EasyChair Preprint

№ 9037

Content-Based Secure Image Retrieval in an Untrusted Third Party Environment

Sandeep Singh Sengar and Sumit Kumar

October 11, 2022

Content-Based Secure Image Retrieval in an Untrusted Third Party Environment

Sandeep Singh Sengar and Sumit Kumar

Abstract In this digital world, where availability of the image-generating tools is quite common and owing to the rapid growth of internet knowledge; people use to exchange massive volume of images every day which results in creating large image repositories. So, retrieving appropriate image available on these repositories is one of the vital tasks. This problem leads to evolving content-based image retrieval (CBIR). As the generation of image increases, people start transferring these images to a remote third-party server, but these images may have personal information. This leads to adding privacy concerns toward the system as transferring personal data to some other place might be a cause of leakage of information or transfer to an unauthorized person. So, to keep this in mind, sensitive images like medical and personal images require encryption before being a contracted out for the privacy-preserving resolutions. In this work, we have deployed ACM for image encryption as well as Asymmetric Scalar Product Preserving Encryption (ASPE) for feature vector encryption and similarity matching. We have demonstrated our results based on various benchmark databases.

1 Introduction

In this section, background, aim and motivation of this work have been elaborated.

Sandeep Singh Sengar
Department of Computer Science, Cardiff Metropolitan University, Cardiff, United Kingdom, e-mail: SSSengar@cardiffmet.ac.uk

Sumit Kumar
Dept. of Informatics Cluster, School of Computer Science, University of Petroleum and Energy Studies, Dehradun-248007, Uttarakhand, India e-mail: sumitvarshney68@gmail.com

1.1 Background

Nowadays, knowledge has developed progressively advanced. This leads to cheap and cutting-edge multimedia devices and has given rise to vast data volumes of multimedia content. Vast data volumes of multimedia consist of audio, video, images etc. Today billions of images are uploaded and downloaded which is creating large amount of data [1, 2, 3]. This large amount of data needs to be stored in the database for several requests such as medical, crime prevention, security, etc.

These solicitations have generated a necessity for effective, secure and efficient ways of storage, search and image retrieval via similar processing procedures. We share images with each other and also publish them for instance on the Internet. Those image collections are important contributors to the public domain of the Internet which is of billions of images. Private image collections or images on the Internet might be the most obvious example, but the use of digital imaging has spread too many application areas.

Modern hospitals are one of the best examples, in which large collections of medical images are succeeded, stored and used every day. Newspapers, image providers, and other firms in the graphic design trade uses digital images in their workflow and databases. One more example is of security industry in which surveillance cameras produces large amount of images. Suppose an institute has advanced a novel face recognition algorithm. The institute will wish that those input images and images present in their database are not revealed publicly or advertise by chance. Another example, we can take of Clinicians who can use CBIR [4, 5] to find the similar cases of patients and facilitate the clinical decision-making processes. The patients may or may not want to reveal their medical images to any other except a particular doctor in medical CBIR applications whether physically or electronically. Therefore, we effort to find a solution to secure storage and image retrieval byway that such goal can be achieved.

Previously, the images were kept with linked labels or thread and search were accomplished on the ground of these labels. Since applying thread to an individual image is a very time-consuming task and also it incorporates human perception about each image. It has been seen very frequently that different human being can perceive different images differently which could result in either getting the wrongly matched image or leave correctly associated images. Another aspect which makes this process unrealistic is today every process is time-dependent i.e. we need to design a system which could produce the result within a particular time-bound and this is not possible which earlier process with such huge volumes of multimedia repositories. Nowadays, with extensive reach of social networks and multimedia tools like digital camera, mobile phones etc., and users became a lot of involved concerning their secrecy and their information kept on servers. Some users even choose to hide their details from database administrator.If stored information on the server is seen by database admin, a user's privacy may be on the urge of breaching if the database or server administrator is faulty and the chances of misusing of this information increase. If an organization's employee details are stored on a server along with their photographs for face recognition, the organization prefers to keep this information out of reach

of any other user or database admin. If this information is not hidden perfectly, a compromised database admin may be able to access them and use it for his/her own benefits, such a situation needs to be avoided. Therefore, going with this direction, it is very much clear that multimedia data security is one of the main concern of today's retrieval system.

1.2 Aim and Motivation

The first part of the paper will focus on image retrieval technique based on feature vector extraction method using both texture and shape feature. Second part will show how an image is securely encrypted at owner's end and decrypted at user side. The main idea is that the owner extract feature of an image, create an image feature vector database and create an encrypted image database and sends it to centralize database we assume the database admin to be honest but curious in nature. On the other hand, user also extract the desired features to form query image feature vector and sends it to the centralized database. In the centralized database the query processor will find similar encrypted images with the query image given by users and sends the result to user. At user end user decrypt images with the owner keys. The output is images with the most similar image in the database. The motivation for creating such a secure system is that the authorized image users can only retrieve the images he needs and database admin also can't breached the privacy of the owner image.

2 Preliminaries

In this section, we will demonstrate the various techniques that we have incorporated during the development of this work. They will be described under the various subsections as follows:

2.1 Local Binary Pattern (LBP)

LBP [6] is a kind of visual descriptor employed for grouping in PC vision. LBP is the specific case of the Surface Range illustration proposed in 1990. Since 1990, LBP has been observed to be an intense module for texture ordering. It has additionally been resolved that when LBP is joined to Histogram of oriented gradients (HOG) [7] descriptor, it add to the recognition performance remarkably on few datasets. A correlation of a few deviations of the first LBP in the arena of foundation subtraction was brought on 2015 by Silva et al. A complete study of the various executions of LBP can be found in Bouwmans et al. The LBP feature vector, in its most straightforward shape, is done in different way:

- Separate the analysed window into cells (e.g. 16x16 pixels for every cell)
- For every pixel in a cell, contrast the pixel with every one of its 8 neighbors (to its left side best, left-center, left-base, right-top, and so forth.). Take after the pixels along a circle, i.e. clockwise or counter-clockwise.
- Where the center pixel's value is taken if the center value is greater than the neighbor's value, express "0". Else, state "1". This results in 8-digit binary number (which is typically changed over to decimal gradually).
- Histogram is computed, over each cell value, of the recurrence of each "number" happening (i.e., every blend of which pixels are smaller and greater than the center). This histogram can be viewed as a 256-dimensional feature vector.
- Alternatively standardize the histogram.
- histograms of all cells which results in the form of feature vector for the whole window.

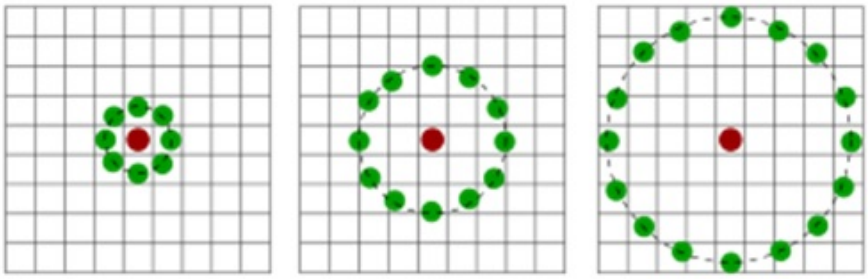

Fig. 1 Three neighborhood cases used to characterize a texture and LBP is calculated

2.2 Arnold Cat Map

In this section, Arnold Cat Map [8] is described in briefly which is used in the image encryption process. The ACM has wide application on image encryption process which is capable to confuse any square image significantly. According to the ACM, when an image undergoes chaotic transformation pixels of the original image get scrambled to some other random position. The ACM works on square image so in our proposed scheme we have used ACM on 128×128 blocks. The ACM process is performed as follows:
$\begin{bmatrix} u' \\ v' \end{bmatrix} = A \begin{bmatrix} u \\ v \end{bmatrix} where A = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}$ The ACM moves the intensity value presence at the co-ordinate (u, v) position to the co-ordinate (u', v') position. The parameters p and q may be considered as a secret key. The user can perform the inverse operation

with knowing
$\begin{bmatrix} u \\ v \end{bmatrix} = A^{-1} \begin{bmatrix} u' \\ v' \end{bmatrix}$ where $A^{-1} = \begin{bmatrix} 1 + pq & -p \\ -q & 1 \end{bmatrix}$

2.3 Asymmetric Scalar Product Preserving Encryption (ASPE)

ASPE [9] was recommended in deprive of any data structures use over encrypted data kNN activities were executed. Many techniques are being used by ASPE for encrypting database points and query point. Invertible matrix is used to encrypt the database points and similarly its inverted matrix to encrypt query points, it avoids attack centered on distance preservation among encrypted data and unencrypted data, henceforth escaping distance recovery. Two Feature vector given in DB i.e. f_{v1} and f_{v2}, their distance $d(f_{v1}, f_{v2})$ could be known from their encrypted values $E_T(f_{v1}, K)$and $E_T(f_{v2}, K)$ .These distance permit the attacker to figure signature and in this way signature connecting attack is done. To oppose these attacks, we require an encryption work that does not uncover distance information. For kNN seek, we watch that correct distance computation isn't fundamental. Or maybe, we just need a distance examination activity. Given two feature vector f_{v1} and f_{v2} in DB, we must choose which of the two feature vector of image is closer to the feature vector of query image i.e. f_{vq}.

- **Key:** a $(d + 1) \times (d + 1)$ invertible matrix M.
- **Feature vector encryption function** $E_T(\cdot)$: Considering a database feature vector f_v. Firstly, creating a feature vector $f_v = (f_v^T, -0.5||f_v||^2)^T$ of dimension $(d+1)$. Secondly, compute an encrypted feature vector $f_v^{'} = M^T f_v$.
- **Query Image feature vector encryption function** $E_q(\cdot)$: Considering a query image feature vector f_{vq}. Firstly, generating a random number $r > 0$. Secondly, creating a feature vector $f_{vq} = r(f_{vq}^T, 1)^T$ of dimension $(d + 1)$. Thirdly, the compute the encrypted query feature vector as $f_{vq}^{'} = M^{-1} f_{vq}$.
- **Distance comparison operator:** Let $f_{v1}^{'}$ and $f_{v2}^{'}$ be the encrypted feature vectors of f_{v1} and f_{v2}, respectively. To know whether the feature vector f_{v1} is nearer to query image feature vector f_{vq} than f_{v2}, we calculate $(f_{v1}^{'} - f_{v2}^{'}) \cdot f_{vq}^{'} > 0$, where $f_{vq}^{'}$ is the encrypted feature vector f_{vq}.
- **Decryption Function:** Considering an encrypted feature vector $f_v^{'}$. The feature vector $f_v = \pi_d M^{T^{-1}} f_v^{'}$, where π_d is a $d \times (d + 1)$ matrix and $\pi_d = (I_d, 0)$, where I_d is $d \times d$ identity matrix.

3 Proposed Work

CBIR is the efficient image retrieval technique but it lacks some security feature. Now, as the generation of image increases, one is not always keen to contain each and every image with oneself and image may contain some personal stuff or those images might be needful to someone at the various point of time so people use to transfer them to some centralized repository. Now, this leads to add privacy concern toward the system as transferring personal data to some other place might be a cause of leakage of information or transfer to not authorized person. Therefore we have proposed secure and efficient technique for image retrieval.

3.1 CBIR Based

Traditionally, searching of the images are utilizing content, labels or watchwords or comment allotted to the image while keeping it into the databases. While if the image which is kept into the databases are not remarkably or particularly labelled or wrongly depicted at that point it's deficient, relentless and to a great degree tedious use of CBIR process on the vast volume of pictures. This issue prompts the development of efficient CBIR process which is utilized for recovering the correct images from the database. In a CBIR system, user selects a query image and extracts its visual image features and combined them together to form the query image feature vector. Now, the same feature extraction process has been employed to each image of the respective database to form feature image database. Afterwards, using a similarity measurement technique query image feature vector is matched with every single feature vector of the feature database to receive some most similar images. This process has been depicted in the figure 3.1.

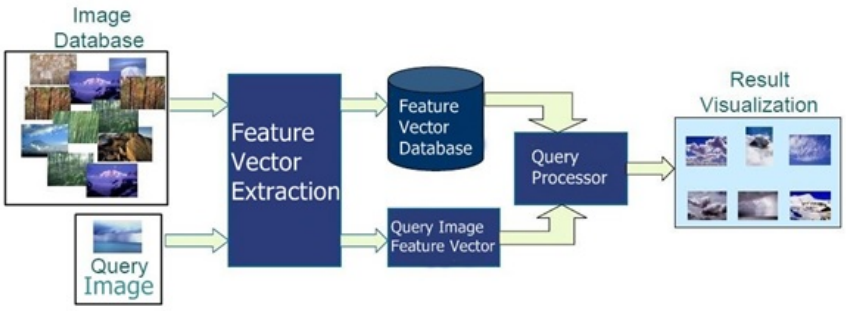

Fig. 2 Basic of Content-Based Image Retrieval

3.2 Image Encryption

As per Arnold's change, a picture is hit with the change that evidently randomizes the first association of its pixels. Be that as it may, if iterated enough circumstances, in the end the first picture returns. The quantity of considered cycles is known as the Arnold's time frame. The period depends on the picture estimate; i.e., for various size pictures, Arnold's period will be diverse. The various steps involves in the image encryption process are given below:

Step 1: Input a RGB image

Step 2: Use numb as variable which is denoted as the No. of Iterations

Step 3: Find the No. of rows and columns.

Step 4: for incr = 1 to numb

```
    for row1= 1 to row
        for col1= 1 to col
            nrowp=row1
            ncolp=col1
            for ite =1 to incr
                Shuffle the positions of the image pixels u
            end
            Result the new encryption image
        end
    end
end
```

3.3 Feature Extraction

Feature extraction is done on all images of respective database in a unique way so that the result of image retrieval is accurate. Block diagram for the feature extraction is given in the figure 3.3

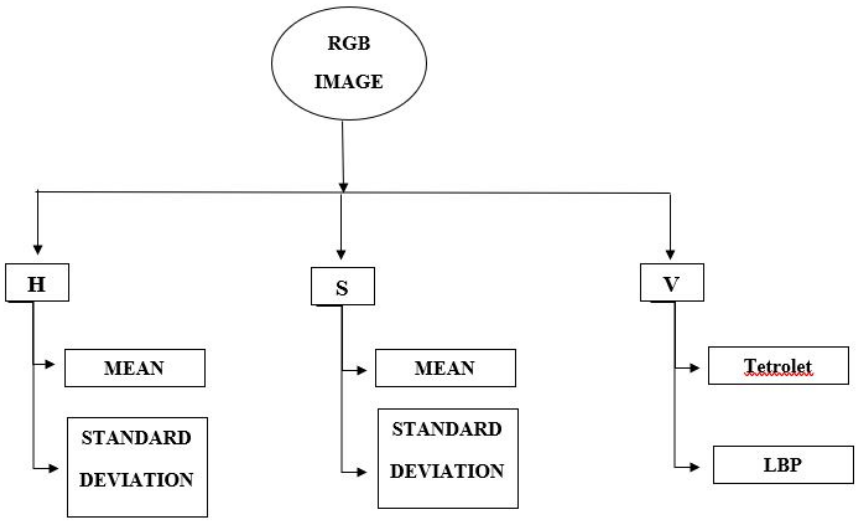

Fig. 3 Image Feature Extraction

4 Experimental Results

We have used four standard image database namely:
1. GHIM-10000 [11]: It contains 10000 different images which is of 20 categories like firecracker, building, cars, horse, Insects etc.
2. Sorted Produce-1400 [4]: It contain 1400 different images which is of 14 categories of food items like potato, apple etc.
3. Oliva & Torralba Scene (OT-Scene) [12]: It contains 2688 different images which is of 8 categories of Scenic beauty.
4. Coral 1000 [10]: It contains 1000 different images which is of 10 categories like dinosaur, beach, bus, roses etc.
All the proposed techniques and the derived results are obtained in MATLAB environment. All classifications contains categories of images of different sizes. The experiment is checked by various number of returning pictures, which fluctuates from 3 to 20. Calculation of precision, recall, Fscore is done on the image databases. Proposed strategies are superior to the older research work as better features of image are being extracted and security is provided to it at top level. Tetrolet as an image feature is never been used for content based image retrieval process. Figure below will show first the secure content based image retrieval results followed by the calculation of precision, recall, Fscore is done on the image databases.

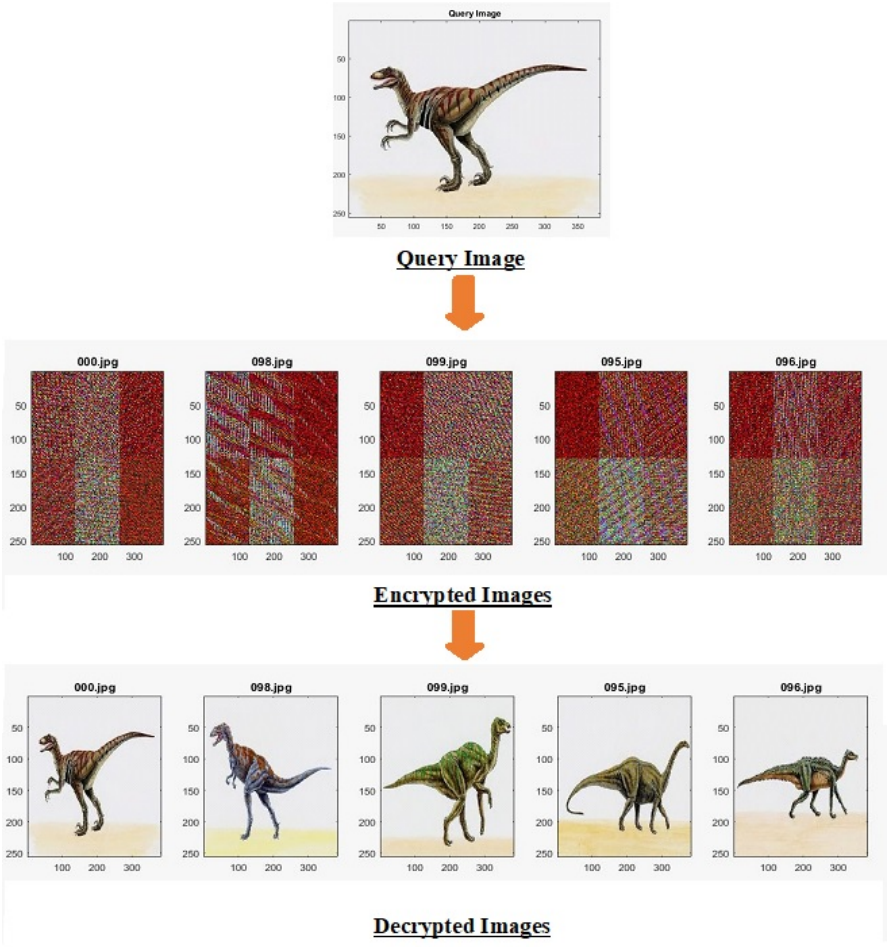

Fig. 4 Result for a Category of Corel-1000 Image

Table 1 Demonstrating the Average Precision, Recall, F-score for Various Databases

Database Name	Average Precision	Average Recall	Average F-score
Corel-1000	64.82	12.96	19.42
GHIM-10000	62.50	2.50	4.80
Produce- 1400	67.80	13.56	20.36
Olivia- 2688	68.20	4.67	8.72

5 Conclusion

In this work, the authors have presented a secure CBIR scheme that not only efficiently retrieved image based on the primitive visual image feature but simultaneously impose security aspects to its transmission. There are three main entities in this work i.e. (i) owner who have the original image database: its responsibility is to generate an encrypted image database, generate an encrypted image feature database, and transfer both databases to the centralized database (ii) user who has a query image and wants to receive the corresponding similar images securely: its responsibility is to extract query image features, form encrypted query image feature vector, and send it to the centralized database (iii) centralized database: by which the main repository and searching process has been carried out at pseudo encrypted domain. The owner has created an encrypted image database using modified ACM with a logistic map, created an encrypted image feature database using the ASPE technique, and transfer these databases to a centralized database. Now, the user has to create the encrypted query image feature vector using the same ASPE technique and transfers it to a centralized database. Afterward, similarity measurement of this query image feature vector among all the encrypted feature vectors of the encrypted feature image database has been carried out in a centralized database to retrieve a few of most similar encrypted images which are to be transferred to the user side. Now, through the received key from the owner side, user will decrypt those received images to get the final output. Similarity measurement in a fully encrypted domain may lead us to the wrong outcomes. Therefore, we have incorporated similarity measurement in the pseudo encrypted domain and got the desired result efficiently and securely.

References

1. Xia, Zhihua, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE transactions on information forensics and security 11, no. 11 (2016): 2594-2608.

2. Sengar, S. S., & Mukhopadhyay, S. (2020). Motion segmentation-based surveillance video compression using adaptive particle swarm optimization. Neural Computing and Applications, 32(15), 11443-11457.
3. Sengar, S. S., & Mukhopadhyay, S. (2020). Moving object detection using statistical background subtraction in wavelet compressed domain. Multimedia Tools and Applications, 79(9), 5919-5940.
4. Kumar, S., Pradhan, J., & Pal, A. K. (2021). Adaptive tetrolet based color, texture and shape feature extraction for content based image retrieval application. Multimedia Tools and Applications, 80(19), 29017-29049.

5. Kumar, S., Pradhan, J., & Pal, A. K. (2017, December). A CBIR scheme using GLCM features in DCT domain. In 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-7). IEEE.
6. Guo, Z., Zhang, L., & Zhang, D. (2010). Rotation invariant texture classification using LBP variance (LBPV) with global matching. Pattern recognition, 43(3), 706-719.

7. Wang, X., Han, T. X., & Yan, S. (2009, September). An HOG-LBP human detector with partial occlusion handling. In 2009 IEEE 12th international conference on computer vision (pp. 32-39). IEEE.
8. Bao, J., & Yang, Q. (2012). Period of the discrete Arnold cat map and general cat map. Nonlinear Dynamics, 70(2), 1365-1375.
9. Kumar, S., Pal, A. K., Islam, S. K., & Hammoudeh, M. (2021). Secure and efficient image retrieval through invariant features selection in insecure cloud environments. Neural Computing and Applications, 1-26.
10. Li, J., and Wang, J. Z. (2008). Real-time computerized annotation of pictures. IEEE transactions on pattern analysis and machine intelligence, 30(6), 985-1002.
11. Liu, G. H., Yang, J. Y., and Li, Z. (2015). Content-based image retrieval using computational visual attention model. pattern recognition, 48(8), 2554-2566.
12. Oliva, A., & Torralba, A. (2001). Modeling the shape of the scene: A holistic representation of the spatial envelope. International journal of computer vision, 42(3), 145-175.