IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Relevance Feedback Content-based Image Retrieval

[1] Aswathy Vijayan, [2] Prof. Priya V V, [3] Prof. H. A. Nisha Rose

[1] Student, [2,3] Assistant Professor

[1,2,3] Department of CSE,

[1] TKM College of Engineering Kollam, Kerala,India

[2,3] College of Engineering Thalassery, Kerala,India

Abstract: Content-based image retrieval (CBIR) consists of retrieving the most visually similar images to a given query image from a database of images. Modern CBIR systems usually adopt interactive mechanism, namely relevance feedback, to enhance the retrieval precision. In the context of an untrustworthy CBIR service provider, the major privacy concern is that the user's search intention could be learned by the service provider. Based on the search intention, the service provider can infer the user's profile such as user's interest, living place, health condition, and even commercial secret. The new Secure Relevance Feedback Content-based Image Retrieval (SRF- CBIR) system can preserve the user's search intention by preventing the query, result, and feedback attacks on the image sets. SRF-CBIR has three stages which are secret query, secret feedback, and native retrieval. Secret query performs the initial query with a privacy controllable feature vector; secret feedback constructs the feedback image set by introducing certain confusion classes following the K- anonymity principle; native retrieval finally re-ranks the images on the user side. SRF- CBIR can deal with query attack, result attack, and feedback attack existing in RF-CBIR. The privacy-preserving performance of SRF-CBIR is significantly improved compared to RF-CBIR, while the retrieval performance sacrifice is acceptable.

***Index Terms* - CBIR, Relevance Feedback, K-anonymity, RF-CBIR.**

I. Introduction

Nowadays, the use of the Internet and digital imaging technologies is increasing, and as a result, a considerable amount of digital images are created and used in various fields such as education, medicine, and so on. The size of image datasets is increasing day by day, and hence their effective retrieval becomes a basic need. An image retrieval system retrieves images from the database of images based on user requests. The most widely used image retrieval approaches [1] are Text-based Image Retrieval (TBIR) and Content-based Image Retrieval (CBIR). In TBIR, the search for images is based on the text descriptions associated with the image. However, TBIR has specific difficulties, especially when the image database is too large. The main drawback is that the user needs to annotate an image manually, and it takes much time for obtaining the result. This type of image search purely depends on the annotation quality and completeness. The other difficulty is that a word can have different meanings. For example, if a user searches for the images of Apple, then the system cannot differentiate either the user is searching for the Apple products or Apple fruit. They have the same name, but they are entirely different things. CBIR overcomes these problems with TBIR and CBIR still works when textual annotations are not available. As a result, CBIR is widely used more than TBIR, and our image search engines such as Google Image Search and Bing Image Search are now available with CBIR implementation. Content-based image retrieval (CBIR) [2, 3] is a widespread technique gradually applied in retrieval systems [1]. Content-based Image Retrieval consists of retrieving the most visually similar images to a given Input image from the database of images. "Content-based" means that, here in this image retrieval system, the search for images analyzes the content of the image rather than the textual annotation associated with the image. Here the term "content" refers to any information derived from the image such as shape, color, texture, and so on.

Feature extraction is a vital part of any CBIR system. Initially, the features of the images in the image database are extracted and store it there. Then the user extracts the features of the query image, and retrieve images with the closest features. Visual features include color, texture, shape, and so on. The main aim of a CBIR system is to retrieves the most similar images from an image database when the user is submitting a query image to the system. The process of finding the similarity or difference between the query image and the database image is referred to as similarity measurement. After computing this, the database images are sorted according to the increasing order of their distance to the query image. Then the images are retrieved from the image database according to this order. There are many distance measures available for evaluating the similarity of two images according to their features. Some of the commonly used measures are Minkowski-Form distance, Euclidean Distance, Manhattan distance, and so on.

The modern CBIR system usually adopts an interactive mechanism, namely Relevance Feedback (RF). In general, a traditional Relevance Feedback Content-based Image Retrieval (RF-CBIR) system consists of two stages, query stage and feedback stage. The sequence diagram of the system is shown in Fig. 1. In the query stage, the user submits an input image P to the CBIR server. The server extracts the low-level features of P and retrieves the most visually similar images to P from the image database D by computing Euclidean distances with respect to the low-level features. Then the top N similar images of P are returned as the initial result R^0. In the feedback stage, the user labels some relevant images in R^0 as F and submits F to the server. The server treats the images in F as positive samples and the randomly selected images from R^0 – F with the same size of F as negative samples. Then a machine learning-based classifier such as Support Vector Machine (SVM) [4] is used to rank the images in the image database and return the top N ranked image as the final result R^1.

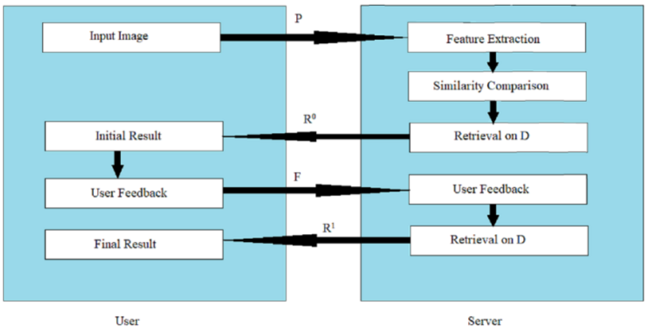

Fig. 1. The sequence diagram of RF-CBIR System

When working with an image, our privacy reserves more importance. The main privacy issue that exists in the CBIR system is that an untrustworthy CBIR server may learn the user's search intention. Then using this search intention, it will infer the user's information such as his interests, living place, health condition, and other secrets. For example, in the medical field, if the user submits a tumor image to the retrieval system, then the server infers the health condition of the user. The privacy problems in RF-CBIR are shown in Fig. 2. The attacks through which CBIR service provider learns the search intention of the user are given below.

- Query Attack: Here, the server learns the search intention of the user by analyzing the input image P.
- Feedback Attack: The search intention is obtained by utilizing the user's feedback image set F.
- Result Attack: The server analyses the results returned to the user, the initial result R^0, and the refined result R^1.

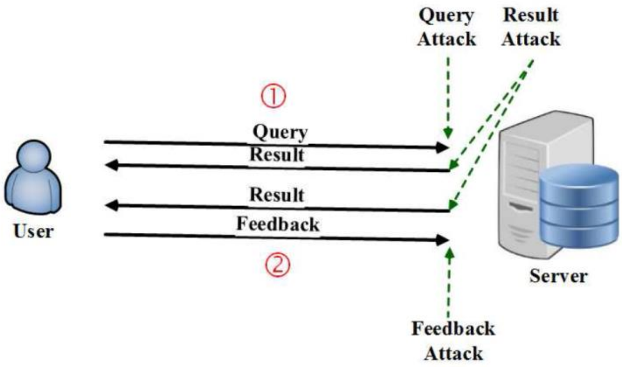

Fig. 2. Privacy Problems in RF-CBIR

In the last two decades, the CBIR systems have been improved a lot. However, there remain some problems which have not been answered satisfactorily. The most crucial problem is the privacy issue. Many researches are happening in this area for improving retrieval performance, but a few focus on the privacy issues existing in the image retrieval system. Hence, the goal of this work is to develop a new privacy protected RF-CBIR image retrieval system which provides more accurate results and protect the user's privacy at the same time in a simple way.

The major objectives of the work are summarized as follows.

- Implement privacy protection in Interactive Content-based Image Retrieval system
- Provide protection from Query attack, Result attack, and Feedback attack
- Prevent service provider from inferring the user's search intention

The rest of the paper is organized as follows. Section II describes the related works. Section III presents the methodology. Section IV reports the experiments and results, and finally, the work is concluded in section V.

II. LITERATURE REVIEW

This chapter discusses the literature in the field of content-based image retrieval. Content-Based Image Retrieval (CBIR) is a useful image retrieval mechanism that retrieves the most visually similar images to the user's query image from the database of images. The problem with the CBIR system is that the retrieval results may not be accurate, and hence the system is not efficient. By integrating human interaction with the system, we can improve the efficiency of the system, which is known as Relevance Feedback Content-based Image Retrieval (RF-CBIR).

Giang et al. [5] proposed an effective feedback related scheme for content-based image retrieval. RF-CBIR tries to improve retrieval performance by taking feedback from the user side on the initial retrieval result. However, there exist some difficulties with these systems. The main limitation is that the user needs to loop a certain number of steps before obtaining the final result; hence the process is inefficient for applications. In this work, they proposed a novel batch mode SVM active learning scheme for relevance feedback in CBIR. Instead of the SVM decision function used in traditional methods, the system allows the user to label using a combined ranking function by choosing a batch of feedback examples. The unique ranking function is formed by combining two scores of SVM function and similarity measure. The retrieval performance can be further improved by keeping a sufficient number of initially labeled samples. In this work, the user's query image is not protected from the server.

The primary and most crucial drawback of RF-CBIR is that the service provider may infer the user's search intension by profoundly analyzing the query image. Nowadays, users are very bothered about the privacy of the query image, and hence they do not want to reveal the query image even to the database. Here comes the relevance of a secure content-based image retrieval system. The main aim of these systems is to prevent the service provider from inferring the user's search intension. Shashank et al. [6] are the pioneers in this direction. They propose an algorithm for PCBIR when the database is indexed using a hierarchical index structure or hash-based indexing scheme:

2.1 Hierarchical Structures

In the hierarchical or tree structures, the leaf nodes represent the images, and each intermediate node contains information related to data stored in its subtree. For querying the index structure, the user initially extracts the feature vector of the query image. During querying, one traverses the index structure by taking a decision at each node to determine which child node(s) we need to traverse next. The query's feature vector and the data at the node are used to make this decision. When a leaf is found, the result is obtained by using the data stored in it. Finally, the result is returned to the user. To prevent the database from learning anything about the query while the user gets the results for his query, keep the path of the traversal unknown to the database. To keep the path unknown, the user should not reveal node(s) being accessed.

The basic idea is that initially, the user extracts the feature vector of the query image and asks the database to send the information at the root node. Then the user decides which child nodes to move next by using the feature vector and the information received based on a decision policy or constraint. For the node of interest at a particular level, the user frames a query, receives the reply from the database, and obtains the information at the node of interest. If the node is a leaf node, then the user makes use of the data at the node to compute results. Otherwise, the user finds the child nodes to move next by applies the decision policy.

2.2 Hash-based Retrieval

A hash function is used to divide the images into the database into bins. The bins are treated as an array of nodes which is similar to the array of nodes in a hierarchical indexing scheme. A hash function is applied to the given query image to determine the bin in which it falls. Suppose the image falls in bin i. Then the user frames and sends a query to obtain the information at node i. The database sent an answer as a reply to the query Q, and the user obtains the information at node i from that answer.

The algorithm is accurate, efficient, fast, and scalable. It preserves the privacy of the user very well and is also feasible. However, this approach increases the interactions between the user and the service provider, where both sides need interacting p times to fetch a node with p bits.

Weng et al. [7] studied the problem of privacy protection in content-based image retrieval and proposed a framework. The basic idea is to use robust hash values as queries so that we can prevent revealing the original content or features to the server. Then we can omit certain bits in a hash value, which again increases the ambiguity for the server. It is very challenging for the server to know the user's intention due to the reduced information received. Once obtain the query, the server returns the hash values of all possible items to the user, and the user searches the returned items for the best match to the interest. Privacy is protected since only hash values are exchanged between the user and the server, privacy is protected. However, this approach is not suitable for the general CBIR task.

Bellafqira et al. [8] proposed a secure CBIR implementation that allows a search in an encrypted image database maintained by a server. It provides data confidentiality, allows the extraction of global image features, and does not require further communications in-between the client and the server during the search. The main drawback of the system is that the user needs to send a large amount of information to the server.

By analyzing these works, we can understand that there exist some difficulties while trying to preserving our privacy during image retrieval. So a new system is developed for handling the privacy issues in a simple manner, which is described in the next section.

III. METHODOLOGY

The new Secure Relevance Feedback Content-Based Image Retrieval (SRF-CBIR) system consists of three stages– secret query, secret feedback, and native retrieval. Secret query constructs the initial query with a privacy controllable feature vector, secret feedback makes the user feedback image set by introducing certain confusion classes, and finally, the native retrieval ranks the retrieved images in the user side locally. Fig. 3 shows the sequence diagram of the scheme.

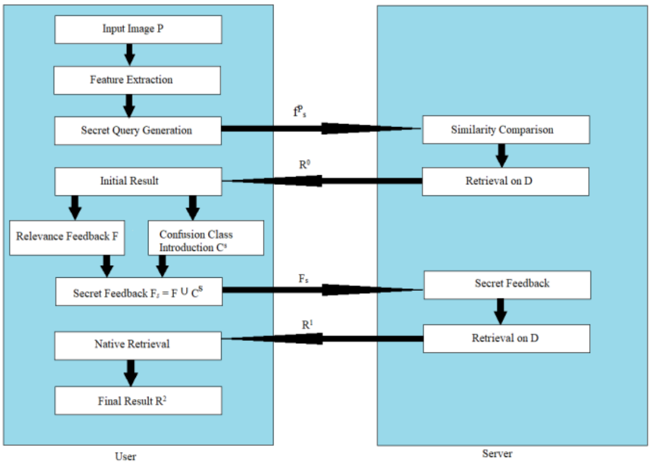

Fig. 3. The sequence diagram of SRF-CBIR

3.1Secret Query

The secret query is introduced to avoid the query attack as well as the result attack on the initial result R^0. Query attack can be avoided by making use of only a part of the P's feature vector f^P_s as a query instead of the query image P. The result attack on R^0 can be reduced by adjusting the privacy information included in the secret query vector f^P_s. Fig. 4 shows the sequence diagram of the secret query method, which consists of two stages.

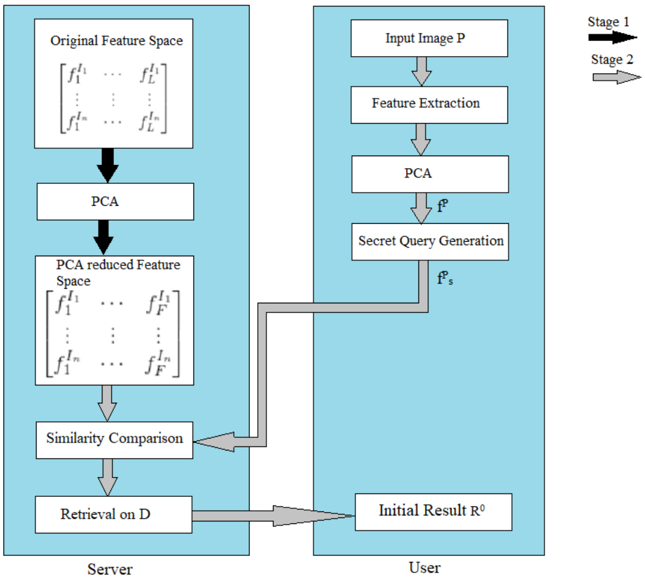
Original Feature Space
$\begin{bmatrix} f_1^{I_1} & \cdots & f_L^{I_1} \\ \vdots & \vdots & \vdots \\ f_1^{I_n} & \cdots & f_L^{I_n} \end{bmatrix}$
PCA
PCA reduced Feature Space
$\begin{bmatrix} f_1^{I_1} & \cdots & f_F^{I_1} \\ \vdots & \vdots & \vdots \\ f_1^{I_n} & \cdots & f_F^{I_n} \end{bmatrix}$
Similarity Comparison
Retrieval on D
Server
Input Image P
Feature Extraction
PCA
f^P
Secret Query Generation
f^P_s
Initial Result R^0
User
Stage 1
Stage 2

Fig. 4. The sequence diagram of Secret Query

3.1.1 Stage 1

In this stage, the service provider performs Principal Component Analysis (PCA) on the original feature set and stores the PCA reduced feature set. Here, PCA is performed before image retrieval for reducing the dimensionality of the feature space [9]. After PCA feature reduction, the feature components are in the descending order of importance.

Suppose the image dataset is D = $\{I_1, \ldots, I_i, \ldots, I_n\}$, the feature vector of image I_i ε D can be denoted as $f^{Ii} = f^{Ii}_1, \ldots, f^{Ii}_j, \ldots, f^{Ii}_L$ and the feature vectors of all images in D can be represented as a matrix M = $(f^{I1}, \ldots, f^{Ii}, \ldots, f^{In})^T$. After PCA, the feature vector of each image in D can be represented as $f^{Ii} = f^{Ii}_1, \ldots, f^{Ii}_j, \ldots, f^{Ii}_F$, and the matrix M_F of feature vectors of all images in D includes only the first F ($F < L$) important PCA feature components.

3.1.2 Stage 2

In this stage, the user develops the secret query vector f^P_s and retrieves images from the image dataset D. Let the user's input image be P. First, the user needs to extract the features of P. As already said, feature extraction is the key part of a CBIR system.

After extracting the features, the user performs PCA on the extracted image features. Now, the feature vector of P can be represented as f^P. Let the secret query vector be f^P_s. Then, the user is required to choose a starting index i and a query vector length l. The secret query is obtained by choosing a continuous segment from f^P satisfying both i and l, which can be formulated as,

$$f^{P}_{s} \ \varepsilon \ \{f^{P}[i{:}(i{+}l{-}1)] | 1 \leq i \leq (F{+}1{-}l)\} \qquad (1)$$

where $f^P[i{:}(i+l-1)]$ denotes a continuous segment from f^P, with the index from i to $(i+l-1)$.

Finally, the server retrieves images from the image dataset D by computing the Euclidean distances with respect to f^P_s and returns the top N similar images as the initial result R^0.

3.2 Secret Feedback

Secret feedback can deal with the feedback attack and result attack on refined result R^1. The basic idea is to introduce certain confusion classes into the feedback image set F to form the secret feedback image set F_s. Here, the image retrieval system adopts K-anonymity [10] as the privacy-preserving principle. According to the K-anonymity principle, relevance feedback is K-anonymity feedback if, in F_s, the number of images belonging to target class G is equal to the number of images belonging to K – 1 other confusion classes $C_1, \ldots, C_{K-1}$. That is,

$$n(G, F_s) = n(C_1, F_s) = \ldots = n(C_{K\text{-}1}, F_s) \qquad (2)$$

where, $n(C_i, F_s)$ is the number of images in F_s belonging to class C_i.

During the relevance feedback stage, the user randomly labels some relevant images in R^0 as F. For making the feedback image set F_s satisfying the K-anonymity principle stated above; the user introduces certain confusion classes to the feedback set F.

ResNet classifies the images in R^0, the resultant classes are represented as $C = \{C_1, \ldots, C_k\}$. K – 1 classes are selected from these classes, which are called confusion classes. The valid classes are those having a size greater than or equal to the size of F, that is $|C_i| \geq |F|$. Also, that classes should not contain any images in G, as $C_i \cap G = \phi$. Now choose K – 1 such classes from C. Let it be C^s. For each of those selected classes, randomly choose |F| images. Then add those K – 1classes with the size of |F| to the feedback image set so that F_s satisfies the K-anonymity principle.

Finally, regarding F_s as positive examples and randomly selected images from $R^0 - F_s$ as negative examples, the server use SVM to rank the images in D and returns the top N ranked images as the refined result R^1.

3.3 Native Retrieval

The retrieval result R^1 would not be satisfactory since some confusion classes are introduced during the secret feedback stage. So the user needs to again rank the images in R^1 locally at the user's side. For that, the user treats F as a positive training set and images in introduced confusion classes as a negative set, and SVM is then trained to rank the images in R^1, thus obtain the final result R^2.

IV. EXPERIMENTS AND RESULTS

The experiments are carried out using the Caltech-256 image dataset.

3.1 Data Set

The Caltech-256 was created by the California Institute of Technology to facilitate computer vision research. The dataset consists of 256 categories of images, each consist of eighty to eight hundred images. The work is implemented using a subset of Caltech-256, which consists of 30 classes, and each class includes 100 images. For the image retrieval task, certain query images are randomly selected from the remaining images in each class from the dataset.

3.2 Feature Extraction

Five low-level features are used to represent images as follows:

- Scalable Color Descriptor (256-dimension) [11]
- Color Layout Descriptor (192-dimension) [11]
- Edge Histogram Descriptor (80-dimension) [12]
- Histogram Oriented Gradient (HOG) Descriptor (3780-dimension) [13]
- Gabor Feature (240-dimension) [14]

Altogether, those features form a 4548-dimension vector. After PCA feature reduction, the feature components are in the descending order of importance. In this work, the top 100 features were kept for balancing dimension reduction and variance preservation.

3.3 Performance Analysis

3.3.1 Privacy Performance

Result attack and feedback attacks are both performed by analyzing the image set of results or feedback, respectively. Here, Maximum Frequency Inferring (MFI) [15] is used for analyzing the result and feedback attacks. In MFI, the images in the image set are categorized into classes, those classes are sorted in the decreasing order of the number of images belonging to them, and the most frequent class will be inferred as G.

3.3.1.1 Query Attack

Query attack is performed by analyzing the input image submitted to the server by the user. In the traditional RF-CBIR system, the server can accurately predict the user's search intention directly with the input image P, but in SRF-CBIR, the user submits only the secret query instead of the input image. So the query attack becomes impossible.

3.3.1.2 Result Attack on R^0

In RF-CBIR, R^0 is retrieved with the total feature vector f^P. In comparison, R^0 is retrieved with the private query f^P_s in SRF-CBIR. Since f^P_s is a part of f^P, the number of images belonging to target class G in R^0 is less than that of RF-CBIR, $n_{SRF}(G, R^0) < n_{RF}(G, R^0)$. Accordingly, the probability that G is the most frequent class in SRF-CBIR is smaller than in RF-CBIR. For a given starting index i and length l, f^P_s is generated from f^P. With the decrease of i, more important feature components will be introduced into $f^P{}_s$, and the number of images belonging to G in R^0 will increase. Consequently, the attack success probability will increase. Fig. 5 presents the success of result attack on R^0.

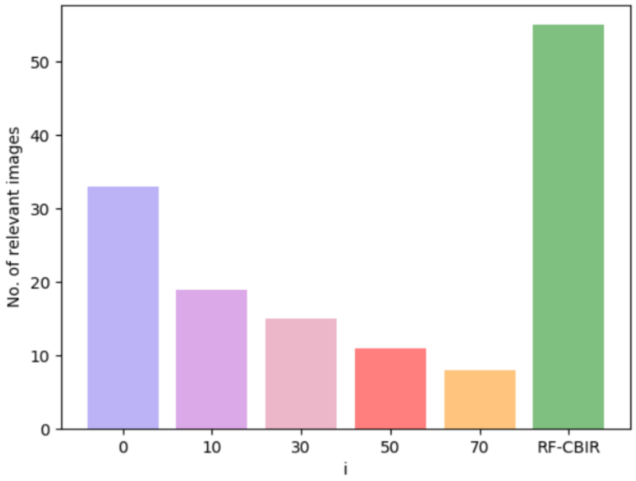

Fig. 5. The success of result attack on R^0

Here, the secret query is generated with i=0, 10, 30, 50, 70, and l=30. The original query in RF-CBIR with the full feature vector is implemented as a baseline. It shows that the number of images belonging to G in R^0 of SRF-CBIR is less than that of RF-CBIR. So, the attack success probability of the secret query in SRF-CBIR is lower than that of the original query in RF-CBIR. It also shows that, for the secret query, with the decrease of i, the number of relevant images in R^0 increases. For example, when i=70, the number of relevant images is 8. When i=0, the number of relevant images increases to 33. So the attack success probability also increases.

3.3.1.3 Feedback Attack

In RF-CBIR, the feedback image set F contains only the relevant images, which are all from the target class. So the attack success probability is 1. In SRF-CBIR, the feedback image set F_s is generated following the K-anonymity principle. Hence, the numbers of images in classes C_1, ..., C_i, ..., C_K are the same. So the size of G is equal to the size of other classes, the probabilities that G ranked at position 1, ..., K will be the same value of 1/K. Fig. 6 shows the success of feedback attack.

The secret query is generated with i=70 and l=30. The top 200 images are returned as the initial result R^0. The secret feedback F_s is created by selecting 5 relevant images in R^0 as F and to make the K-anonymity feedback F_s, add certain confusion classes with different K values. The traditional RF-CBIR is implemented as a baseline. It shows that the attack success probability of SRF-CBIR is lower than that of RF-CBIR. Also, it can be observed that with the increase of K, the attack success probability decreases. The reason is that with the increase of K, more confusion classes are introduced to the feedback set.

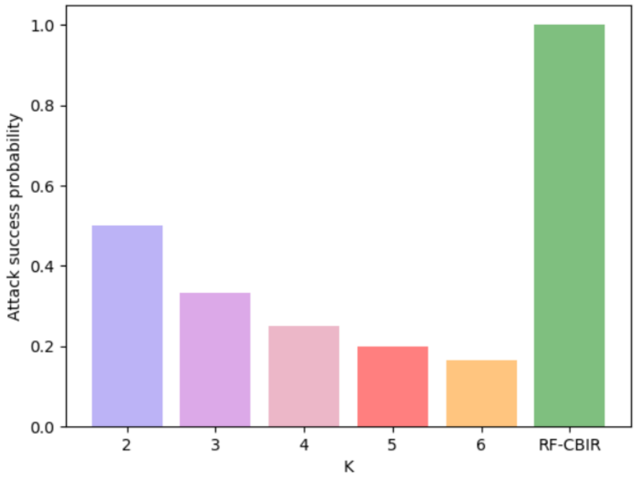

Fig. 6. The success of feedback attack

3.3.1.3 Result Attack on R^1

In RF-CBIR, R^1 is retrieved with the feedback image set F with the SVM classifiers. The retrieval accuracy is improved through feedback; therefore, the success probability of attack with MFI increases compared to that on R^0. On the other side, because of the classification error of the SVM classifier, inappropriate images will exist in R^1. Thus, the success probability of attack with MFI is smaller than that on F. In SRF-CBIR, R^1 is retrieved with the feedback image set F_s. Ideally, the retrieved result R^1 will have the same class distribution as F_s. However, because of the classification error of the SVM classifier, some images from noisy classes will be presented in R^1. Suppose there are t noisy classes with the approximate size of classes in F_s, then attack success probability will be 1/K+t which is less than 1/K.

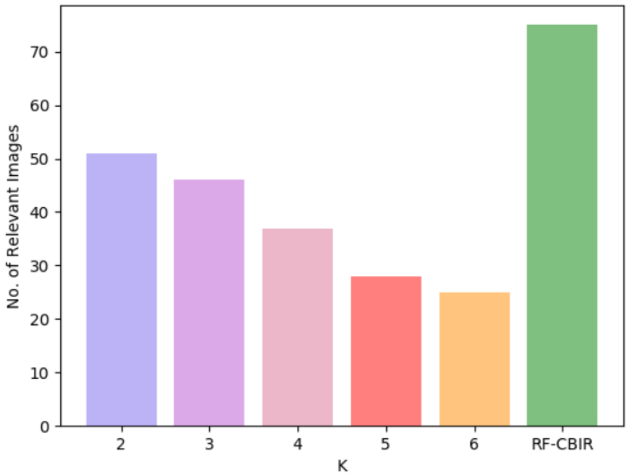

Fig. 7. The success of result attack on R^1

Fig. 7 shows the success of result attack on R^1. Here, the success of the attack in SRF-CBIR is lower than that of RF-CBIR. Also, with the increase of K, the attack success probability in SRF-CBIR decreases. This is because more confusion classes are introduced with the increase of K.

3.3.2 Retrieval Performance

The input image and the final result R^2 is shown in Fig. 8 and Fig. 9 respectively. Here, the secret query is developed with i=70 and l=30. Then top 200 similar images are obtained as the initial result R^1. Now the user labels 5 relevant images in R^0 as F and introduce 3 confusion classes to make the secret feedback F_s. Then we can see that most of the retrieved images in final result are relevant. But with the increase of K, the retrieval precision drops a little. The reason is that more confusing classes are presented in the procedure of private feedback and native retrieval.

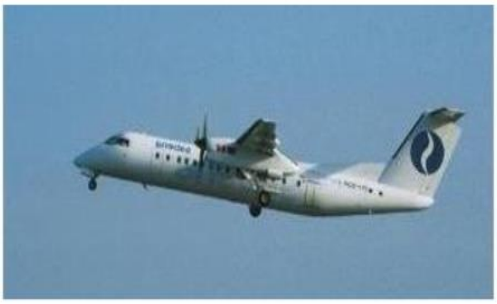

Fig. 8. The input image P

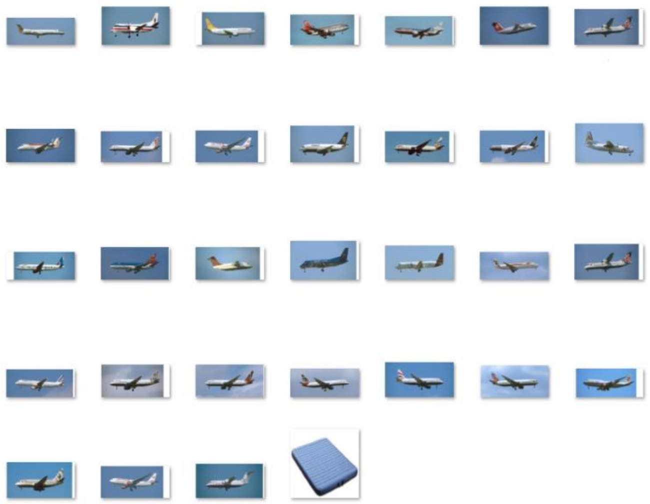

Fig. 9. The final result R^2

The retrieval performance of the new SRF-CBIR is measured on the result of native retrieval after secret feedback, which is on R^2. The secret query and traditional RF-CBIR are implemented as references. The retrieval performance of three retrieval systems is shown in Fig. 10, and the retrieval performance of SRF-CBIR with different K values is shown in Fig. 11

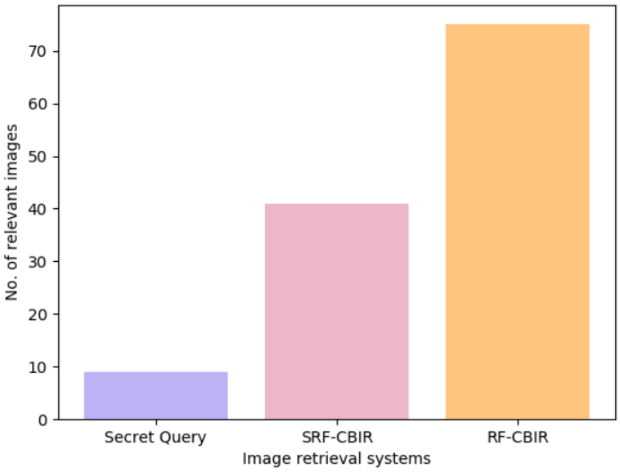

Fig. 10. The retrieval performance of different image retrieval systems

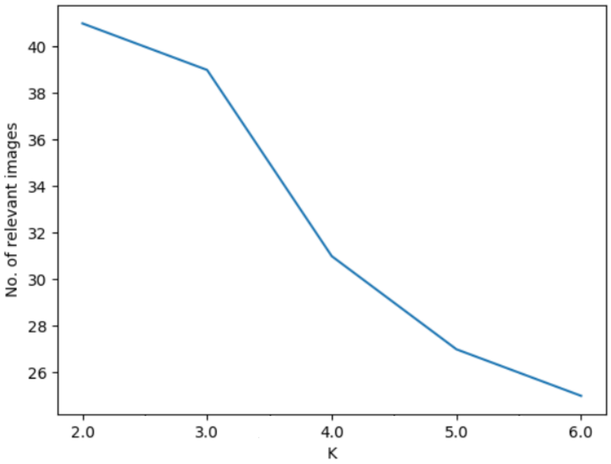

Fig. 11. The retrieval performance of SRF-CBIR with different K

By comparison with the secret query, the retrieval performance is improved significantly in both RFCBIR and SRF-CBIR. For example, the number of relevant images in the final retrieval result when retrieved top 200 images are 9, 75, and 41 in the secret query, RF-CBIR, and SRF-CBIR (K= 2) respectively. The retrieval performance of new SRF-CBIR is slightly lower compared to RF-CBIR. In SRF-CBIR, when K increases, the retrieval performance drops a little. The reason is that more confusion classes are presented in the procedure of private feedback and local retrieval.

V. CONCLUION

The new method of image retrieval, Secure Relevance Feedback Content-based Image Retrieval (SRFCBIR) can protect the user's search intention and at the same time, provides the relevant images. SRF-CBIR consists of three stages: secret query, secret feedback, and native retrieval. The new secret query method performs the initial query with a privacy controllable feature vector. The new secret feedback method introduces confusion classes into the feedback image set to protect user intention. The native retrieval finally re-ranks the images on the user side locally. Providing the data exchanged with the user, the service provider can learn the search intension through the query, result, and feedback attacks. SRFCBIR can deal with these attacks existing in RF-CBIR. It shows that the new scheme can effectively control privacy leakage and significantly reduce the attack success probability. The results demonstrate that the privacy-preserving performance of SRF-CBIR is significantly improved compared to RF-CBIR, while the retrieval performance sacrifice is acceptable.

VI. ACKNOWLEDGMENT

This work is supported by department of computer science and engineering in TKM College of Engineering Kollam.

REFERENCES

[1] Y. Rui, T. S. Huang, and S. F. Chang, "Image Retrieval: Current Techniques, promising directions, and open issues," Journal of visual communication and Image Representation. vol. 10, no. 1, pp. 39–62, 1999.

[2] A. W. M. Smeulders, M. Worring, S. Santini, A. Gupta, and R. Jain, "Content-based image retrieval at the end of the early years," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 12, pp. 1349-1380, 2000.

[3] R. Datta, J. Li, and J. Z. Wang, "Content-based image retrieval: Approaches and trends of the new age," in The 7th ACM SIGMM International Workshop on Multimedia Information Retrieval. Hilton, Singapore, 2005, pp. 253-262.

[4] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning. vol. 20, no. 3, pp. 273–297, 1995.

[5] T. G. Ngo, Q. T. Ngo, and D. D. Nguyen, "Image Retrieval with Relevance Feedback using SVM Active Learning," in International Journal of Electrical and Computer Engineering. Vol. 6, No. 6, pp. 3238 – 3246, 2016.

[6] J. Shashank, P. Kowshik, K. Srinathan, and C. V. Jawahar, "Private content based image retrieval," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Anchorage, AK, 2008, pp. 1-8.

[7] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet, "A privacy-preserving framework for large-scale content based information retrieval," in IEEE Transactions on Information Forensics and Security. vol. 10, no. 1, pp. 152–167, 2015.

[8] R. Bellafqira, G. Coatrieux, D. Bouslimi, and G. Quellec, "Content-based Image Retrieval in Homomorphic Encryption Domain," in IEEE Conference on Medicine and Biology Society. 2015.

[9] I. Jolliffe, "Principal component analysis,". Wiley Online Library, 2002.

[10] L. Sweeney, "K-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. vol. 10, no. 5, pp. 557–570, 2002.

[11] J.-R. Ohm, L. Cieplinski, H. J. Kim, S. Krishnamachari, B. Manjunath, D. S. Messing, and A. Yamada, "The MPEG- 7 color descriptors," IEEE Transactions on Circuits and Systems for Video Technology. 2001.

[12] T. Sikora, "The MPEG-7 visual standard for content description-an overview," IEEE Transactions on Circuits and Systems for Video Technology. vol. 11, no. 6, pp. 696–702, 2001.

[13] Nikita Kaushik, Ritu Rawat, and Anshika Bhalla, "A Brief Study of Different Feature Detector and Descriptor," in International Journal of Advanced Research in Computer and Communication Engineering. vol. 5, issue 4, April 2016.

[14] B. S. Manjunath and W. Y. Ma, "Texture features for browsing and retrieval of image data," IEEE Transactions on Pattern Analysis and Machine Intelligence. vol. 18, no. 8, pp. 837–842, 1996.

[15] Y. Huang, J. Zhang, L. Pan, and Y. Xiang, "Privacy Protection in Interactive Content Based Image Retrieval," in IEEE Transactions on Dependable and Secure Computing. vol. 17, no. 3, pp. 595–607, 2018.