

**Encryption Independent Multi Owner Multi User Secure
Content Based Image Retrieval for JPEG Images**



By

Sameem Shabbir

(Registration No: 00000401894)

Department of Information Security

Military College of Signals

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)

**Encryption Independent Multi Owner Multi User Secure
Content Based Image Retrieval for JPEG Images**



By

Sameem Shabbir

(Registration No: 00000401894)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Master of Science in
Information Security

Supervisor: Dr. Abdul Ghafoor

Co Supervisor : Dr. Shahzaib Tahir

Military College of Signals

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)


THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by Mr / Ms **Sameem Shabbir** (Registration No. **00000401894**), of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ Masters Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of Masters degree. It is further certified that necessary amendments as point out by GEC members and evaluators of the scholar have also been incorporated in the said thesis.


Signature: 

Name of Supervisor Dr. Abdul Ghafoor

Date: _____

Signature (HoD):  HoD
Information Security
Military College of Sigs


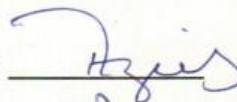
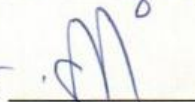
Date: 23-09-2024

Signature (Dean/Principal): 


Date: 26/9/24 **Brig**
Dean, MCS (NUST)
(Asst Masood, Ph.D)

NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY**MASTER THESIS WORK**

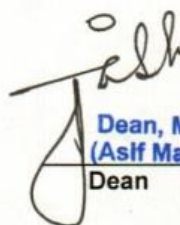
We hereby recommend that the dissertation prepared under our supervision by **Sameem Shabbir MSIS-21 Course** Regn No **0000401894** Titled: "**Encryption Independent Multi Owner Multi User Secure Content Based Image Retrieval for JPEG Images**" be accepted in partial fulfillment of the requirements for the award of **MS Information Security** degree.

Examination Committee Members1. Name : **Asst Prof Dr Sadiqa Arshad**Signature: 2. Name: **Asst Prof Dr Faiz-ul-Islam**Signature: Co-Supervisor's Name: **Assoc Prof Dr Shahzaib Tahir**Signature: Supervisor's Name: **Prof Dr Abdul Ghafoor**Signature: 

Date: _____


 HoD
 Information Security
 Military College of Signals
 Head of Department

Date _____

COUNTERSIGNEDDate: 26/9/24

 Brig
 Dean, MCS (NUST)
 (Asif Masood, PhD)
 Dean

CERTIFICATE OF APPROVAL


This is to certify that the research work presented in this thesis, entitled “Encryption Independent Multi Owner Multi User Secure Content Based Image Retrieval for JPEG Images.” was conducted by Sameem Shabbir under the supervision of Dr Abdul Ghafoor. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Military College of Signals, National University of Science & Technology Information Security Department in partial fulfillment of the requirements for the degree of Master of Science in Field of Information Security Department of information security National University of Sciences and Technology, Islamabad.

Student Name: Sameem Shabbir

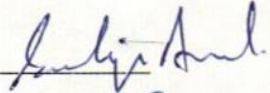
Signature: 

Examination Committee:


a) External Examiner 1: Dr Shahzaib Tahir. (MCS)

Signature: 

b) External Examiner 2: Dr. Sadiqa Arshad. (MCS).

Signature: 


c) External Examiner 3: Dr Faiz Ul Islam. (MCS).

Signature: 

Name of Supervisor: Dr. Abdul Ghafoor

Signature: 

Name of Dean/HOD. Dr Muhammad Faisal Amjad

Signature: 
HOD
Information Security
Military College of Sigs

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled **Encryption Independent Multi Owner Multi User Secure Content Based Image Retrieval for JPEG Images** is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/ revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature:  _____

Name: **Sameem Shabbir** _____

Date: _____

AUTHOR'S DECLARATION

I **Sameem Shabbir** hereby state that my MS thesis titled "**Encryption Independent Multi Owner Multi User Secure Content Based Image Retrieval for JPEG Images**" is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature:  _____

Name: **Sameem Shabbir** _____

Date: _____

DEDICATION

Dedicated to the children of Palestine.

ACKNOWLEDGEMENTS

I would like to especially thank my mother, father and faculty members, without whose guidance and support I would not be here.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	IX
LIST OF TABLES	XII
LIST OF FIGURES	XIII
LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS	XIV
ABSTRACT	XVI
CHAPTER 1: INTRODUCTION	1
1.1 Secure CBIR (S-CBIR)	3
1.2 Motivation	4
1.3 Aim and Objective	4
1.3.1 Design Goals	5
1.3.2 Security Goals	5
1.4 Research Contribution	5
1.5 Thesis Organization	6
CHAPTER 2: PRELIMINIARIES	8
2.1 S-CBIR Requirements	8
2.2 Categories of S-CBIR	9
2.2.1 Feature Extract & Encrypt	9
2.2.2 Encrypt and Feature Extract	10
2.3 Security in S-CBIR	12
CHAPTER 3: LITERATURE REVIEW	15
3.1 Feature Extract and Encrypt Schemes	15
3.2 Encrypt and Extract Features Schemes	16
3.3 Weakness / Research Gap	21
CHAPTER 4: ANATOMY OF JPEG	23
4.1 JPEG Compression Process	23
4.1.1 Preliminaries	23
4.1.2 Quantization	24
4.1.3 Entropy Coding	24
4.2 JPEG File Format	25
4.2.1 Define Huffman Table Marker	26
4.2.2 JPEG Reading in Bit Format	28
4.3 Decoding JPEG	28
CHAPTER 5: PROPOSED SYSTEM	31
5.1 Prerequisites	31
5.2 Overview of The Proposed Scheme	32

5.3	Segmented Encryption	34
5.4	Feature Extraction	37
5.5	Image Retrieval	37
CHAPTER 6: EXPERIMENTATION & RESULTS		40
6.1	Experimentation	41
6.1.1	Feature Engineering	41
6.1.2	Model Selection	42
6.2	Performance	43
6.2.1	Encryption Performance	43
6.2.2	Feature Extraction	43
6.2.3	Retrieval Performance	44
6.2.4	Retrieval Efficiency	44
6.3	Security	45
6.3.1	Security of Image Data	45
6.3.2	Security of JPEG Segments Less Image Data	46
6.3.3	Information Leakage	46
6.4	Analysis	47
SUMMARY OF RESEARCH WORK		49
CHAPTER 7: CONCLUSIONS AND FUTURE RECOMMENDATION		51
7.1	Conclusion	51
7.2	Future Work	52
REFERENCES		53

LIST OF TABLES

	Page No.
Table 1: Comparison of S-CBIR Schemes	11
Table 2: Summary - Literature Review	19
Table 3: Encryption Time	43
Table 4: Retrieval Performance	44

LIST OF FIGURES

	Page No.
Figure 1: Generic CBIR System [14].....	2
Figure 2: S-CBIR Requirements.....	9
Figure 3: Generic Feature Extract and Encrypt S-CBIR System [15].....	10
Figure 4: Generic Encrypt and Feature Extract System [16].....	11
Figure 5: Baseline JPEG Compression Process [17].....	25
Figure 6: JPEG File Structure [11].....	27
Figure 7: Content Owner(s) in Proposed Scheme.....	33
Figure 8: Query User(s) in Proposed Scheme.....	34
Figure 9: Encrypted vs Un-encrypted Depiction (Yellow highlighted is unencrypted part)	36
Figure 10: Cloud in Proposed Scheme.....	38
Figure 11 : Confusion Matrix (K-Means).....	45
Figure 12: Confusion Matrix (MLP).....	45

LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

ASPE	Asymmetric Scalar-product Preserving Encryption
CBIR	Content Based Image Retrieval
CCA	Chosen-Ciphertext Attack
COA	Ciphertext-Only Attacks
CPA	Chosen-Plaintext Attack
DCT	Discrete Cosine Transform
DHT	Define Huffman Table
DQT	Define Quantization Table
ECB	Electronic Codebook
EOI	End of Image
FFDSH	Framework For the Deep Supervised Hashing
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Experts Group
LSH	Locality Sensitive Hashing
mAP	Mean Average Precision

ML	Machine Learning
MLP	Multi Layer Perceptron
OS	Operating System
RAM	Random Access Memory
RIOT	Radical Image Optimization Tool
S-CBIR	Secure CBIR
SOI	Start of Image
SOS	Start of Scan
SVM	Support Vector Machine
TBIR	Text-Based Image Retrieval
XGBoost	Extreme Gradient Boosting classifier

ABSTRACT

Image retrieval systems help users to browse and search among extensive images in real-time. Various image retrieval techniques have been developed over the years. Content based image retrieval is a technique employed to search and retrieve similar images based on their visual content (query image) rather than text-based query. On the other hand, secure content-based image retrieval is meant to retrieve similar images from encrypted images. At present, various secure content-based image retrieval schemes have been developed which encrypt images first and extract features subsequently. However, none of existing schemes uses NIST approved / globally accepted encryption nor there are any techniques available which gives liberty to user to use any encryption scheme resulting in restricting user's liberty, which is contradictory to multi-user environment of cloud. In this research, we propose a novel paradigm which gives independence to users to use any encryption primitive as per their security needs. Applicable to optimized JPEG images, our proposed system employs segmented encryption to encrypt image data segment of JPEG images. Subsequently, Huffman tables; extracted from encrypted images are used for retrieval tasks employing machine learning in both supervised and unsupervised domain. Experiments reveal that our scheme achieves excellent performance in terms of efficiency.

Keywords: Secure CBIR; Encrypt and feature extract, JPEG, Encryption, Huffman tables, Machine Learning.

CHAPTER 1: INTRODUCTION

Rapid development, advancement and accessibility of low-cost image capturing devices, such as smartphones, digital cameras, security cameras etc, have significantly contributed towards exponential growth in number of images being produced. To cater for storage needs; users either develop their own infrastructure or use cloud. Cloud storage offers numerous advantages, such as scalability, accessibility, and cost-efficiency. Thus, cloud is fast becoming an ideal solution for managing huge amounts of image data. Users can easily upload, store, and access their images from anywhere with an internet connection, fostering a seamless experience for personal and professional use.

The convenience offered by cloud has led to an unprecedented accumulation of images on cloud services. More and more individuals / organizations are storing vast amounts of images on the cloud. In order to enhance data usability from immensely huge image storage, we need image retrieval techniques. Image retrieval techniques offer means to efficiently and accurately locate specific images within vast datasets. Image retrieval techniques ensure that the users can quickly and intuitively access the images they need, thereby improving the overall efficiency and effectiveness of data utilization in both personal and professional settings. As the volume of stored images continues to grow, the importance of developing and refining these retrieval techniques becomes increasingly important for maintaining the usability and accessibility of large-scale image repositories.

To cater for the diverse needs of users, various image retrieval techniques have been developed over the years. These techniques enable users to retrieve images based on different criteria. One of the commonly known methods is Text-Based Image Retrieval

(TBIR). In TBIR, images are searched using text queries. TBIR does not give liberty of finding similar images based upon query image. Moreover, this method relies on the accuracy and comprehensiveness of the image annotations, which can be labor-intensive and prone to human error. Other techniques of image retrieval include Sketch-Based Image Retrieval (rough sketch of the image is the query) and Content-Based Image Retrieval (CBIR).

CBIR is a technique employed to search and retrieve similar images based on their visual content (query image) rather than text-based query. CBIR uses the actual content of the images, such as color, texture, shape or any other visual features to perform searches. In a generic CBIR system, images are uploaded to database / cloud by the content owner. Query user is the one who needs to find the relevant images. Query user generates query in form of an image. The CBIR system performs similarity checks on the query image viz-a-viz the images database and returns similar images.

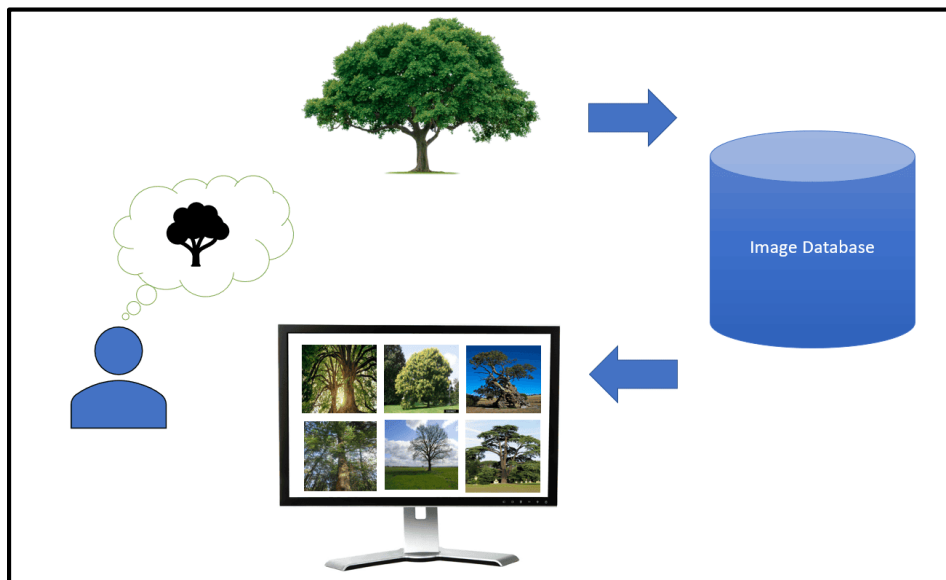


Figure 1: Generic CBIR System [14]

1.1 Secure CBIR (S-CBIR)

The need to ensure the security and privacy of user images stored in the multi-user environment of the cloud has led to adoption of various security measures. Encryption is one of the methods employed to ensure confidentiality of data. Encrypted images are transformed into scrambled format thus hiding the original content, making it unreadable to unauthorized individuals.

Encryption effectively randomizes and destroys recognizable patterns in the data, thereby protecting sensitive information from unauthorized access and potential breaches. However, the use of encryption presents a significant challenge for conventional CBIR techniques. Methods on which traditional CBIR rely i.e. color, texture, shape or any other visual features, have been encrypted now. There are no patterns in encrypted images which can be used by traditional CBIR.

To address this challenge, S-CBIR has evolved. S-CBIR techniques are designed to facilitate image retrieval directly from encrypted images without the need for decryption, thereby maintaining data security and privacy throughout the retrieval process. In a generic S-CBIR system, images are encrypted prior to uploading to database / cloud by the content owner. Query user generates query in form of either an encrypted image or in form of an extracted feature from the image. The S-CBIR system performs similarity checks on the query viz-a-viz the encrypted images / encrypted features database and returns similar encrypted images to the query user. Query user, upon receipt of encrypted images, decrypts them for subsequent use.

1.2 Motivation

The development of robust SCBIR systems holds significant implications for various domains. In healthcare, it can facilitate secure medical image retrieval for diagnostics without compromising patient privacy. Similarly, in law enforcement, SCBIR can enable secure image-based criminal identification. As research in SCBIR progresses, striking a balance between retrieval accuracy and data security is also crucial. This will ensure the ethical and secure utilization of CBIR technology across diverse applications.

However, in existing Encrypt and extract features S-CBIR, there is neither any technique which uses NIST approved / globally accepted encryption nor there are any techniques available which gives liberty to use any encryption scheme. Cloud is a multi – user, multi-owner environment which should not confine users. Whereas, in all of the existing schemes, the content owners are forced to use the novel encryption schemes. Owner of sensitive data may not trust a newly developed encryption primitive. Moreover, restricting users to a particular encryption scheme restricts user’s liberty, which is contradictory to multi-user environment of cloud.

1.3 Aim and Objective

Our research is meant to develop an Encrypt and Feature Extract CBIR system for JPEG images which not only provides improved security for the image data but also gives the users the liberty to use any encryption primitive / scheme. We will use Machine Learning on extracted features from encrypted images and will evaluate the performance on Corel 1K dataset in terms of time to encrypt, feature extraction time, mean average Precision (mAP)

1.3.1 Design Goals

To design a S-CBIR system as per following

- Design an Encrypt and Feature Extract S-CBIR model.
- Proposed model to give independence to users with regards to choice of encryption primitive.
- Proposed model to support multi-user multi-owner i.e. not restricted to one user settings
- Liberty of encryption to also apply on query image i.e. Encryption scheme of query image and the images in the database may be different.
- Proposed model to support adaptive key.

1.3.2 Security Goals

To give liberty to Cloud users to select encryption primitive / scheme as per their security needs.

1.4 Research Contribution

Our proposed scheme is a step towards practical implementation of S-CBIR in real world scenarios. Our proposal gives independence in selection of encryption primitive as per the security modelling of users. To the best of our knowledge, no such contribution has been made so far.

1.5 Thesis Organization

The thesis is organized into seven chapters. While, first chapter is introduction, details on remaining chapters are as follows.

Chapter 2 contains the preliminary knowledge essential to understanding of the research. It enables the reader from content based image retrieval to Secure content based image retrieval. It dwells upon the requirements of S-CBIR and further explains the two categories of S-CBIR. In the end, intricate details on security of S-CBIR are covered.

Chapter 3 gives an overview of the recent research in the domain of S-CBIR. Feature extract and encrypt schemes are briefly touched upon in section 2.2.1. Encrypt and feature extract schemes are thoroughly covered in next section. In the end research gap is identified.

Chapter 4 enables the reader on the JPEG compression. Our research is focused upon JPEG and utilizes the inherent advantages of JPEG for utilization in CBIR. Therefore initial part of the chapter gives a general overview of the JPEG compression while the later part contains the details on Huffman table. It ends with a brief note on how to decode a JPEG image.

Chapter 5 explains the proposed system. It defines the pre-requisite required for the system, followed by an overview of the proposed system. Subsequently, details on the Segmented encryption, feature extraction process and image retrieval are covered.

Chapter 6 is about the results and experimentation performed to reach to those results. The experimentation part is primarily covered in two domains i.e. experimentation

on feature engineering and experimentation on model selection. Second part of the chapter gives the results in terms of retrieval efficacy, efficiency and performance.

Chapter 7 concludes the thesis. Conclusion is followed by future work which contains recommendations on how to further improve upon the proposed scheme.

CHAPTER 2: PRELIMINARIES

This chapter is meant to set the foundation and provide readers with the base knowledge by providing an essential background to the study. CBIR is already being used by internet users in form of Google image search etc. Next on horizon is the domain of secure CBIR. A brief intro of S-CBIR has been covered in Chapter 1. In this chapter we will begin with specific requirements of S-CBIR, followed by categorization of S-CBIR. In the end security requirements of S-CBIR have been covered.

2.1 S-CBIR Requirements

Prior to advent of S-CBIR, traditional CBIR systems focused on time efficiency and query effectiveness. Time efficiency implies that how quick a user gets similar images based upon the query image. Query effectiveness gives an idea of similarity index i.e. how much related the output images are to the input. E.g if the query image contains image of a cat then how many of retrieved images contains cats. Generally, both these requirements are contradictory i.e. achieving high on one is at the cost of another.

In S-CBIR, as mentioned above, a new dimension of security has been added. This implies addition of a new requirement. A S-CBIR system has to focus on 3 requirements i.e. time efficiency, query effectiveness and security. Security primarily relies on Encryption. The Encryption scheme used and how it is used will decide the security level.

Addition of security dimension added new complexity to CBIR systems. Increasing security generally results in decrease in query effectiveness and time efficiency and vice

versa. An ideal S-CBIR system would be the one to achieve maximum on all 3 of the requirements.

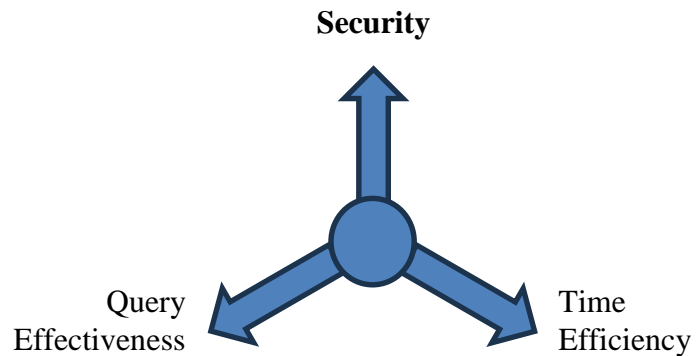


Figure 2: S-CBIR Requirements

2.2 Categories of S-CBIR

S-CBIR can be divided into two categories i.e. 1) Feature extract and encrypt and 2) Encrypt and extract features. Primarily, the difference not only lies in the sequence of encryption and feature extraction but also in the modus operandi of the schemes.

2.2.1 Feature Extract & Encrypt

In this technique features are extracted prior to encryption of images. After extraction of features, the images are encrypted. Both encrypted images and features are uploaded to cloud. There is diversity in literature as far as encryption of features is concerned. Nevertheless, feature encryption does offers better security and privacy but also

impedes the retrieval. For image retrieval, the query user follows the same steps i.e. feature extraction, encryption and uploading to cloud. Similar images are retrieved basing upon the query features. In this category, the image owner has an extra burden of extracting features from images.

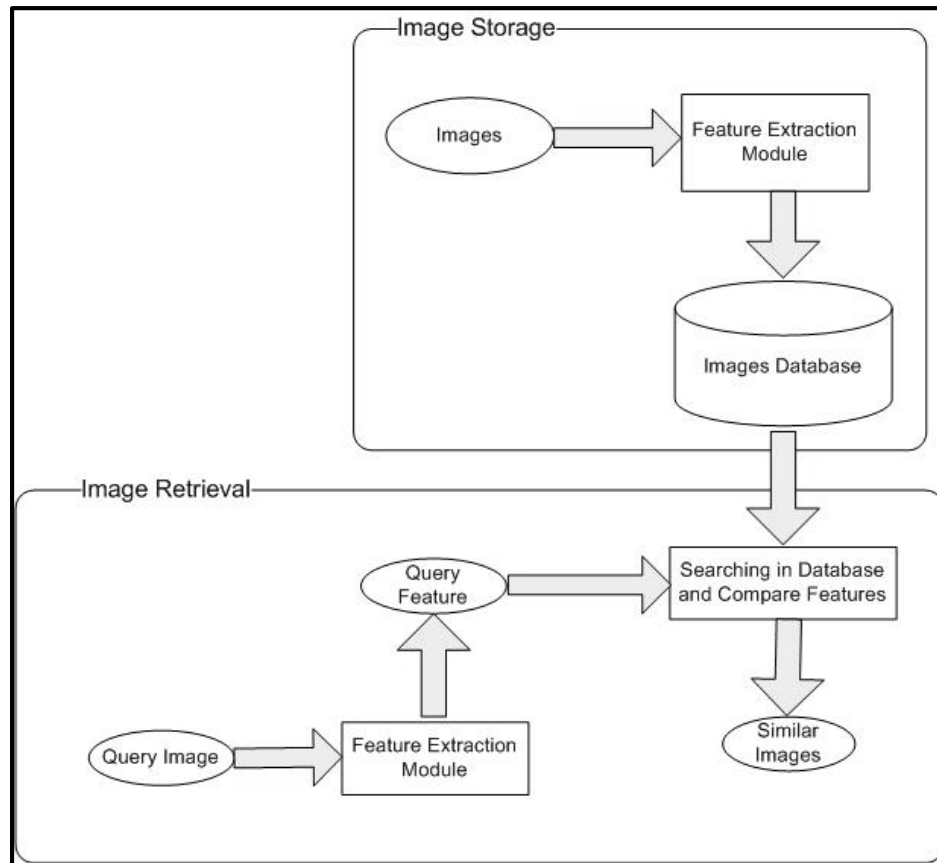


Figure 3: Generic Feature Extract and Encrypt S-CBIR System [15]

2.2.2 *Encrypt and Feature Extract*

In this technique features are extracted directly from encrypted images. Image owner is only responsible to Encrypt the images. After encryption the images are sent to cloud. The query user is also responsible for encryption only. Encrypted images from the query user are uploaded to cloud. The cloud then extracts features from the

encrypted images and then runs similarity algorithms. Similar encrypted images are returned to query user based upon encrypted query image. Query user decrypts images for subsequent use.

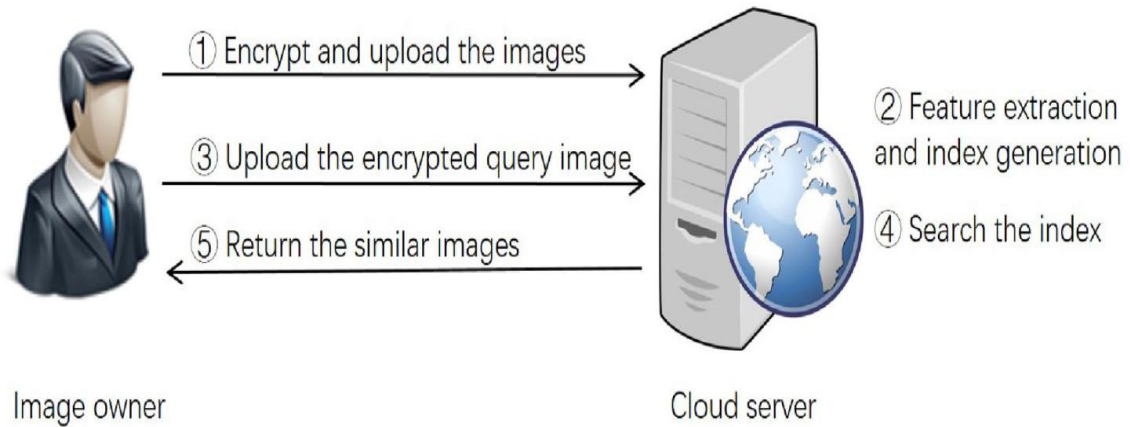


Figure 4:Generic Encrypt and Feature Extract System [16]

A comparison of both the schemes is given in Table 1: Comparison of S-CBIR Schemes.

Table 1: Comparison of S-CBIR Schemes

Aspect	Feature Extract & Encrypt	Encrypt and Feature Extract
Image Owner's Responsibility	Feature extraction and encryption	Encryption only

Query Responsibility	User's	-do-	-do-
Feature Extraction		Done before encryption	Done on encrypted images in the cloud
Cloud Dependence		Moderate	High

2.3 Security in S-CBIR

Security element in S-CBIR is primarily ensured by encrypting images. As mentioned above, the encryption scheme used and how it is used determines the security level. Key points with regards to security are briefly given in succeeding paragraphs.

Cryptanalysis is used to determine security. Secure against Ciphertext-Only Attacks (COA) is the minimum level of security. Others (in order of increasing security) include Known-Plaintext Attack (KPA) Resistant, Chosen-Plaintext Attack (CPA) Resistant and Chosen-Ciphertext Attack (CCA) Resistant. CCA is the strongest level of security.

There are certain Encryption primitives or algorithms which have been thoroughly tested worldwide. AES and DES are the two commonly known, thoroughly tested algorithms. AES is the NIST approved encryption algorithm. DES is no longer included in NIST approved encryption algorithm. A unique advantage of AES over DES is of

underlying math. The math / logic used in S-box of AES is publicly available. However, for DES it was not available.

One major challenge in encryption is key management. Key management includes the process of generating, distributing, and storing cryptographic keys. Poor key management can compromise the effectiveness of encryption. Secondly it is also important to keep in mind that updating existing systems and infrastructure to support new cryptographic standards can be a complex and resource-intensive process. Compatibility with legacy system, seamlessly integration with existing workflows and operations, data migration etc are some of the challenges in shift to new cryptographic standards.

With the specific requirements in view, different applications have developed their own encryption primitives. However, new algorithms must be thoroughly tested to ensure they are truly resistant and efficient for practical use. Encryption development and testing phases are generally lengthy. E.g. Post-Quantum Cryptography Standardization program and competition by NIST was launched in 2016 to update their standards to include post-quantum cryptography. The program is still ongoing.

With the advent of quantum computing, the robustness of current encryption algorithms is being tested. Quantum computing represents a significant leap in computational power – a challenge in backdrop of brute force attacks. Nevertheless, most of the symmetric encryption schemes including AES are likely to survive in post quantum stage while existing asymmetric encryption schemes (RSA etc) are not post quantum safe.

In this chapter we have build the foundation knowledge regarding S-CBIR systems. We laid the groundwork for understanding the specific requirements and categorization of

S-CBIR. By detailing the fundamental aspects and security needs of S-CBIR, we have established a comprehensive background for the subsequent chapters. Prior to moving to the proposed scheme, it is necessary to have a thorough understanding of what has been done so far in our proposed area of work. Then in later chapters, the insight provided in this chapter will serve as reference as we delve on application phase of our proposed scheme.

CHAPTER 3: LITERATURE REVIEW

This chapter presents the work carried out in the proposed domain of S-CBIR. By examining previous research and developments in the field, this review aims to identify key trends, methodologies, and gaps in the existing systems. Feature extract and encrypt schemes are briefly touched upon in section 3.1. Encrypt and feature extract schemes are thoroughly covered in the next section. Subsequently comparison of research is given. In the end research gap is identified.

S-CBIR is an active research area. As already mentioned, S-CBIR can be divided into two categories i.e. 1) Feature extract and encrypt and 2) Encrypt and extract features. Although our research falls in the category of “Encrypt and extract features”, but in order to give the readers an understanding of overall CBIR context, a brief literature overview of “Feature extract and encrypt” is also given. Subsequently, latest trends in “Encrypt and extract features” schemes have been covered with bias towards JPEG images in “Encrypt and extract features” category.

3.1 Feature Extract and Encrypt Schemes

Qiuyu Zhang et al. [10] targeted improvement in feature extraction module by proposing a feature fusion construction scheme named as Framework For the Deep Supervised Hashing (FFDSH). FFDSH uses two deep feature extractors, namely VGG16 and 4-layer CNNs. Evaluation is performed on CIFAR-10 and NUS-WIDE. Max mAP of 0.98 and 0.83 respectively has been achieved.

Anju J et al. [9] proposed a Privacy Preserving CBIR. They used MPEG-7 visual descriptor as features. Five out of two feature vectors were combined to form a new feature vector. Asymmetric Scalar-product Preserving Encryption (ASPE) and Locality Sensitive Hashing (LSH) is employed to ensure security and privacy. Moreover, query feature vector is also encrypted in trapdoor to ensure privacy. Image encryption and feature extraction is done by image owner. For searching the index, image/query users create a query trapdoor using modified feature vectors generated from the query image. The query trapdoor mainly comprises L hash buckets generated by hashing modified query feature vectors along with encrypted feature vector. On getting the query trapdoor, the images that fall in the same hash buckets as that of the query trapdoor are retrieved by the cloud server. Tests are performed on Corel-10k. Against all images categories, a max retrieval precision of 0.34 has been achieved while index generation time is 130.59 seconds. Search time is 3 ms.

3.2 Encrypt and Extract Features Schemes

Hang Cheng et al. [2] developed a retrieval scheme for encrypted JPEG images based on a Markov process. The proposed encryption method involved encrypting Discrete Cosine Transform (DCT) coefficients with a stream cipher followed by permutation. The binary sequences with respect to the quantization tables from the file header are encrypted by performing XOR operation with stream cipher. Further encoded binary sequences is pseudo-randomly permuted in a same component. Intra-block, inter-block, and inter-component dependencies among DCT coefficients is modeled by Markov process and utilized in multiclass SVM for image retrieval. The scheme provided liberty to use any stream cipher and also supported different multiple users with different encryption keys. But, [3] indicated that in this scheme the image dataset used for training the retrieval model

needed to be provided in advance, thus limiting utility. Moreover encryption time and feature extraction time is not evaluated.

Peiya Li et al [3] proposed to encrypt JPEG by replacing original 8×8 DCT with the orthogonal transform followed by 8×8 blocks' permutation. For retrieval, the server calculates the histograms of transformed coefficients located at different frequency positions. By computing the distance between the histograms of encrypted query image and database cipherimages, similar images are returned. The proposed scheme does not produce additional computation. Moreover compression performance of JPEG is also unaffected. However, [5] pointed out use of shallow features from cipher-images, which are unable to express enough information which in turns affects retrieval performance.

Qihua Feng et al. [5] proposed image encryption during JPEG compression process, by encrypting VLI code of Discrete Cosine Transform (DCT) coefficient with a stream cipher. Length of VLI code (remains unchanged, before and after encryption) and global Huffman code frequency of cipher images are employed as features. Retrieval is based upon Vision Transformer. The scheme can employ both supervised and unsupervised settings and it provided good retrieval performance in comparison to others. However, visual safety, as claimed by authors, is slightly lower than other schemes. Moreover, proposed scheme used plain text image as input of BLAKE hashing algorithm to generate key. Thus key management challenges, can't be ruled out in practical implementation.

For image encryption, Zhixun Lu et al., [6] applied orthogonal transform on 8×8 blocks, followed by permutation of quantized blocks followed by use of stream cipher on AC and DC VLI code. Huffman-code histograms from cipher-images are used as an input

to self-attention neural networks model for image retrieval. Cosine distance is used for similarity measure and nearest images are returned to query user. The paper used deep learning and thus provides good retrieval performance on big data sets. Nevertheless the encryption is claimed to be secure only under ciphertext only attack.

Encryption scheme of Peipeng Yu et al. [7] involves xoring the VLI binary code and quantization tables with separate keys. Subsequently, permutation is performed on 8 x 8 blocks of JPEG image. Unencrypted part of DCT coefficients i.e. r (run length) and index and the position of 8 x 8 DCT coefficient blocks in a big-block are used as a features. Manhattan distance between the feature vectors is used to determine similarity. The proposed scheme ensures JPEG compatibility and no increase in file size. Moreover precision is also improved from previous schemes. However, encryption scheme is not different from previous schemes and hence security is not improved in this scheme either.

The only attempt to improve security in a S-CBIR system in SE domain was done by Hua Wang et al [4] who attempted CBIR on AES encrypted images. AES in Electronic Codebook (ECB) mode with 128 bit key length was used for encryption. To counter effects deterministic encryption, block permutation is employed. For feature extraction, the encrypted image is divided into big-blocks, which are made up of several adjacent 4x4 blocks. Then, local feature vectors are extracted from such big-blocks. K-means algorithm is employed to generate vocabulary. Similarity is determined by measuring distance of feature vectors. This was the first attempt to focus on security. It attempted to retrieve images from an encryption algorithm which is secure in known-plaintext domain. However, precision of retrieval is not very high. Moreover use of AES was also limited to 128 bit key which is shortest amongst the approved key lengths.

In yet another attempt to focus on security, Haihua Liang [8] added the aspect of integrity in their proposed system. MD5 or SHA has been proposed for hashing during encryption stage. Comparison of hash value provides integrity check. However, [6] pointed out on low precision in proposed scheme. Moreover, the encryption scheme is also secure in known ciphertext attack model and thus confidentiality is not improved.

Comparison of all schemes is given in Table 2: Summary - Literature Review

Table 2: Summary - Literature Review

Paper	Encryption Method	Retrieval Model	Pros	Cons	Liberty of Enc	Novel Enc
Hang Cheng et al. [2]	Encrypts DCT coefficients with stream cipher, followed by permutation. XOR encryption of binary sequences with stream cipher and pseudo-random permutation.	Models intra-block, inter-block, and inter-component dependencies using Markov process and multiclass SVM.	Flexibility in choice of stream cipher Supports multiple users with different keys.	Lacks evaluation of encryption and feature extraction time	No	Yes
Peiya Li et al. [3]	Replaces 8×8 DCT with orthogonal transform and permutes 8×8 blocks.	Uses histograms of transformed coefficients and measures distance between histograms for similarity.	No additional computation Retains JPEG compression performance.	Shallow features Low retrieval performance.	No	Yes

Qihua Feng et al. [5]	Encrypts VLI code of DCT coefficient with stream cipher during JPEG compression.	Uses Vision Transformer, leveraging VLI code length and global Huffman code frequency as features.	Good retrieval performance, supports both supervised and unsupervised settings.	Less visual safety Key management challenges due to plain text input for key generation.	No	Yes
Zhixun Lu et al. [6]	Applies orthogonal transform, permutes quantized blocks, and uses stream cipher on AC and DC VLI code.	Employs Huffman-code histograms and self-attention neural networks, using cosine distance for similarity.	Good retrieval performance on large datasets.	Secure only under ciphertext-only attack.	No	Yes
Peipeng Yu et al. [7]	XORs VLI binary code and quantization tables with separate keys, followed by 8×8 block permutation.	Uses unencrypted parts of DCT coefficients and positions of 8×8 blocks, with Manhattan distance for similarity.	Maintains JPEG compatibility No file size increase	Similar to previous schemes, security not significantly enhanced.	No	Yes
Hua Wang et al. [4]	Uses AES in ECB mode with 128-bit key, followed by block permutation.	Divides encrypted image into big-blocks, extracts local feature vectors, and uses K-means for	Retrieves images securely in known-plaintext domain.	Low retrieval precision Limited to 128-bit key of AES.	No	Partial (AES in ECB followed by block permutation)

		vocabulary generation.				
Haihua Liang [8]	Incorporate s integrity check with MD5 or SHA during encryption.	Based on hash value comparison for integrity.	Adds integrity aspect.	Low precision Confidentiality not improved significantly.	No	Yes

3.3 Weakness / Research Gap

As evident from above mentioned papers, the encryption scheme are secure in known cipher text attack model only. Moreover, novel encryption schemes have been devised specifically for the requirement of CBIR which may not be trusted by data owners’. Only Hua Wang et al. attempted CBIR using AES. However AES in ECB mode is not recommended and to counter ECB mode, block permutation is applied after AES encryption to hide pattern. Moreover, key length is also restricted to key length is restricted to 128 bits. The scheme also consumes considerable time and has low precision.

Furthermore, at present, Multi-party Multi-owner is not supported in any of the above mentioned schemes. The image owner is bound to use a prescribed encryption scheme for CBIR to work. This restricts user’s liberty which is contradictory to multi-user environment of cloud.

From the above discussion, it can be safely concluded that at present there is neither any searchable encryption based CBIR which uses NIST approved encryption nor there is any technique available which gives liberty to use any encryption scheme.

In this chapter we performed the literature review in the field. Literature review is covered in category of Feature extract and encrypt schemes and Encrypt and feature extract schemes. This review aimed to identify key trends, methodologies, and gaps in the existing systems as given in last part of chapter.

CHAPTER 4: ANATOMY OF JPEG

Since our research is focused on JPEG images, it is therefore prudent to have an overview of JPEG images. This chapter gives a comprehensive review on JPEG compression process specifically with regards to our research. Inherent features of JPEG standard on which our research is based are explicitly explained.

JPEG, stands for Joint Photographic Experts Group. JPEG standard, published in 1992 [18], is the most widely used method to compress digital images [19]. JPEG is lossy compression i.e. some information is lost during compression process.

4.1 JPEG Compression Process

JPEG compression process includes: color space conversion to YCbCr followed by down sampling, discrete cosine transform (DCT), quantization, and entropy coding.

4.1.1 Preliminaries

Digital images can be represented in RGB color model or YCbCr color model. As a first step in JPEG conversion; a RGB image is converted to YCbCr color model. The reason for conversion is that human eye is more sensitive to luminance (brightness) than chrominance (color). Moreover, it gives advantage of efficient handling of color information. Next exploiting the fact (human eye is less sensitive to color detail than to brightness), the Cb and Cr components are down sampled at a lower resolution than the Y component. A common down sampling ratio is 4:2:0 (Chrominance components sampled to half the horizontal and vertical resolution of the luminance component). This step

reduces the amount of data needed to be processed in subsequent steps, thus contributing to the overall compression.

Next comes the step of Discrete Cosine Transform (DCT). The image is divided into 8x8 pixel blocks. Each block is transformed from the spatial domain data (pixel values) into frequency domain data. After DCT we get 64 coefficients. The first coefficient is called DC coefficient, and it represents the average color. The remaining coefficients are called AC coefficients and represent the detail information (AC components) at various frequencies.

4.1.2 Quantization

Quantization results in data loss but also contributes to The 8 x 8 DCT block is divided by quantization tables i.e. Each DCT coefficient is divided by a corresponding value in a quantization table and rounded to the nearest integer. JPEG standard includes optimized or default quantization tables which are optimal for most of the images. However, the JPEG standard doesn't impose restriction to use the default quantization tables. Hence the quantization tables are stored in JPEG image header.

4.1.3 Entropy Coding

Last step in JPEG compression is Entropy coding. Huffman coding is utilized to further compresses the quantized DCT coefficients by eliminating redundancies. The quantized coefficients (as received from above mentioned step) are first converted into a one-dimensional zigzag sequence, which groups low-frequency coefficients (more important for visual quality) at the beginning and high-frequency coefficients (less important) at the

end. Huffman coding is then applied to this sequence, using variable-length codes for different frequencies of occurrence to achieve compression. Symbols that occur more frequently are assigned shorter codes. Similar to quantization tables, Huffman tables can vary from one image to another and are also stored in image header.

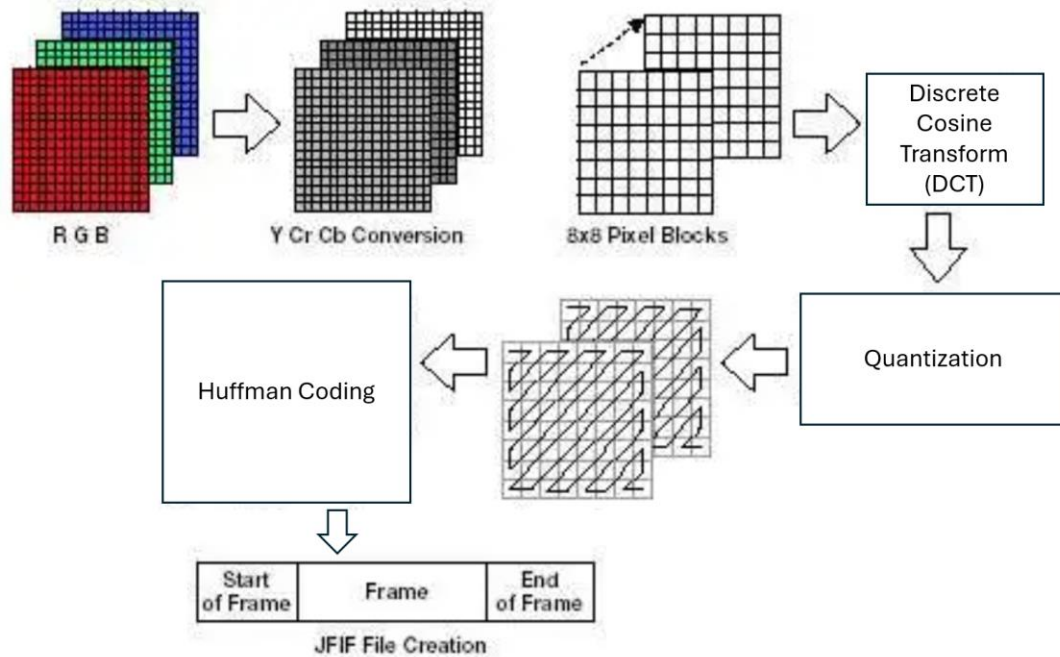


Figure 5: Baseline JPEG Compression Process [17]

4.2 JPEG File Format

A JPEG file is composed of segments. Segments are separated by markers. The markers ensure proper interpretation of the image data. A marker is 2 bytes long. Out of the two bytes, the first byte is set to 0xFF, while the second byte varies and thus it identifies what the marker contains. Certain markers may repeat in a JPEG file. SOI (Start of Image) marker, represented by 0xFFD8, signifies the beginning of the JPEG file and is mandatory

1st marker of every JPEG file. Similarly End of Image (EOI) is marked by 0xFFD9. Define Quantization Table (DQT) defines the quantization tables used in the image compression process. As mentioned above, Quantization tables determine how much compression is applied to different parts of the image. Start of Scan (SOS) 0x FFDA marks the beginning of image data and contains the compressed image bitstream. Nevertheless, for the purpose of research, Define Huffman Table (DHT) marker is specifically worth mentioning.

4.2.1 Define Huffman Table Marker

The Define Huffman Table (DHT) marker specifies one or more Huffman coding tables used during the entropy coding phase of JPEG compression. It is identified by 0xFFC4. Each Huffman table maps symbols (which represent lengths of zero runs followed by non-zero DCT coefficient values) to specific binary codes. The number of DHT markers may vary from image to image.

The DHT may vary from image to image. Specifically for optimized images, the DHT of every image is different from each other. The structure of DHT is as following:

Marker: 0xFFC4

Length: 2 bytes indicating the length of the segment

Table Class and Identifier: 1 byte where the first 4 bits indicate the table class (0 for DC, 1 for AC) and the last 4 bits define the table number (0-3)

Bit-lengths: 16 bytes representing the number of codes for each possible code length (1 to 16 bits)

Symbols: A list of symbols, with each symbol corresponding to a specific Huffman code length. It contains the actual Huffman table.

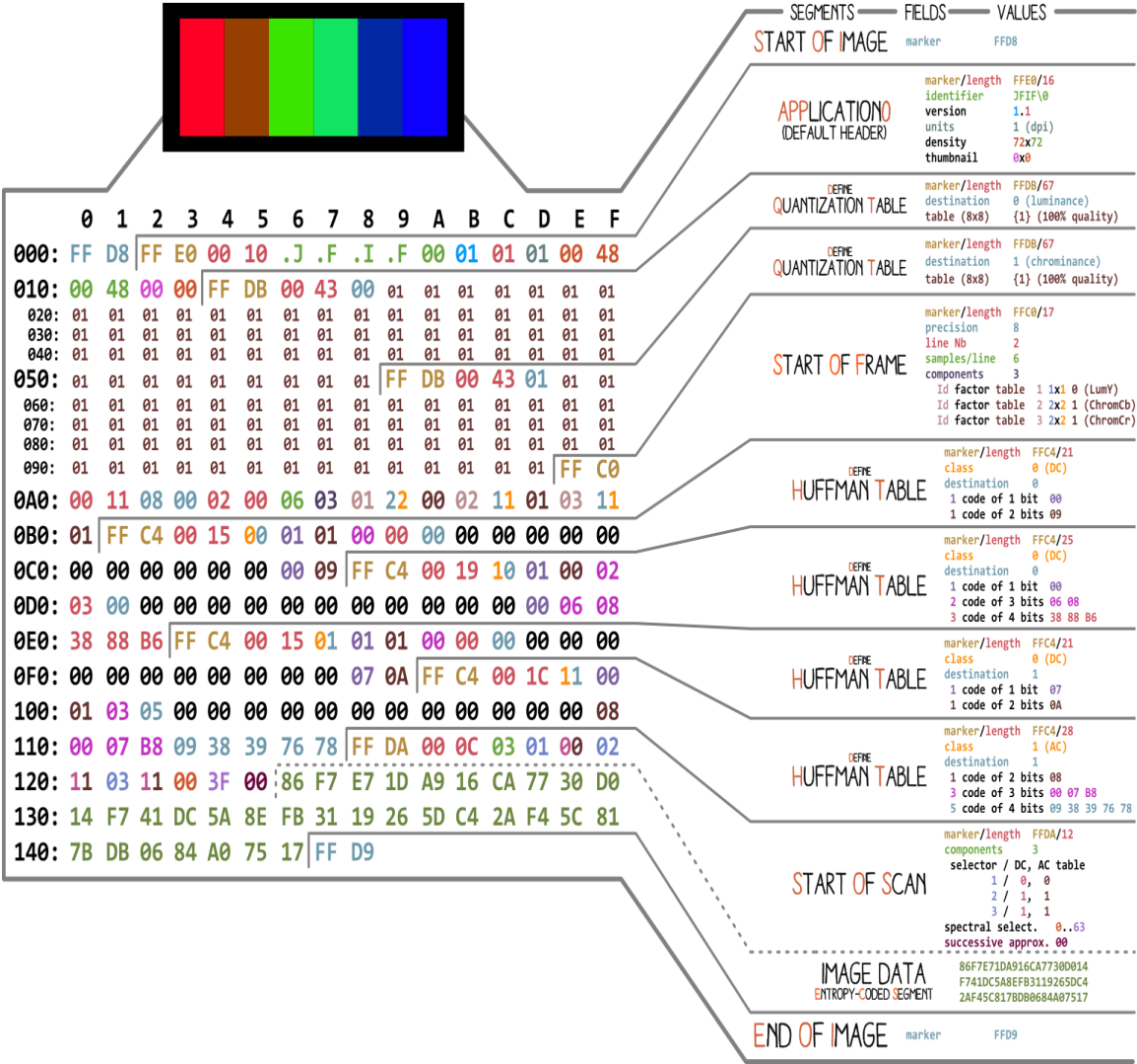


Figure 6: JPEG File Structure [11]

4.2.2 *JPEG Reading in Bit Format*

For viewing JPEG files, one may use any standard application or software. However, for the purpose of this research, a more technical approach was necessary. Hence, JPEG files had been studied in hexadecimal format which reveals the underlying data structure of the file.

It facilitates reading header information which is otherwise oblivious in photo viewers. Software “Hex Editor Neo” has been used for analyzing header information. It is a robust tool designed specifically for viewing and editing hexadecimal data, making it an ideal choice for inspecting the intricate details of JPEG file headers.

4.3 Decoding JPEG

The decoding process is reverse of the compression steps. Starting from decoding the entropy-coded data, to dequantization, to inverse DCT, to reassembling of 8 x 8 blocks and finally conversion from YCbCr color space back to the RGB color space for display. Few important things to note in decompression – specifically with regards to DHT marker are:

- The information to decode a JPEG image is included in the header of JPEG. Generally, the size of header is less than 3 KBs
- The integrity of information contained in DHT (Define Huffman Table) Segment is important. Even 1 bit change in DHT table renders the image un-readable.
- The DHT marker defines how the compressed data should be interpreted during the decompression process. However, it doesn't contain the actual image data. Hence, data contained in DHT can't be used to re-construct an image. In other words,

Huffman table is the summary of an image. It contains the overall information of an image. Without the actual image data and other vital information contained in the segments of JPEG, the DHT marker alone cannot be used to reconstruct the image.

- Generally, JPEG files often use standard Huffman tables which are predefined by the JPEG specification. Standard Huffman tables work reasonably well for a variety of images but are not tailored to the specific characteristics of the individual image being compressed. However, standard Huffman tables can speed up the encoding process because the tables do not need to be generated or optimized during compression.
- In optimized JPEGs, the Huffman tables are generated specifically for the image being compressed. Optimization process involves analyzing the frequency of the quantized DCT coefficients in the image and creating Huffman tables that are tailored to these frequencies. Optimized Huffman tables result in more efficient compression but require additional computational effort during the compression process.
- JPEG image optimization may include many steps like generation of custom Huffman tables, reducing the sampling ratio, using customized quantization tables etc. For the purpose of this research optimized JPEG images are defined as those images which employ custom Huffman table for each image. Other optimization steps may or may not be present.

An overview of the JPEG compression process and the advantages embedded in the standard is given in this chapter. Readers are encouraged to read [20] for thorough understanding of the standard. Moreover, a series on JPEG encoder/ decoder [21] is also found very helpful in understanding.

CHAPTER 5: PROPOSED SYSTEM

In this Chapter we will dwell upon our proposal. After giving details on prerequisites, and brief overview, we have explained our encryption methodology, feature extraction and image retrieval . Roles of each entity of the proposed system i.e. Cloud, Image owners and Cloud users are also covered in this chapter.

Our proposed model is similar to Encrypt and Feature Extract schemes. Image owner encrypts the images and uploads them to the cloud. All subsequent tasks (Feature Extraction, Similarity measure etc) are performed by the Cloud.

5.1 Prerequisites

It is important to note that our proposed scheme is applicable to optimized JPEG images. It is assumed that the cloud users have optimized JPEG images. If not, then there are two scenarios i.e. user has JPEG images or user has images in any other format than JPEG. In both the cases, the first step will be to convert these images into optimized JPEG images.

For the purpose of this research, we have used Radical Image Optimization Tool (RIOT) [12]. RIOT is a free, user-friendly program that offers a variety of optimization options to enhance JPEG images. This tool is particularly effective because it allows users to fine-tune compression settings, adjust image quality, and strip unnecessary metadata, all of which contribute to reducing file sizes while maintaining acceptable image quality. Moreover, the feature of batch processing is also available.

One incidental advantage of optimizing JPEG images is that users can significantly reduce file sizes without noticeable loss in image quality. Optimizing a JPEG or generating an optimized JPEG from RGB file is a bit more in processing requirements. It is because it scans the image data twice. After the first scan it generates the optimized Huffman table which is used to create image data. However, in present scenarios, challenges to cloud storage and data transfer (which is directly proportional to file sizes) are more pronounced than processing speeds. Hence the proposed system offers an incidental advantage of reduction in file sizes which is a crucial requirement in today's environment.

5.2 Overview of The Proposed Scheme

The proposed scheme consists of two ends i.e. cloud and cloud user. Cloud users comprise of query users and content owners. Query user and content owner can be same. Each end has its own defined responsibilities. This setting is more practical than proposing a model with three entities i.e. Cloud, Content Owner and Query User. In our scheme, the user end can incorporate any number of content owner and query users as per the cloud environment.

As an initial step, the content owner encrypts, and uploads encrypted images to the cloud. The content owner has the liberty to use any encryption scheme as per the threat modeling or security requirements. The content owner also has the liberty to use different encryption scheme for different categories of images.

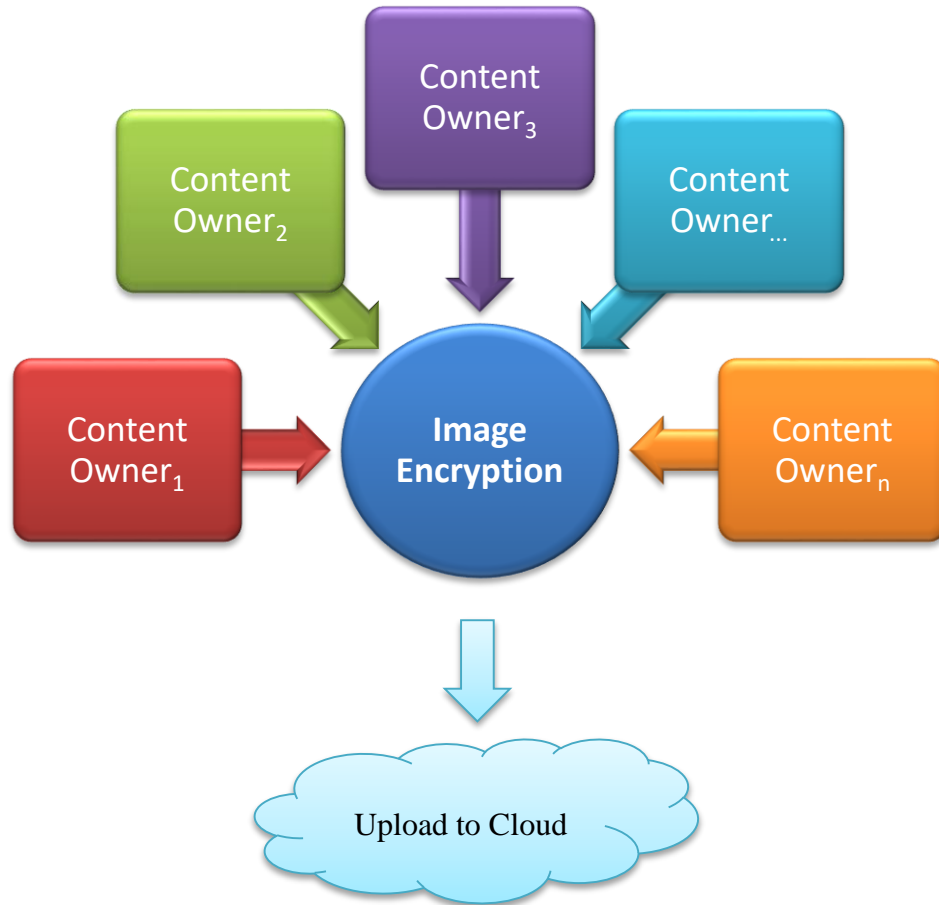


Figure 7: Content Owner(s) in Proposed Scheme

For retrieving similar images, the query user uploads the encrypted query image to the cloud. It must be noted that the encryption scheme of query image and encrypted images database can be different i.e there is no binding in our proposed model to follow same encryption scheme. The cloud performs similarity search and returns similar encrypted images to the query user. The query user, upon receiving the encrypted similar images, decrypts the images.

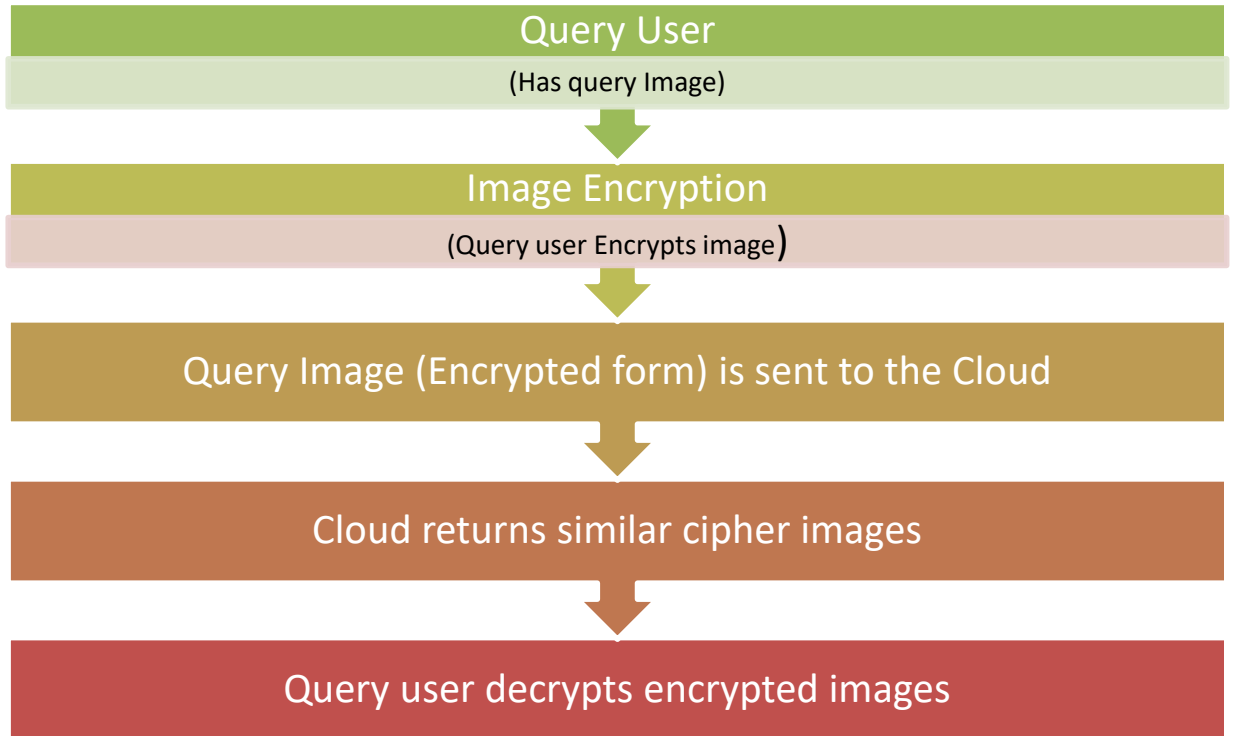


Figure 8: Query User(s) in Proposed Scheme

5.3 Segmented Encryption

One of the main differences lies in our proposed scheme lies in encryption. Instead of complete or partial encryption, *Segmented Encryption* has been proposed. The concept of Segmented Encryption is scarcely found in literature and is not standardized [5], [24] and it has not been defined as such. Therefore, it is imperative to standardize the definition of Segmented Encryption. Segmented Encryption means encrypting segments of a file. The segments need to be already present in the file as defined by the file format. Segments should not be confused with chunks.

As already mentioned, for retrieval tasks, some form of features are required. In previous schemes, some authors have employed partial encryption e.g. to encrypt the AC coefficients of JPEG while leaving the DC coefficients un-encrypted. Such partial encryption is generally more time consuming.

Our research leverages upon the already established segments of JPEG file. For the purpose of this research, Segmented Encryption means encrypting the segments. We have encrypted the image data segment of JPEG file, while leaving the other segments unencrypted. Image data starts with FFDA marker. Post FFDA marker, all data is encrypted.

Figure 9: Encrypted vs Un-encrypted shows a JPEG file in hexadecimal form. It gives an approximate visual depiction on how much portion of JPEG data will be encrypted or otherwise. Hexadecimal values in red will be encrypted while values in black and highlighted in yellow will not be encrypted. The depiction is based upon the images of Corel 1k dataset. It is pertinent to note that once the file size increases, the ratio of encrypted portion will increase because the header size generally remains below 500 Bytes.

Algorithm 1. Image Encryption

Input: Original Image I and Key K

Output: Cipher Image C

1. Read original image in binary mode.
2. Pad the data as per requirement of encryption primitive.
3. Find the start and end markers.
4. Encrypt the image data between the markers with Key K
5. Construct Cipher image by combining the original data up to the start marker and the encrypted data.

RETURN Cipher Image C

It is pertinent to mention here that key management (Key generation, storage, life, post life etc) is an important area in any cryptographic implementation. Same is not under the purview of this research but must be given due attention, so as to avoid any false sense of security.

5.4 Feature Extraction

This task is performed by the Cloud. The cloud has all the images in encrypted form. Since we have used segmented encryption, hence the data in Huffman tables is intact and can be used as a feature. Huffman table of each image is extracted to create an index. Features are Huffman tables and length of Huffman tables.

Algorithm 3. Feature Extraction

Input: Cipher Images C

Output: Feature Vector

1. Read Cipher Images C in binary mode.
2. Find the DHT (\backslash xFFC4) markers.
3. Read DHT data as vector

RETURN Feature Vector

5.5 Image Retrieval

The query user encrypts the image and sends the query to the cloud. Choice of encryption primitive lies with the query user. Process of encryption should follow requirements of segmented encryption. Upon receipt of an encrypted image, the cloud extracts Huffman tables from the encrypted image. Extracted Huffman table is given as an input to the trained model. The model outputs the similar images which are sent to the query user. Decryption is performed at query user end.

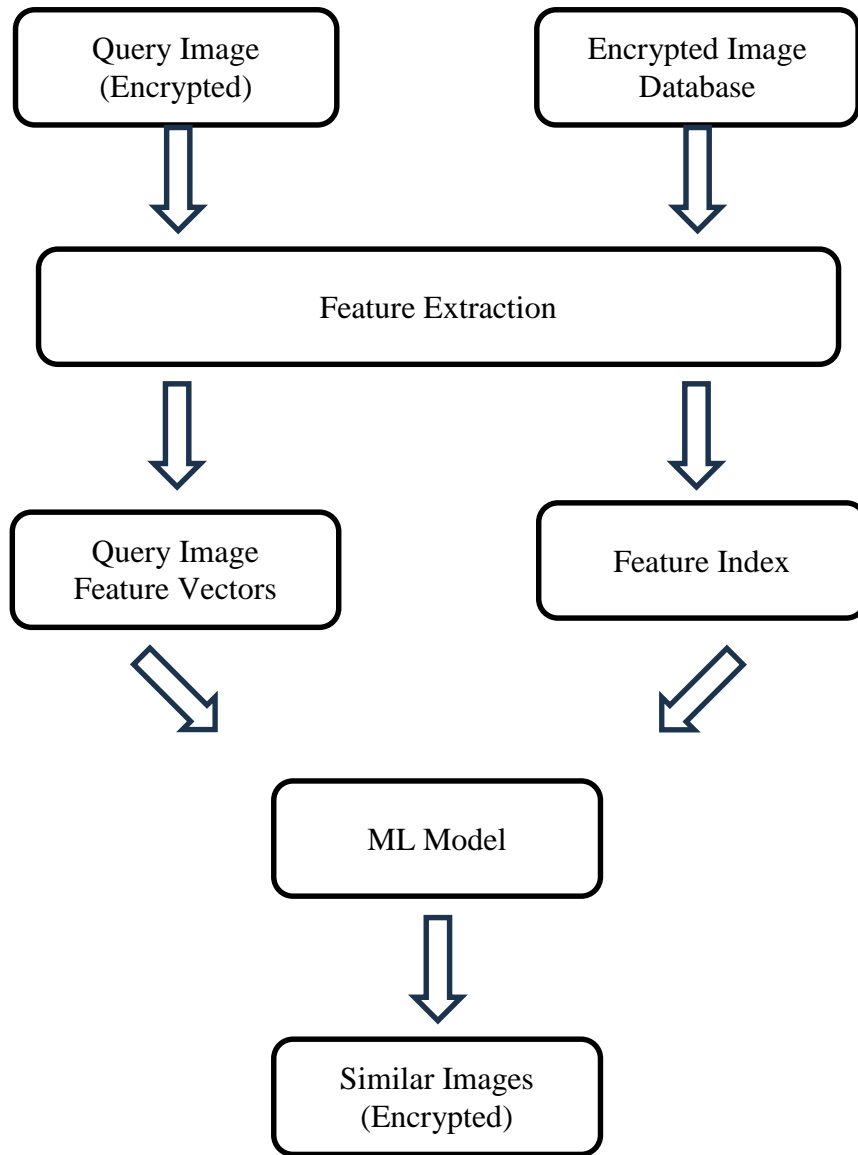


Figure 10: Cloud in Proposed Scheme

We have employed machine learning for similarity search. Various supervised and unsupervised models have been tested. Results of K-means in unsupervised domain and

Multi-layer Perceptron (MLP) classifier in supervised domain have been found the best ones which will be explained further in next chapter.

In this chapter we have gone through the contours of our proposal. Roles and tasks of each entity and how each entity will accomplish it's assigned task were covered. In next chapter, we will move towards demonstration part through experimentation on Corel 1k dataset.

CHAPTER 6: EXPERIMENTATION & RESULTS

This chapter is about implementation of the proposed scheme and subsequent evaluation on Corel 1k dataset. In the beginning, test environment is explained, then the chapter covers details on experiments performed followed by best results achieved.

Corel 1k dataset is used for experimentation. It is used for experimentation in various image retrieval literature. Corel 1k dataset has 1,000 images divided into 10 classes. The dataset is balanced with 100 images in each class. The 10 classes include :

1. Beaches
2. Buses
3. Dinosaurs
4. Elephant
5. Flowers
6. Foods
7. Horses
8. Monuments
9. Mountains and snow and
10. People and villages.

Implementation of the proposed scheme is performed on following

Language	Python 3.1
Operating System	Windows 10
OS Type	64 Bits
System Specifications	12th Gen Intel(R) Core(TM) i5-1235U,1.30 GHz CPU, 8 GB RAM

It is also pertinent to mention here that Corel 1k dataset uses default huffman tables. Since optimized JPEG is a prerequisite in our proposed scheme, the first step was converting the images into optimized images. RIOT software has been used for converting the images into optimized images. All subsequent tests have been performed on optimized Corel 1k dataset.

6.1 Experimentation

6.1.1 Feature Engineering

Feature engineering is imperative for machine learning. In feature engineering, the first step is to understand the dataset. We need to identify the uniqueness of our features. Our research was unique in sense that, unlike normal machine learning problems, we did not have huge set of features available. We had one long feature – the huffman table. Extracted length of huffman table varied from 266 Bytes to 378 Bytes.

Various steps have been performed to improve upon the model which are explained in succeeding paragraphs.

Initial 2 bytes of Huffman code are length of Huffman table. This value was utilized to make a new feature i.e. “length”. However, addition of “length” did not improve the results and thus was discarded as a feature.

Another option explored was to standardize the length of Huffman table. Variable length of Huffman table was truncated to minimum length by discarding the head or the tail. This resulted in the generation of two new features i.e. “trunc_head” and “trunc_tail”. During model training phase, it was observed that feature “trunc_head” performed better than “trunc_tail” or original Huffman table.

Since Huffman table contained long strings of hexadecimal value, hence in yet another attempt, the hexadecimal values were treated as words for n-grams model. This also did not prove to be helpful.

6.1.2 Model Selection

Owing to uniqueness of our feature, various supervised and un-supervised machine learning models have been tried. We have used sklearn framework in Google Colab. In un-supervised domain K-means, Gaussian Mixture Model, Spectral clustering, Bigram clustering etc have been applied. Results of K-means have been found superior to all other in terms of mean average precision (mAP).

In supervised domain, models tried included Random forest, Support Vector Machine, Extreme Gradient Boosting classifier (XGBoost) and Multi Layer Perceptron

(MLP) classifier. Results of MLP have been found superior to all other in terms of mean average precision (mAP).

6.2 Performance

6.2.1 Encryption Performance

Next step was to perform segmented encryption on Corel 1k dataset. Although the user is at liberty to use any encryption scheme, but for the purpose of experimentation, we have applied segmented encryption incorporating AES[22] and triple DES [23]. AES has been selected as it is NIST approved and globally tested. Tripple DES is legacy and can still be found in many applications. Encryption time of each is shown in Table 3:

Encryption Time

Table 3: Encryption Time

	Encryption Time (Seconds)			
	AES – 128	AES – 192	AES – 256	Tripple DES
Time	0.54	0.57	0.58	1.47

6.2.2 Feature Extraction

Features are extracted from encrypted images by the cloud. The cloud extracts the feature and generates an index. The system took 3.01 seconds to extract the features.

6.2.3 Retrieval Performance

In line with previous research, Mean Average Precision (mAP) has been used [13] to evaluate the retrieval performance of the proposed scheme. Higher mAP means better retrieval performance and vice versa. mAP of both the trained models are given in Table 4: Retrieval Performance.

6.2.4 Retrieval Efficiency

Search time is used to measure the efficiency of the proposed scheme. Search time of both the trained models are given in Table 4: Retrieval Performance.

Table 4: Retrieval Performance

	K-Means (Un-supervised)	MLP (Supervised)
mAP	0.201	0.284
Time (ms)	1.1	0.45

Confusion Matrix for both of the trained models is as shown in following figure. Horizontal lable are the actual classes while vertical label are the predicted classes. The classes are in alphabetical order i.e starting from beaches, buses and so on. Classification of entire dataset in K-Means are shown, while for MLP, test results on 30 % test set are shown.

```

[[13  1 11 16 14  3 18 14  2  8]
 [ 0 83  0  2  0 15  0  0  0  0]
 [15  0 12  1  9  0 14 23  6 20]
 [26  0 12  1  6  0 20 22  1 12]
 [22  0  7  5 15  1 27 11  2 10]
 [ 1  7  0 36  7 46  1  0  0  2]
 [16  0  2 16 22  5  8 16  0 15]
 [12  3  4 28 14 15  8  3  0 13]
 [ 7  0 24  4  3  1 10 14 28  9]
 [11  0  7 21 31  5  5  8  0 12]]

```

Figure 11 : Confusion Matrix (K-Means)

```

[[ 1  0  1  2  2  3  0  2  6  5]
 [ 0 27  0  0  0  0  0  1  0  1]
 [ 0  0 11  0  0  0  0  3  2  0]
 [ 0  0  0  6  1  1  3  1  3  3]
 [ 0  0  1  0 12  1  2  2  2  2]
 [ 1  0  2  0  1 10  2  1  1  3]
 [ 0  1  0  2  2  2  7  0  1  3]
 [ 0  0  1  1  1  2  0  5  3  3]
 [ 1  0  3  3  2  0  1  2  5  1]
 [ 0  0  0  2  1  1  2  3  0 11]]

```

Figure 12: Confusion Matrix (MLP)

6.3 Security

6.3.1 Security of Image Data

The image data is encrypted as per security needs of the user. The user is independent to choose the encryption scheme. Hence the proposed scheme can fall in any category from Cipher text Only Attack (COA) to Chosen Cipher text Attack (CCA) depending on the employed encryption scheme.

6.3.2 Security of JPEG Segments Less Image Data

This is the unencrypted part which is used for similarity check. As depicted in Figure 9: Encrypted vs Un-encrypted Depiction (Yellow highlighted is unencrypted part) the unencrypted portion is very less. An attacker can't decode image data even if it can get the Huffman tables. Huffman tables contain the codes which are required to decode the data in image data segment. Unlike ASCII code, Huffman codes vary from image to image. A typical Corel 1k image contains around 25,000 Bytes. Whereas Huffman table is around 160 bytes. Hence it can be safely concluded that Huffman tables alone doesn't lead to breach of confidentiality of image data.

6.3.3 Information Leakage

Image header, similarity pattern and the access pattern are included in the information leaked to the cloud. Similarity pattern means that the cloud server knows which images are similar to each other. Moreover, the cloud server knows which images are returned to the image owner in every search. This is called the access pattern. The leakage of the similarity pattern and the access pattern are the common trade-offs to efficient search in searchable encryption schemes. Hiding similarity and access patterns falls in category of privacy preserving schemes which is beyond the scope of this research.

6.4 Analysis

The requirements mentioned in 1.3.1 Design Goals and Security Goals have been met in the proposed system. The system does not impose any restrictions on choice of encryption module. Encryption scheme of query image and images in database can be different. The system supports multi-owner multi-user settings and also supports adaptive key.

Furthermore, upon doing critical analysis of the proposed scheme it is revealed that amongst the three requirements of S-CBIR scheme as mentioned in Figure 2: S-CBIR Requirements, query effectiveness (measured by Map) is on the lower side. The reason lies in feature selection.

Features can be categorized in two forms i.e. Global features and local features. Global features are holistic in nature and gives information on overall content of the image. Local features contain information on image content. Local features are generally derived from small patches or regions of an image. Local features are designed to be invariant to changes in illumination, viewpoint, and other factors that can affect the image's appearance. In general, high mAP is achieved with local features.

Huffman tables are global features. As they contain information on the overall content of the image. Since, our scheme is using Huffman tables, hence mAP is comparatively lower than the schemes which are employing local features. Ways and means to improve mAP and other aspects are covered in last chapter.

In this chapter we have tested our proposed concept on Corel 1k dataset. Experimentation results validate the concept of our proposed scheme. Further we will give the summary of the research followed by future work recommendations.

SUMMARY OF RESEARCH WORK

Image retrieval systems play a critical role in enabling users to browse and search huge image databases in real-time. Over the years, various techniques have been developed to increase the effectiveness and efficiency of image retrieval systems. One of the major areas, i.e. content-based image retrieval (CBIR) has gained significant attention. CBIR is a technique that searches and retrieves images based on their visual content, rather than based upon text-based queries. This method is an alternate to text-based query and it uses features such as color, texture, and shape to find similar images.

With the advent of encryption, Secure content-based image retrieval (S-CBIR) has emerged. It takes the CBIR concept a step further by focusing on retrieving similar images from encrypted image datasets. In today's digital era, where privacy and security are paramount, SCBIR provides a means to ensure that images can be securely stored and accessed, thus giving minimal effect on usability. Various SCBIR schemes have been developed, typically involving the encryption of images followed by feature extraction. However, these schemes often fall short on in one critical aspect i.e. the flexibility and robustness of the encryption methods used. None of the existing schemes employ NIST-approved or globally accepted encryption standards, and they do not allow users the freedom to choose their preferred encryption methods. This limitation is particularly of concern in a multi-user environment of cloud, where different users may have varying security requirements.

To address these challenges, our research proposes a novel concept that gives users the independence to choose any encryption primitive as per their security needs. Our approach

is applicable to optimized JPEG images. Our system employs segmented encryption, focusing on encrypting the data segment of JPEG images. This method not only ensures robust security but also maintains the efficiency of image retrieval processes. Additionally, Huffman tables extracted from the encrypted images are utilized for retrieval tasks, leveraging machine learning techniques in both supervised and unsupervised domains.

Experimental results demonstrate that our proposed scheme excels in terms of performance and efficiency. By allowing users to choose their encryption methods, our system provides a flexible and secure solution for image retrieval in cloud environments. The use of segmented encryption and advanced machine learning techniques ensures that the retrieval process remains accurate and efficient, even when dealing with encrypted image data. This research represents a significant advancement in the field of secure content-based image retrieval, offering a practical solution that balances security and usability in real-world applications.

CHAPTER 7: CONCLUSIONS AND FUTURE RECOMMENDATION

7.1 Conclusion

Cloud is a multi –user, multi-owner environment which thrives on the liberty which it provides to its users. One of the major challenges in domain of S-CBIR was lack of independence with regards to choice of Encryption scheme. In all of the existing Encrypt and extract features S-CBIR schemes, the content owners are forced to use the novel encryption schemes proposed by researchers. Owner of sensitive data may not trust a newly developed encryption primitive.

Our proposed scheme is a step towards practical implementation of S-CBIR in real world scenarios. We have developed an Encrypt and Feature Extract CBIR system which gives the users the liberty to use any encryption primitive / scheme. This also provides improved confidentiality for the image data.

Proof of concept is given by implementing the proposed scheme on Corel 1k dataset in Python. Satisfactory results have been achieved on time to encrypt, feature extraction time and mAP. mAP is on the lower side, in comparison with existing schemes. This is due to use of global features only. However, the advantage of liberty in encryption outweighs slightly less mAP.

The proposed scheme is applicable to optimized JPEG images only. This is a limitation but also an advantage since, optimized JPEGs are lesser in size and hence storage efficient.

7.2 Future Work

As mentioned above, the proposed scheme is applicable to optimized JPEG and has slightly lesser mAP. In future we intend to improve upon these aspects.

- It is intended to improve mAP of proposed scheme by incorporating specifically designed deep learning algorithms.
- Expanding the proposed scheme to other categories of images. This involves identifying the segments of image which can be used as feature, evaluating it's security implications and implementing the proposal.
- Proposed scheme may also be tested on real world scenarios, where security needs are high and varying e.g health care or military images database etc.

REFERENCES

- [1] Cheng H, Zhang X, Yu J, Zhang Y. Encrypted JPEG image retrieval using block-wise feature comparison. *Journal of Visual Communication and Image Representation*. 2016 Oct 1;40:111-7.
- [2] Cheng H, Zhang X, Yu J, Li F. Markov process-based retrieval for encrypted JPEG images. *EURASIP Journal on Information Security*. 2016 Dec;2016:1-9.
- [3] Li P, Situ Z. Encrypted jpeg image retrieval using histograms of transformed coefficients. In2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2019 Nov 18 (pp. 1140-1144). IEEE.
- [4] Wang H, Xia Z, Fei J, Xiao F. An AES-based secure image retrieval scheme using random mapping and BOW in cloud computing. *IEEE Access*. 2020 Mar 25;8:61138-47.
- [5] Feng Q, Li P, Lu Z, Li C, Wang Z, Liu Z, Duan C, Huang F, Weng J. Evit: Privacy-preserving image retrieval via encrypted vision transformer in cloud computing. *IEEE Transactions on Circuits and Systems for Video Technology*. 2024 Feb 26.
- [6] Lu Z, Feng Q, Li P. Encrypted JPEG Image Retrieval via Huffman-code Based Self-Attention Networks. In2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2022 Nov 7 (pp. 1-6). IEEE.
- [7] Yu P, Tang J, Xia Z, Li Z, Weng J. A privacy-preserving JPEG image retrieval scheme using the local Markov feature and bag-of-words model in cloud computing. *IEEE Transactions on Cloud Computing*. 2023 Jan 2.
- [8] Liang H, Zhang X, Cheng H. Huffman-code based retrieval for encrypted JPEG images. *Journal of Visual Communication and Image Representation*. 2019 May 1;61:149-56.

- [9] Anju J, Shreelekshmi R. PCBIR-CV: A privacy-preserved content-based image retrieval using combined visual descriptors for cloud. *Software Impacts*. 2023 Sep 1;17:100529.
- [10] Zhang, Q., Wang, Z., Hu, X., & Chen, R. (2023, August). A Content-Based Image Retrieval Scheme for Encrypted Domain Using Feature Fusion Deep Supervised Hash. In 2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE) (pp. 34-39). IEEE.
- [11] Corkami. (n.d.). formats/image/JPEGRGB_dissected.png at master · corkami/formats.GitHub.https://github.com/corkami/formats/blob/master/image/JPEGRGB_dissected.png
- [12] SABO, L. (2021, January). Radical Image Optimization Tool. *RIOT*. Retrieved July 13, 2024, from <https://riot-optimizer.com/>
- [13] H. Schütze, C. D. Manning, and P. Raghavan, Introduction to information retrieval. Cambridge University Press Cambridge, 2008, vol. 39.
- [14] Baeldung. (n.d.). Content-Based Image Retrieval (CBIR) vs. Text-Based Image Retrieval (TBIR). Baeldung. Retrieved July 15, 2024, from <https://www.baeldung.com/cs/cbir-tbir>
- [15] Ravani, R., Baniasadi, M., & Mirali, M. (2010). A Concurrent Approach to Content-Based Image Retrieval using Color Coherency. In *IPCV* (pp. 462-465).
- [16] Z. Xia, L. Jiang, D. Liu, L. Lu and B. Jeon, "BOEW: A Content-Based Image Retrieval Scheme Using Bag-of-Encrypted-Words in Cloud Computing," in *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 202-214, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2927215.
- [17] EE Times. (January 23, 2003.). Baseline JPEG Compression Juggles Image Quality and Size. EE Times. Retrieved July 15, 2024, from <https://www.eetimes.com/baseline-jpeg-compression-juggles-image-quality-and-size/>

- [18] Hudson, G., Léger, A., Niss, B., Sebestyén, I., & Vaaben, J. (2018). JPEG-1 standard 25 years: past, present, and future reasons for a success. *Journal of Electronic Imaging*, 27(4), 040901-040901.
- [19] Hudson, G., Léger, A., Niss, B., & Sebestyén, I. (2017). JPEG at 25: Still going strong. *IEEE MultiMedia*, 24(2), 96-103.
- [20] Pennebaker, W. B., & Mitchell, J. L. (1992). *JPEG: Still image data compression standard*. Springer Science & Business Media.
- [21] Harding, D. (2018, September). *Everything you need to know about JPEG*. [Video]. YouTube.https://www.youtube.com/watch?v=CPT4FSkFUgs&list=PLpsTn9TA_Q8VMDyOPrDKmSJYt1DLgDZU4
- [22] Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael.
- [23] Merkle, R., & Hellman, M. (1981). On the security of multiple encryption. *Communications of the ACM*, 24(7), 465–467.
- [24] Man, Z., Li, J., Di, X., & Bai, O. (2019). An image segmentation encryption algorithm based on hybrid chaotic system. *IEEE access*, 7, 103047-103058.
- [25] Xie, L., Hong, R., Zhang, B., & Tian, Q. (2015, June). Image classification and retrieval are one. In *Proceedings of the 5th ACM on International Conference on Multimedia Retrieval* (pp. 3-10).