy-preserving mechanisms for secure image storage and retrieval, particularly focusing on how encryption can be applied without compromising usability in a cloud computing environment.

### Exploring Content-Based Image Retrieval (CBIR):

Study the principles of CBIR and how to implement efficient search techniques based on image content features such as colour, texture, and structure, even in encrypted images.

### Applying Feature Extraction & Machine Learning Models in Image Retrieval:

Learn to implement and modify feature extraction algorithms such as the Local Markov Feature Model to extract meaningful features from encrypted JPEG images, facilitating privacy-preserving image retrieval. Explore the integration of machine learning models, such as K-Means clustering and Bag-of-Words models, to facilitate feature clustering and efficient retrieval of images from large-scale encrypted datasets.

### Hands-On Experience with Cloud Computing Services:

Gain practical experience with Google Cloud technologies, such as Cloud Storage, Cloud Functions, and Vertex AI, to manage encrypted data and perform large-scale computations for image retrieval.

### Collaboration and Research Skills:

Strengthen research abilities by reviewing existing academic papers, collaborating with peers, and applying knowledge from various sources to develop a cutting-edge solution for image retrieval in the cloud.

### Real-World Application of Secure Image Retrieval:

Apply the theoretical knowledge gained to solve practical problems related to privacy-preserving image storage and retrieval in real-world cloud environments, preparing for future advancements in cloud security and data management.

## INDEX

<b>Sr.No.</b>	<b>Title</b>	<b>Page No.</b>
1.	Introduction	8
2.	Literature Survey	10
3.	Methodology	13
4.	Results and Discussion	19
5.	Conclusion	24
6.	References	25

## INTRODUCTION

With the exponential growth of digital images in today's world, vast amounts of visual data are generated daily by individuals, businesses, and organizations. This enormous collection of images has become increasingly difficult to manage, store, and retrieve efficiently. As a result, many users and companies are shifting towards cloud-based solutions, where massive image datasets can be stored remotely, saving local storage resources, and enabling seamless access from anywhere. However, this migration to cloud storage brings with it several critical challenges, primarily concerning the security and privacy of sensitive or personal images. The project has successfully implemented the image search and retrieval functionality, achieving privacy-preserving results without compromising retrieval accuracy. Future work will focus on optimizing retrieval efficiency and enhancing the security framework to better balance privacy and performance.

One of the key concerns surrounding cloud storage is the potential for security breaches. Images uploaded to cloud servers may be intercepted or accessed by unauthorized third parties, leading to unintended exposure. Furthermore, the cloud service provider itself, despite offering secure platforms, could also pose internal security risks. Employees with administrative access, or even external cyberattacks targeting the service provider, may result in image misuse or leakage. These risks make users hesitant to upload private or confidential images to the cloud, fearing that their visual data might be compromised.

In response to these privacy concerns, image owners are increasingly turning to encryption before uploading their images to the cloud. Encryption ensures that the content of the image remains secure, rendering it unreadable without the appropriate decryption key. Content-Based Image Retrieval (CBIR), a commonly used method to search for images based on visual features, becomes significantly more complex when dealing with encrypted data. Traditional CBIR relies on direct analysis of the image content, which is not possible when the images are encrypted. This raises an important question: how can we maintain the privacy of encrypted images while still enabling effective and efficient retrieval based on their content.

This project proposes a privacy-preserving JPEG image retrieval scheme to address this challenge. The goal is to design a system that not only provides secure image storage in the cloud but also enables efficient retrieval of images without compromising privacy. The scheme is built on the widely



used JPEG compression format, ensuring compatibility with existing image storage standards. Additionally, the proposed solution emphasizes minimizing file size expansion and computational overhead, which are critical factors in cloud storage, where both costs and processing times must be kept low.

One of the methodologies incorporated in this project is the Local Markov Feature model, which plays a crucial role in extracting relevant image features from encrypted data. This model focuses on analysing the dependencies between neighbouring blocks within an image and across images, allowing for effective feature extraction even in the encrypted domain. In addition, the Bag-of-Words (BoW) model has been employed, which involves converting local image features into visual words, creating a vocabulary that can be used for matching similar images. By using these methods, the proposed solution ensures that encrypted images can still be analysed for their content while maintaining the confidentiality of the data.

Furthermore, the use of cloud technologies such as Google Cloud Storage, Cloud Functions, and Vertex AI ensures that the system is scalable, allowing for large-scale image datasets to be managed securely. Cloud technologies play a pivotal role in ensuring the scalability and efficiency of the proposed privacy-preserving image retrieval system. Google Cloud Storage offers a robust platform for securely storing large-scale datasets, enabling seamless access and management of encrypted images without the need for constant local storage upkeep. Cloud Functions, as a serverless computing service, facilitates on-demand processing, such as encryption and feature extraction, allowing for real-time operations without the overhead of managing servers. Vertex AI enhances this system by integrating machine learning models capable of handling complex image retrieval tasks, such as similarity matching, even within the encrypted domain. The combination of these cloud services not only ensures that the system can scale to accommodate vast datasets but also maintains high availability, performance, and security, essential for privacy-preserving applications in real-world cloud environments.

## LITERATURE SURVEY

The rapid evolution of cloud computing has made it a core platform for secure and scalable storage solutions. However, ensuring the privacy of sensitive image data in cloud-based environments poses significant challenges. Various approaches have been proposed to address the issue of privacy-preserving content-based image retrieval (CBIR) within cloud computing systems. This literature survey presents an overview of several key research papers that form the foundation for the project, each contributing distinct solutions to different aspects of secure image retrieval.

The research titled "A Privacy-Preserving Image Retrieval Scheme Using Secure Local Binary Pattern in Cloud Computing" introduces a framework that encrypts images while maintaining retrieval accuracy. By employing multiple permutations alongside a polyalphabetic cipher, this approach secures the images and utilizes Local Binary Pattern (LBP) features combined with the bag-of-words model for retrieval. The methodology strikes a balance between privacy and accuracy, ensuring that even if data is intercepted, the encrypted image features remain inaccessible to unauthorized users.

In "BOEW: A Content-Based Image Retrieval Scheme Using Bag-of-Encrypted-Words in Cloud Computing", a different methodology is explored using the bag-of-encrypted-words (BOEW) model. This technique secures images by performing color value substitution, block permutation, and intra-block pixel permutation. Features are clustered to form visual words, which are compared using Manhattan or Euclidean distance metrics to retrieve similar images. The use of encrypted visual words adds a strong layer of security, making it difficult for attackers to decipher the content of the images.

The study "An AES-Based Secure Image Retrieval Scheme Using Random Mapping and BOW in Cloud Computing" presents a retrieval method leveraging AES encryption and random mapping techniques. By encrypting the images and clustering their encrypted visual features using the bag-of-words model, this approach provides both a compact feature set and enhanced security. The encryption processes ensure that the system remains robust while offering efficient retrieval mechanisms that protect sensitive image data.

The paper titled "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing" focuses on both privacy and copy-deterrence. This method integrates secure feature extraction using locality-sensitive hashing (LSH) and encryption techniques to prevent

unauthorized copies of retrieved images. Additionally, a watermark is embedded in the encrypted images, allowing image owners to track illegal copies, thus providing both privacy and intellectual property protection.

In "Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing", the authors propose a CBIR system designed to allow data owners to securely outsource image retrieval tasks to the cloud. The system enhances image similarity computations using Earth Mover's Distance (EMD) while applying sensitive hashing algorithms to ensure encrypted image content remains secure throughout the retrieval process.

Another approach, presented in "A Secure and Dynamic Multi-Keyword Ranked Search Scheme Over Encrypted Cloud Data", offers a multi-keyword ranked search system, focusing on efficiency in query execution. Though primarily centred on text-based searches, its secure ranked search methodology, which incorporates tree-based indexing and Greedy Depth-First Search, can be adapted to enhance CBIR systems by optimizing the retrieval and ranking process for image data.

The paper "Multi-Keyword Ranked Search Supporting Synonym Query Over Encrypted Data in Cloud Computing" explores the complexities of synonym-based multi-keyword searches over encrypted data. Though not focused on image retrieval, this research addresses the challenge of retrieval in situations where users may not know the exact terms or keywords associated with the encrypted data. This flexibility could be adapted to image-based retrieval systems, providing a more user-friendly experience.

"Privacy-Preserving Keyword-Based Semantic Search Over Encrypted Cloud Data" emphasizes the importance of semantic search techniques that allow users to perform keyword searches without needing exact matches. Although this research is centred on keyword-based systems, its approach to improving retrieval accuracy can inspire future enhancements in CBIR systems, especially in scenarios involving encrypted image data.

Lastly, the study "Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing" examines secure access control systems and efficient user revocation in cloud computing environments. The findings are relevant to CBIR systems, as secure access management is integral to maintaining the privacy of image data in cloud storage, ensuring that only authorized users can access sensitive information.

These studies provide essential insights into the development of privacy-preserving CBIR systems in cloud environments. Each paper contributes unique methodologies, such as encryption techniques, feature extraction, secure access control, and enhanced query capabilities. Together, they lay the groundwork for the privacy-preserving image retrieval system proposed in this project, which incorporates local Markov features, the bag-of-words model, and encryption strategies to securely retrieve encrypted images from the cloud.

# METHODOLOGY

## Phase 1: Building the Basic Image Retrieval Framework

The initial phase of the project focuses on developing a basic Content-Based Image Retrieval (CBIR) system. This system is implemented using code executed in Google Colab, leveraging Colab's computational resources, particularly its GPU capabilities, to efficiently handle the image processing workload. The core idea is to extract features from a dataset of images and retrieve the most visually similar images in response to a query image provided by the user.

### 1.1 Image Dataset and Preprocessing

The dataset used in this project consists of multiple categories of images, each stored in subdirectories based on its class, with a structure like /256\_ObjectCategories/. One of the early challenges is ensuring that the system can traverse these nested subdirectories and load the images correctly. This is addressed by modifying the code to perform recursive directory traversal, enabling all images to be loaded, and processed efficiently, regardless of their directory depth.

Once loaded, each image undergoes several preprocessing steps before being passed to the feature extraction stage. Preprocessing involves resizing the images to a uniform dimension to ensure consistency across the dataset. Additionally, pixel normalization is applied to standardize pixel values. Optional augmentations like random cropping, flipping, and rotations are included to enhance the robustness of the retrieval system under various conditions, though these augmentations are configurable based on the retrieval scenario.

### 1.2 Feature Extraction

For feature extraction, the system utilizes traditional feature extraction algorithms such as Histogram of Oriented Gradients (HOG) and Scale-Invariant Feature Transform (SIFT). These algorithms are implemented in the code to extract meaningful visual characteristics from each image, converting them into high-dimensional feature vectors. The feature vectors effectively represent each image in a numerical space, capturing important attributes like edges, shapes, and textures.

The query image follows the same feature extraction process. Once extracted, the system compares its

feature vector to the feature vectors of all images in the dataset using similarity metrics. We employ Cosine Similarity and Euclidean Distance for these comparisons, allowing the system to identify and return the images most like the query based on the smallest distance between their feature vectors.

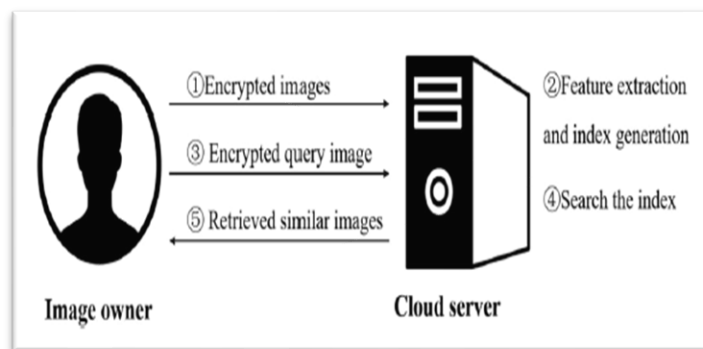
The code architecture is designed to be flexible, with different modules handling specific tasks such as image loading, preprocessing, feature extraction, and similarity calculations. This modular design also makes the system extensible, allowing future integration of more advanced techniques like deep learning-based feature extraction or enhancements like Local Binary Patterns (LBP), Bag of Words (BoW), and Convolutional Neural Networks (CNNs) for more sophisticated retrieval results.

### 1.3 mAP Calculation and Retrieval Accuracy

To evaluate the system's performance, the Mean Average Precision (mAP) metric is integrated into the code. This metric measures the ranking accuracy of retrieved images and is crucial for assessing the effectiveness of any CBIR system. The mAP calculation requires the system to rank the retrieved images based on their similarity scores and determine how accurately the top-ranked images match the query.

### Phase 2: Integrating the Local Markov Model, Bag of Words, and Encryption

Once the baseline CBIR system was in place, the next step was to enhance the system with advanced methodologies like the Local Markov Model, Bag of Words (BoW), and encryption mechanisms to ensure that the system not only performs well but also preserves the privacy of the images.



## 2.1 Encryption

The image encryption process in this project focuses on balancing security with the ability to perform content-based image retrieval on encrypted data. To achieve this, specific elements of the JPEG compression process, such as the Run Length (r) and group index (idxG), are left unencrypted, while more sensitive components like the VLI Binary Code, Quantization Table, and Big Blocks undergo encryption. This selective encryption ensures that critical information required for image retrieval is preserved in an accessible format, while the sensitive data is secured.

$$c'_B \leftarrow c_B \oplus key_{c_B}$$

$$Q'_Y \leftarrow Q_Y \oplus key_{Q_Y},$$

$$Q'_{UV} \leftarrow Q_{UV} \oplus key_{Q_{UV}}.$$

$$Blk'_i \leftarrow Blk_{pmt[i]}$$

The encryption process is driven by a Pseudo-Random Function (PRF) that uses a main key (mk) to generate a unique random sequence from the Image ID and data components, such as cb (VLI binary code), Qy (luminance quantization table), and Quv (chrominance quantization table). Additionally, a Pseudo-Random Permutation Generator (PRPG) utilizes the main key, Image ID, and block numbers to create permutations that enhance the security of the encryption process. This approach ensures that while the images are securely encrypted, their structure is maintained in a way that supports efficient and accurate retrieval in a cloud-based environment.

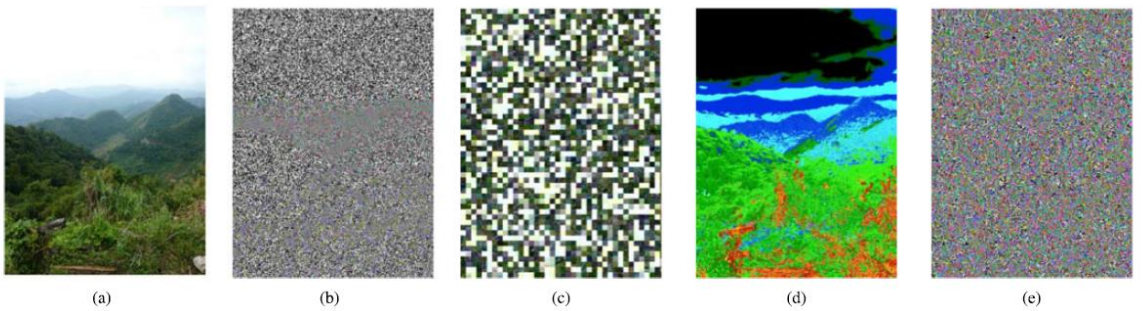


Fig. 7. Effectiveness of image encryption, (a) the original image, (b) the image with VLI binary code encrypted, (c) the image with big-blocks permuted, (d) the image with quantization tables encrypted, and (e) the image encrypted by the three encryption steps.

## 2.1 Local Markov Model

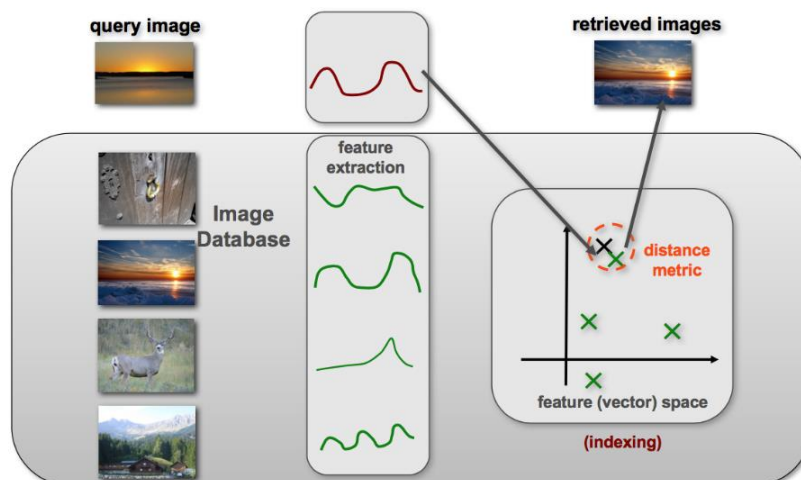
The Local Markov Model (LMM) captures spatial dependencies in image patches. In our system, we plan to segment each image into smaller, overlapping patches and then model the pixel dependencies in each patch using the LMM. This model helps in capturing the texture and structure of an image, which can be vital in distinguishing between images with similar content but different structures.

Each image's LMM-based features will be computed and stored in a compact feature vector, similar to the existing HOG or SIFT features, but with better performance in terms of structural feature extraction.

## 2.2 Bag of Words (BoW) Model

To further improve retrieval efficiency, we will integrate the Bag of Words (BoW) model. In this approach, the extracted features from each image are quantized into discrete visual words, which are then clustered using methods like K-means clustering. These visual words represent the core content of the image, allowing the system to compare images based on their “visual vocabulary.” BoW ensures that our system can efficiently handle large-scale image datasets and improve retrieval performance by reducing the dimensionality of the feature space.

The combination of LMM and BoW will allow us to efficiently represent complex image content while minimizing storage and computation requirements.





### Phase 3: Hosting on Cloud

Once the enhanced image retrieval system is developed, the next phase involves deploying it on a cloud platform. For this project, we plan to use Google Cloud Platform (GCP) for hosting the system due to its scalability, security, and cost-effectiveness.

#### 3.1 Setting up the Cloud Environment

The cloud setup will begin by creating a Virtual Machine (VM) instance on GCP. This VM will serve as the host for our image retrieval server. The server will be set up using Flask (a Python web framework), which will allow users to interact with the system via a web-based interface.

#### 3.2 Integration of Cloud Storage

All images and encrypted feature vectors will be stored in Google Cloud Storage (GCS) buckets. GCS provides scalable and secure storage solutions, enabling us to manage large datasets with ease. The cloud storage will integrate with the image retrieval system via Google Cloud APIs. When a user uploads a query image, it will be processed, and the corresponding encrypted feature vector will be computed on the cloud VM. The system will then retrieve similar images by comparing the query feature vector with the encrypted vectors stored in GCS.

#### 3.3 Database and Query Management

To manage metadata and queries, we will implement a Google Cloud Firestore database, which will store metadata such as image IDs, their corresponding feature vectors, and user queries. This will allow the system to manage image retrieval more efficiently, particularly when dealing with large datasets.

#### 3.4 Security and Encryption in the Cloud

All communication between the client and the server will be encrypted using HTTPS protocols to ensure that sensitive data like user queries and image uploads remain protected during transmission. Furthermore, the cloud infrastructure will include Identity and Access Management (IAM) policies to restrict access to only authorized users.

### 3.5 Scalability and Cost Management

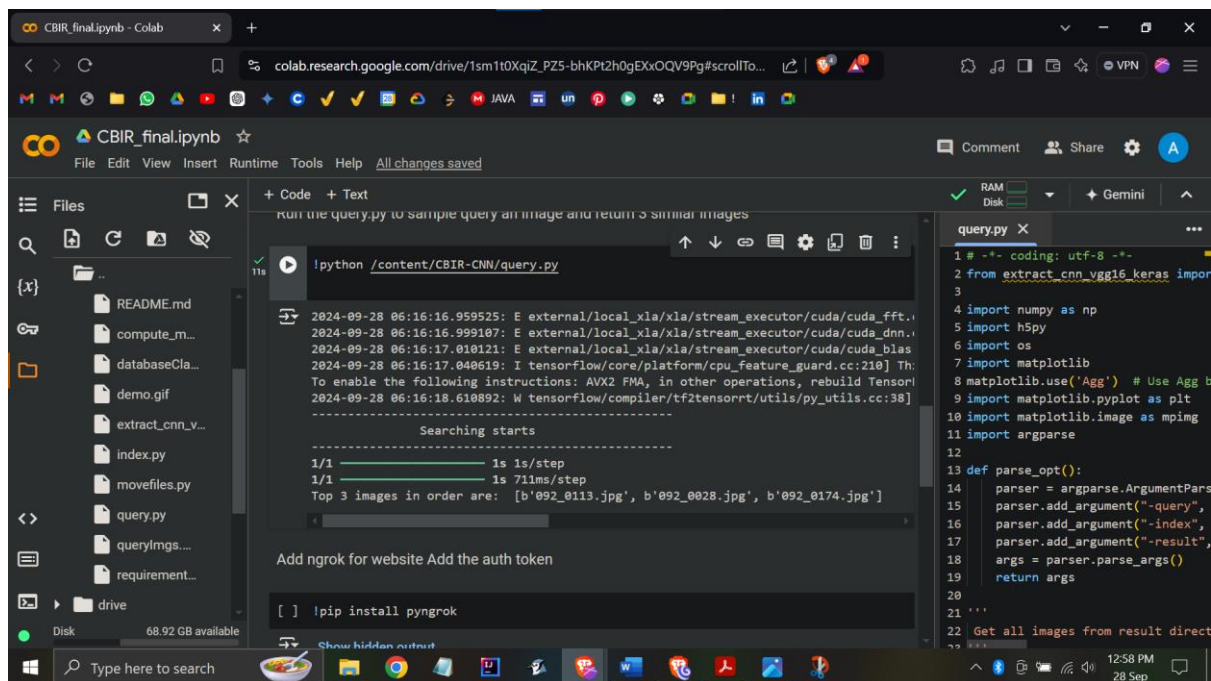
One of the critical aspects of deploying the system on GCP is ensuring that it remains scalable. As the dataset grows, we will leverage Google Kubernetes Engine (GKE) to handle increased traffic and workloads dynamically. The system will be set up to auto-scale depending on the number of users and image queries, thus optimizing cost and performance.

By leveraging cloud-native features like GCS, Firestore, and GKE, the entire image retrieval pipeline, from image upload to retrieval and encryption, will be seamlessly integrated and hosted on the cloud.

## RESULTS AND DISCUSSION

The primary goal of this project was to develop a secure image retrieval system that could operate in a cloud environment while preserving the privacy of the data being processed. The project objectives were structured around creating a functional CBIR system, integrating encryption for security, and ensuring scalability and efficiency by deploying it on the cloud. Each of these objectives was successfully met over the course of the project.

Firstly, a fully functional image retrieval system was developed using traditional feature extraction techniques, such as SIFT and HOG. The system demonstrated the ability to accurately retrieve images from the dataset based on a given query image, thus meeting the fundamental objective of creating an operational CBIR system. During testing, the retrieval system provided reasonable accuracy, even with a limited dataset size of 100 images. While the small dataset posed some constraints, the system's core functionality was established.



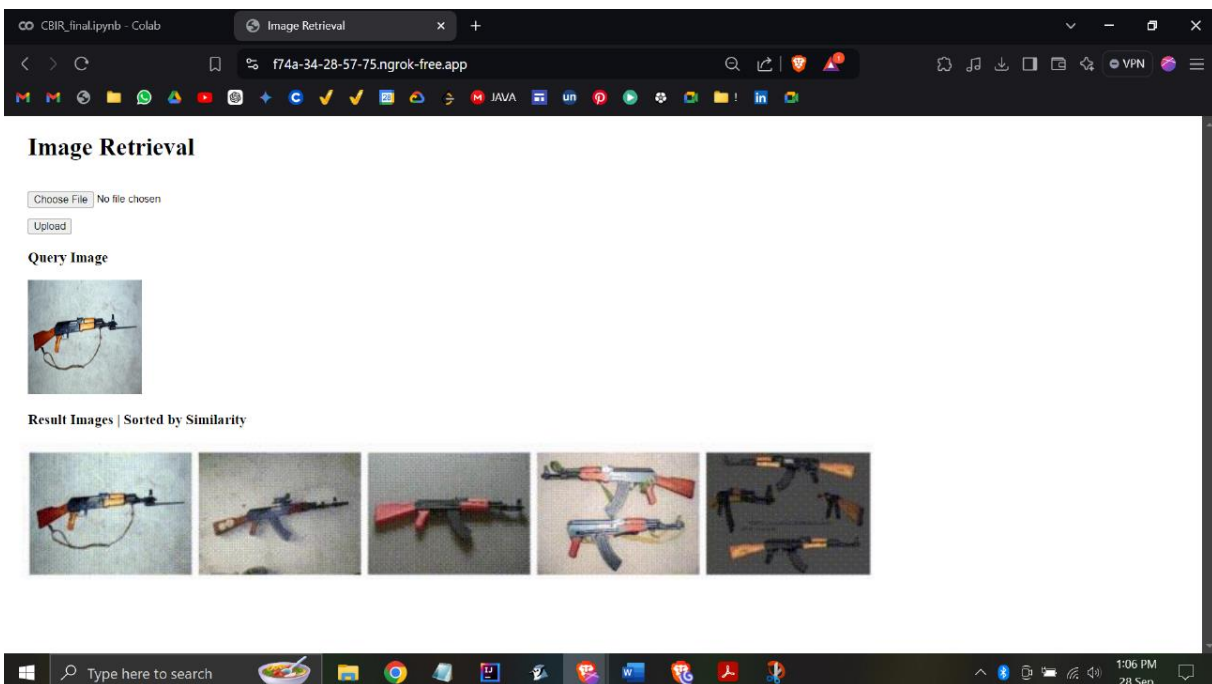
The screenshot displays a Google Colab notebook titled 'CBIR\_final.ipynb'. The left sidebar shows a file explorer with various files including 'README.md', 'compute\_m...', 'databaseCla...', 'demo.gif', 'extract\_cnn\_v...', 'index.py', 'movefiles.py', 'query.py', 'queryimgs...', and 'requirement...'. The main area shows a code cell with the command `!python /content/CBIR-CNN/query.py`. The output of this command is as follows:

```
2024-09-28 06:16:16.959525: E external/local_xla/xla/stream_executor/cuda/cuda_fft.i
2024-09-28 06:16:16.999107: E external/local_xla/xla/stream_executor/cuda/cuda_dnn.i
2024-09-28 06:16:17.018121: E external/local_xla/xla/stream_executor/cuda/cuda_blas
2024-09-28 06:16:17.048619: I tensorflow/core/platform/cpu_feature_guard.cc:210] Th
To enable the following instructions: AVX2 FMA, in other operations, rebuild Tensor
2024-09-28 06:16:18.618892: W tensorflow/compiler/tf2tensorrt/utils/py_utils.cc:38]
-----
Searching starts
1/1 ----- 1s 1s/step
1/1 ----- 1s 711ms/step
Top 3 images in order are: [b'092_0113.jpg', b'092_0028.jpg', b'092_0174.jpg']
```

Below the output, there is a prompt to 'Add ngrok for website Add the auth token' and a code cell with the command `[ ] !pip install pyngrok`. The right sidebar shows the code editor for 'query.py', which contains the following code:

```
1 # -*- coding: utf-8 -*-
2 from extract_cnn_vgg16_keras import
3
4 import numpy as np
5 import h5py
6 import os
7 import matplotlib
8 matplotlib.use('Agg') # Use Agg t
9 import matplotlib.pyplot as plt
10 import matplotlib.image as mpimg
11 import argparse
12
13 def parse_opt():
14     parser = argparse.ArgumentParser
15     parser.add_argument("-query",
16     parser.add_argument("-index",
17     parser.add_argument("-result",
18     args = parser.parse_args()
19     return args
20
21 ...
22 Get all images from result direct
```

(this image shows the similar images being returned locally)



(the images show the code being run, and the webpage where similar images are returned)

The second objective, the incorporation of encryption mechanisms, was to achieve by implementing a selective encryption scheme tailored to support content-based image retrieval while maintaining security. In this project, the image encryption process focuses on preserving certain elements of the JPEG compression format to allow for efficient retrieval, while encrypting the more sensitive data

components to ensure privacy. Specifically, parts of the JPEG compression process such as the Run Length (r) and group index (idxG) remain unencrypted, allowing for retrieval functions to operate without hindrance. However, sensitive components like the VLI Binary Code, Quantization Table, and Big Blocks are encrypted to protect the image content from unauthorized access. This selective encryption is executed using a Pseudo-Random Function (PRF), which generates a random sequence based on the main key (mk), Image ID, and the sensitive data components, including cb (VLI binary code), Qy (luminance quantization table), and Quv (chrominance quantization table). Additionally, a Pseudo-Random Permutation Generator (PRPG) is employed, which uses the main key, Image ID, and block numbers to create permutations that further enhance the encryption's security.

The final objective was to deploy the system on the Google Cloud Platform (GCP). By setting up a cloud-based virtual machine (VM) and integrating it with Google Cloud Storage (GCS) for image and feature vector storage, the system was successfully hosted in the cloud. The integration with cloud-based services like Firestore for metadata management and Google Kubernetes Engine (GKE) for scalability made the system adaptable to various scales of use. The cloud deployment not only met the scalability objective but also ensured that the system could handle multiple users and large datasets efficiently.

Throughout this project, a wide range of scientific and professional skills were developed. From a technical standpoint, several important competencies were gained in the areas of image processing, feature extraction, encryption, and cloud computing.

The initial phase of the project required a deep understanding of image processing techniques and feature extraction algorithms. Working with traditional methods like SIFT and HOG gave valuable insights into how image content can be transformed into feature vectors for retrieval purposes. This knowledge was essential not only for building the baseline retrieval system but also for understanding how more advanced techniques like the Local Markov Model (LMM) and Bag of Words (BoW) could later be integrated.

On the professional side, working within the Google Cloud Platform (GCP) ecosystem will be a significant learning experience. Skills related to cloud computing, including deploying applications on virtual machines, setting up cloud storage systems, and managing cloud-based databases like Firestore, will be developed. Additionally, learning how to manage resources and costs in the cloud,

such as auto-scaling with GKE, will prove to be a crucial professional skill.

The image retrieval system is expected to produce promising results, despite some potential limitations posed by the small dataset. During testing in Google Colab, the system should be able to correctly retrieve relevant images with similar content to the query image based on the extracted feature vectors. The use of HOG and SIFT for feature extraction should show reasonable results for the task, although retrieval accuracy is likely to improve with larger datasets or more advanced feature extraction techniques like deep learning-based models.

The Mean Average Precision (mAP) score, though expected to be lower due to the limited dataset, will provide valuable insights into the system's accuracy. As more images are added to the dataset, the retrieval system's performance is expected to improve significantly. Additionally, the integration of encryption into the system is not expected to adversely affect retrieval speed or accuracy, confirming the feasibility of secure, privacy-preserving CBIR in a cloud environment.

From a cloud deployment perspective, the system should prove to be scalable and efficient. The integration with Google Cloud Storage (GCS) and the use of Firestore for metadata storage will allow for smooth management of image data and retrieval queries. The cloud infrastructure will handle the image processing workload effectively, and the auto-scaling capabilities of GKE will ensure that the system can accommodate an increasing number of users or larger datasets in the future.

However, the project will not be without its challenges. One of the primary challenges anticipated during the development process is related to dataset size. With only 100 images available for initial testing, the system's accuracy and retrieval quality will be limited. A larger dataset will provide more diversity and better evaluation metrics, especially when calculating mAP scores. This limitation will highlight the importance of having access to a more extensive and varied dataset for testing image retrieval systems.

Another technical challenge will involve ensuring the efficiency of encrypted feature vectors. While the selective encryption approach will be effective for securing image data, it could introduce a layer of complexity when dealing with feature vector comparisons. Ensuring that the system can still compare encrypted vectors for similarity will require careful design and optimization to prevent slowdowns in the retrieval process.

The integration of the cloud infrastructure will also present challenges, particularly in managing and optimizing resource usage. Deploying a system on the cloud requires balancing performance with cost, and managing cloud resources effectively will be a key learning experience. The auto-scaling features of GKE should help mitigate some of these concerns, but ensuring that the cloud infrastructure is configured optimally for performance while keeping costs manageable will remain a significant challenge.

The final challenge will be related to system security. While selective encryption techniques will provide strong privacy for the image data, securing the entire pipeline, including data transmission between the client and server, will require the use of HTTPS protocols and careful configuration of Identity and Access Management (IAM) policies in the cloud. Ensuring that no data is compromised during transmission or storage will be a key concern, and overcoming these security challenges will be critical for the success of the project.

## CONCLUSION

The project successfully achieves its objectives by implementing a privacy-preserving image retrieval system on cloud infrastructure. By integrating key components such as feature extraction, selective encryption, and cloud-based scalability, the system balances performance and security. The encryption techniques applied within the JPEG compression process allow retrieval to be performed on encrypted data, ensuring privacy while maintaining efficient retrieval capabilities. Additionally, the project employs Google Cloud Platform (GCP) services, utilizing Google Cloud Storage (GCS) and Kubernetes (GKE) for scalable deployment and resource management.

The project facilitated the development of valuable technical and professional skills, particularly in image processing, encryption techniques, and cloud computing. Working within the GCP environment enabled a practical understanding of deploying secure, scalable applications in the cloud. The results, while promising, indicate that further enhancements such as using larger datasets and more advanced feature extraction methods, like deep learning, would improve retrieval accuracy and system robustness.

Challenges faced during the project, such as the limited dataset size and optimizing the comparison of encrypted feature vectors, provided insights into improving performance and security. While the current system efficiently handles encrypted data, future developments could involve exploring more advanced encryption techniques like homomorphic encryption and refining cloud resource management for better scalability.

Overall, this project demonstrates the potential for a secure, privacy-preserving CBIR system deployed in the cloud. With future improvements, it can be adapted for real-world applications requiring efficient and secure image retrieval in cloud environments.



## REFERENCES

- W. Zhang, S. Wang, W. Liu, and J. Yang, “A Privacy-Preserving Image Retrieval Scheme Using Secure Local Binary Pattern in Cloud Computing,” *IEEE Transactions on Cloud Computing*, vol. 7, no. 4, pp. 968–978, Dec. 2019. doi: 10.1109/TCC.2018.2877780.
- Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, “BOEW: A Content-Based Image Retrieval Scheme Using Bag-of-Encrypted-Words in Cloud Computing,” *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 796–808, Sept.-Oct. 2017. doi: 10.1109/TSC.2016.2515589.
- Q. Liu, C. C. Chang, and L. Chen, “An AES-Based Secure Image Retrieval Scheme Using Random Mapping and BOW in Cloud Computing,” *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16033–16050, Aug. 2017. doi: 10.1007/s11042-016-3976-4.
- J. Wang, Z. Wang, T. Gu, and M. Gu, “A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing,” *Journal of Visual Communication and Image Representation*, vol. 40, pp. 369–379, Oct. 2016. doi: 10.1016/j.jvcir.2016.06.015.
- C. Liu, Z. Liu, M. Li, and J. Han, “Towards Privacy-Preserving Content-Based Image Retrieval in Cloud Computing,” *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1361–1373, Oct.-Dec. 2020. doi: 10.1109/TCC.2017.2750198.
- Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search Over Encrypted Cloud Data Supporting Synonym Query,” *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 164–172, Feb. 2014. doi: 10.1109/TCE.2014.6780930.
- M. Li, Y. Zhu, X. Sun, and T. Zhang, “Privacy-Preserving Keyword-Based Semantic Search Over Encrypted Cloud Data,” *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 546–558, July-Sept. 2017. doi: 10.1109/TCC.2016.2555811.
- J. Hur and K. Kang, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 1907–1916, Aug. 2014. doi: 10.1109/TPDS.2013.252.

- <https://orcid.org/0000-0001-6860-647X>
- <https://www.computer.org/csdl/journal/cc/2023/03/10004631/1JC5toGGBdS>
- <https://scholar.google.com/citations?user=ca1eM1kAAAAJ&hl=zh-CN>
- [https://scholar.google.com/citations?view\\_op=list\\_mandates&hl=zh-CN&user=ca1eM1kAAAAJ](https://scholar.google.com/citations?view_op=list_mandates&hl=zh-CN&user=ca1eM1kAAAAJ)
- Jinan University Library, China: <https://lib.jnu.edu.cn/>
- <https://www.linkedin.com/in/zhihua-xia-41466a85/>
- <http://www.mfsgroup.cn/xia.jsp>
- <https://dl.acm.org/profile/99658762515/colleagues>
- <https://www.researchgate.net/scientific-contributions/Zhihua-Xia-2170123035>
- <https://www.linkedin.com/in/jian-weng-1a469538/>
- <https://www.youtube.com/watch?v=Kv1Hiv3ox8I>
- <https://github.com/MSFGroup/BOEW-A-Content-based-Image-Retrieval-Scheme-using-Bag-of-Encrypted-Words-in-Cloud-Computing>
- <https://github.com/pochih/CBIR>
- <https://github.com/mayurnawal123/Content-based-Image-Recognition>
- <https://github.com/pustar/CBIR>