ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Relevance Feedback Using Auditing Scheme in Content-based Image Retrieval in Cloud Computing Environment

Sonali Panchal[1], Shital Gaikwad[2]

P.G. Student, Department of CSE, MPGI Institution of Engineering and Technology, Khupsarwadi, Vishnupuri, Nanded, (M.S.), India[1]

Assistant Professor, Department of CSE, MPGI Institution of Engineering and Technology, Khupsarwadi, Vishnupuri, Nanded, (M.S.), India[2]

ABSTRACT: Content-Based Image Retrieval (CBIR) is the incorporated Computer of the Image Retrieval issue for instance issue of chasing down pictures on Cloud in enormous datasets. To understand request semantics and customers wants so as to grant submitted results in regards to exactness, Relevance Feedback is combined into CBIR structure. Essential analysis structure will manufacture the precision of yield and will pass on the hugest yield. In the watermark-based tradition, a novel watermark is explicitly embedded into the mixed pictures by the cloud server before pictures are sent to the inquiry customer. In this manner, when an illegal picture copy is found, the unlawful inquiry customer who appropriates the photos can be trailed by the watermark extraction. Feature vectors get guaranteed by the safe hashing figuring, analyzing and preparing age are used at picture customers side for affirmation reason. TPA (Third Party Auditor) is used to recognize coercion or malevolent activities performed in a cloud circumstance. In our proposed framework we are including the method of misrepresentation recognition by producing Trapdoor utilizing a hashing calculation, as a file is made with the UID and the client pictures with the names after link are only a trapdoor is created.

KEYWORDS: Content-Based Image Retrieval, relevance feedback, trapdoor generation, encryption, and decryption of images, hashing algorithm, auditing, cloud computing, watermark-based protocol.

I. INTRODUCTION

This project is the work that proposes an accessible encryption plot, considering the dishonest query users who may distribute the retrieved images to the individuals who are approved. Security of users and image transfer in the network is the main concern. Security of images during transfer is maintained using cryptography techniques. The efficiency is enhanced by locality-sensitive hashing index generation. Moreover, the unlawful production of user images is followed with the assistance of the watermark-based convention. A watermark-based convention is intended for the copy-deterrence purpose. Specifically, after completing the search operation requested by an image user, a unique watermark associated with the image is imperceptibly embedded into the retrieved images. Then, the watermarked images are sent to the image user. When an illegal copy of the image is found, the unlawful query user who made the illegal distribution can be traced by the watermark extraction. This will help to deter the illegal distribution. An elaborate watermark-based convention in the encryption area is designed for copy-deterrence in a cloud computing scenario. No one can open an encrypted file on the cloud side. As it is been encrypted it can only be seen or decrypted using our application.

Different from common watermarking techniques, the proposed protocol needs to embed the watermark directly into the encrypted images via the cloud server. After receiving the encrypted and watermarked images, the query user needs to decrypt the images directly, and the decryption should not affect the watermark in the images. For increasing the accuracy rate of output and for delivering the most relevant output we will be using relevance feedback

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

system. Multiple layer feedback system over encrypted images is a unique contribution. In our proposed system we are including the technique of fraud detection using a hashing algorithm.

II. LITERATURE SURVEY

Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren, all in their paper titled "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing" focused on CBIR with preserving privacy and copy deterrence in cloud computing. For privacy-preserving purposes, sensitive images, need to be encrypted before outsourcing which makes the CBIR technologies in plaintext domain to be unusable [1].

Jing Xin and Jesse S. Jin, both in their paper titled "Relevance Feedback for Content-based Image Retrieval using Bayesian Network" focused on relevance feedback is how to effectively utilize the feedback information to improve the retrieval performance. This paper presents a relevance feedback scheme using a Bayesian network model for feedback information adoption [2].
Bavisha, Madlin Asha, both in their paper titled "A keyword-based user privacy-preservation and copy-deterrence scheme for image retrieval in the cloud" ensures user privacy, a keyword-based technique is introduced to provide uniqueness for the users and their images and security of images during transfer is maintained using cryptography techniques. The search efficiency is enhanced by locality-sensitive hashing index table construction, and illegal publication of user images is traced with the help of watermark-based protocol [3].

Zhihua Xia, Yi Zhu, Xingming Sun, Zhan Qin and Kui Ren, IEEE Members and Senior Members, all in their paper titled "Towards Privacy-preserving Content-based Image Retrieval in Cloud Computing" focused on CBIR applications which are rapidly developed along with the increase in the quantity, availability and importance of images in our daily life. In this paper, a privacy-preserving CBIR scheme, allows the data owner to outsource the image database and CBIR services to the cloud, without revealing the actual content of the database to the cloud server [10].

Nasir Memon and Ping Wah Wong, both in their paper titled "A Buyer-Seller Watermarking Protocol" focused on the interactive buyer-seller protocol for invisible watermarking in which the seller does not know the exact watermarked copy that the buyer receives. Hence the seller cannot create copies of the original content containing the buyer's watermark. This prevents the buyer from claiming that an unauthorized copy may have originated from the seller [12].

Z. Xia, X. Wang, X. Sun and Q. Wang, all in their paper titled "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data" focused on a special tree-based index structure and propose a "Greedy depth-first search" algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between the encrypted index and query vectors [20].

K. Gopalakrishnan, Nasir Memon, Poorvi L. Vora, all in their paper titled "Protocols for Watermark Verification" focused onadding a watermark signal to the digital image that can later be extracted or detected to make an assertion about the image. Two types of watermarks exist: visible and invisible. Visible watermarks typically contain conspicuously visible messages or company logos indicating the ownership of the image. Invisible watermarks, on the other hand, are unobtrusive modifications to the image and the invisibly watermarked image visually appears similar to the original [21].

B. S. Manjunath, Jens-Rainer Ohm, Vinod V. Vasudevan and Akio Yamada all in their paper titled "Color and Texture Descriptors" focused on presenting an overview of color and texture descriptors that have been approved for the Final Committee Draft of the MPEG-7 standard. The color descriptors in the standard include a histogram descriptor that is coded using the Haar transform, a color structure histogram, a dominant color descriptor, and a color layout descriptor. The three texture descriptors include one that characterizes homogeneous texture regions and another that represents the local edge distribution [22].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

III. PROPOSED SYSTEM AND METHODOLOGY

A. System Architecture

The goal of the framework is to ensure the protection of picture clients and security for pictures both amid capacity and access against inquisitive outcasts and to beat all issues like information honesty, information protection, duplicate discouragement, watermarking, and redistributing the encoded pictures and related troublesome issues. This framework secures the protection of picture information in substance based picture recovery re-appropriating applications against an inquisitive cloud server and the unscrupulous question clients. Distributed computing offers an extraordinary open door for the on-request access to plentiful calculation and capacity assets, which settles on it an appealing decision for the picture stockpiling and CBIR redistributing.

The main contributions are listed below:

- User data are collected by the administrator and generates an Id and that Id is concatenated with the user image name, which it sends the result of concatenation and UID to the user.
- An index is created with the UID and the user images with the names after concatenation are nothing but a trapdoor is generated.
- Administrator stores the index and the encrypted database in a cloud server.
- The user searches for a particular image with the name after concatenation and UID in encrypted form.
- The watermark is added to the user images with his/her unique watermark bits.
- No one can open an encrypted file on the cloud side. As it is been encrypted it can only be seen or decrypted using our application.
- The user decrypts the image using the private key, a watermarked original image is obtained.
- Relevance Feedback is added so that user can get exact match result as per his/her image query.
- Relevance feedback is used for increasing accuracy rate of output for delivering the most relevant output.
- Multiple layer feedback system over encrypted images be a unique contribution.

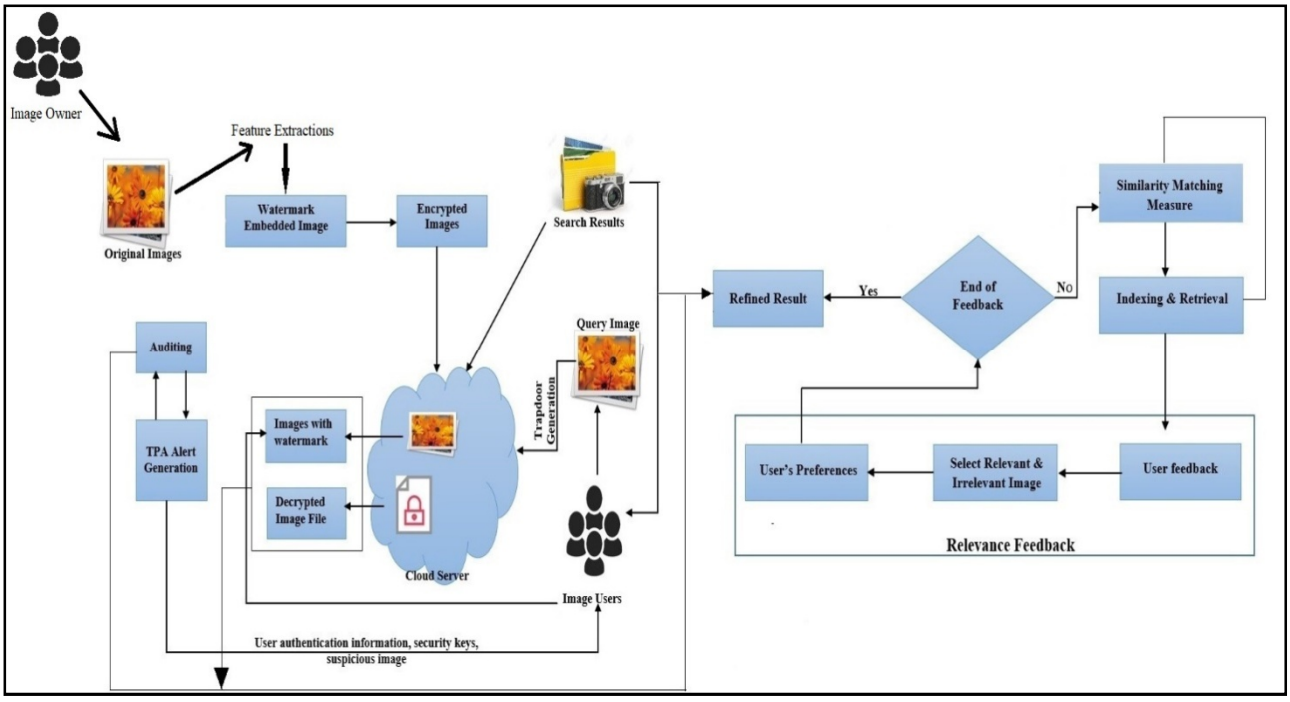

Fig.1:System Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Following are the phases which describe how the proposed system works gradually:

1. Original images are encrypted by image owner on cloud server, meanwhile encrypted index of those images are saved on cloud server along with user authentication information.
2. The watermark-based protocol is applied to those images.
3. Image owner sends the suspicious image to Watermark Certification Authority (WCA) checks for the possible illegal distributor. User lists are stored with WCA by image owner.
4. WCA generates watermark on those secured images and transfers them towards cloud server.
5. After that encrypted images are embedded with a watermark on a cloud server.
6. Once the watermark is embedded then the search image result is forwarded to image users. Image user now will fire image query and features will be extracted.
7. CBIR will check similarity measures between fired image query and stored database of images.
8. The image is processed is processed by indexing and image retrieval scheme with the help of CBIR.
9. Then the human interaction system i.e. Relevance Feedback System will give the result as relevant or irrelevant images iteratively with the help of users preferences.
10. After that user will give proper feedback for the retrieved result, if yes then the final refined result will be displayed and if not, then again the system will check similarities matching measure and will again ask for relevance feedback iteratively.
11. Final refined results will be images with a watermark, otherwise alert generation is sent back to image owner.
12. Images are decrypted and watermark will be extracted back again as per user's requirement.

B. Applications of Proposed System

1. Search for a picture to go with a broad story or search to illustrate a document
2. General browsing to make an interactive choice
3. Simple users search for one specific image on the web
4. Education and Training
5. Medical Diagnosis
6. Fashion and Publishing
7. Police crime Branch for photo recognition in crime prevention
8. Cartography-Mapmaking from photographs, synthesis of weather maps
9. Multimedia like Journalism and Advertising
10. Home Entertainment
11. Fingerprint or retina scanning for access privileges in the security check
12. Trademark image registration, where a new candidate mark is compared with existing marks to ensure no risk of confusing property ownership.
13. Architectural and engineering designer needs to be aware of previous designs, particularly if these can be adapted to the problem at hand. Hence the ability to search design archives for previous for previous examples which are in some way similar, or meet specified suitability criteria, can be valuable.

C. Flowchart of Proposed System

System components, the constituents of a system includes

1. Feature Extraction: An image is processed and extracted to obtain RGB values from the color of images.
2. Index Generation: With the help of hashing and signature, index and the secret key is generated.
3. Watermark Embedding: Watermark is embedded on image.
4. Image Encryption: For encrypted image format, Encryption algorithm i.e. AES encryption is used.
5. Trapdoor Generation: Trapdoor i.e. secret key which is generated at the time of index generation is generated.
6. Cloud Upload: A file is uploaded on a cloud server
7. Cloud Retrieved: Decrypted image format with no fraud and watermark is extracted, using the Decryption algorithm i.e. AES decryption, as well as watermark extraction algorithm.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

8. Relevance Feedback: Match result is displayed, i.e. relevant image result is displayed, using Relevance Feedback algorithm.

Flowchart of the Proposed System is as shown in figure2, which describes the stepwise flow of the proposed system.

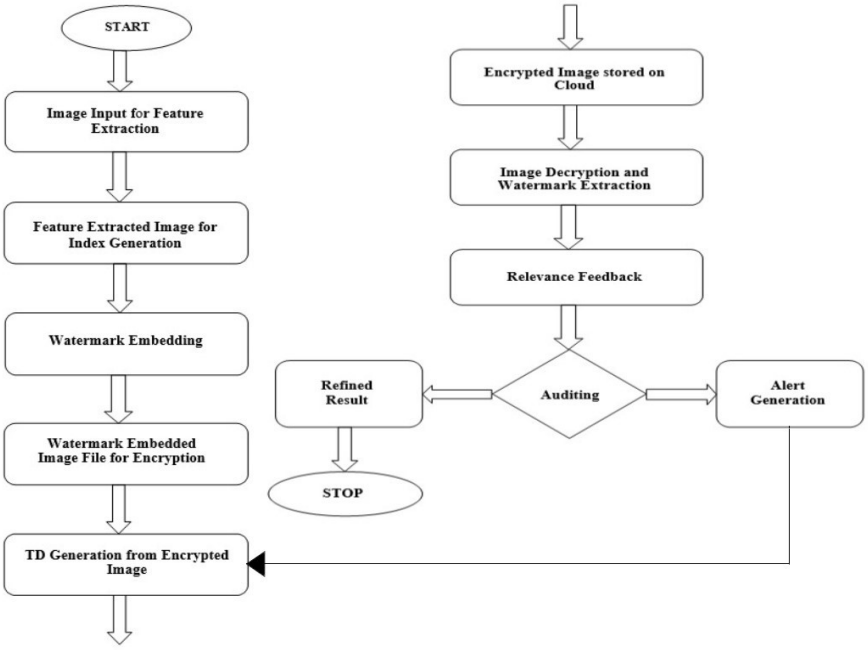

Fig.2: Flow chart of Proposed System

IV. PSEUDO CODE FOR PROPOSED SYSTEM

1. Encryption and Decryption Pseudo code

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[0, Nb-1])

   for round = 1 step 1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   out = state
end
```

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   for round = Nr-1 step -1 downto 1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
      InvMixColumns(state)
   end for

   InvShiftRows(state)
   InvSubBytes(state)
   AddRoundKey(state, w[0, Nb-1])

   out = state
end
```

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

2. Watermark Embedding and Extraction

$\mathcal{R}' \leftarrow \text{WatermarkEmb}(\mathcal{R}, w, k_{emb1}, k_{emb2}, k_{emb3})$

1. For each encrypted image $c \in \mathcal{R}$
   1) Divide c into $s \times s$ sized nonoverlapping blocks. The watermark is a sequence of binary bits denoted as $w = w_1, w_2, ..., w_{N_w}$. A set of blocks $\{BK_i\}_{i=1}^{N_w}$ are chosen by a pseudorandom function with the secret key k_{emb1}. Each block will carry one bit of the watermark.
   2) For each watermark bit $w_i, i \in [1, ..., N_w]$,
      a) The pixels in block BK_i are divided into two sets S_0 and S_1 according to a pseudorandom function with the secret key k_{emb2};
      b) If $w_i = 0$, flip the bits of pixels in S_0. Otherwise, flip the pixel bits in S_1. In order to preserve the image quality, we make less flipping on higher bit-planes. We denote the ratios of flipped bits on 8 bit-planes as $\epsilon = [\epsilon_1, \epsilon_2, ..., \epsilon_8]$. That is to say, for the i-th bit-plane, there are $N_w \times s^2 \times \epsilon_i/2$ bits will be flipped randomly. The flipped positions are determined by k_{emb3}.
2. Output the encrypted and watermarked image set $\mathcal{R}'$.

$w_t \leftarrow \text{WatermarkExtra}(m_t, m_o, k_{emb1}, k_{emb2}, k_{emb3})$

1. Divide m_t into nonoverlapping blocks with the size $s \times s$.
2. Locate the set of blocks $\{BK_i\}_{i=1}^{N_w}$ that carries the watermark bits $w = w_1, w_2, ..., w_{N_w}$ according to the secret key k_{emb1}.
3. For each $i \in [1, N_w]$,
   1) Divide the pixels in BK_i into two sets S_0 and S_1 according to the secret key k_{emb2};
   2) Flip the pixels in S_0 and S_1 respectively according to $[\epsilon_i]_{i=1}^{8}$ and k_{img3} to get two blocks BK_i^0 and BK_i^1. Construct the corresponding block BK_i from the original image with the secret key k_{emb1}. Calculate $\delta_0 = \sum_{p_j \in BK_i, p_j^0 \in BK_i^0} (p_j^0 - p_j)^2$ and $\delta_1 = \sum_{p_j \in BK_i, p_j^1 \in BK_i^1} (p_j^1 - p_j)^2$. If $\delta_0 < \delta_1$, the watermark bit is extracted as '0'. Else, the watermark bit is extracted as '1'.
4. Output the extracted watermark w_t.

3. Auditing Scheme

Following pseudocode is for trapdoor generation i.e. auditing. [11]

1. Start
2. Read data owner id(udoid)
3. If (doid ≠ udoid)
4. Stop
5. Read file name from AWS
6. Retrieve No. of blokes from TPA xml
7. Select the blocks number the user want to verify.
8. Get the auxiliary information for block chal from TPA xml
9. Based on Auxiliary information generate new root for MHT
10. If (new root ≠ root) file modified
11. Else File not modified
12. Stop.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

4. Relevance Feedback

Following pseudo code is for relevance Feedback. [3]

1. After the initial feedback, all the relevant images are used to build the Bayesian network and the link weights are calculated.
2. Perform the inference propagation to update the belief values of all the nodes in the network.
3. Select the relevant images whose belief is above the threshold as the positive feedback information.
4. Update the link weights using the chosen relevant images.
5. The updated belief values are set as new prior beliefs for the next iteration.
6. Start a new iteration of retrieval using the updated positive feedback information.
7. IF the user continues to give feedback judgement
8. New relevant objects get added to the network.
9. Go back to step 2 with the updated weights and prior beliefs.
10. Else stop the retrieval process and wait for the new query.

V. SIMULATION RESULTS

1. Time and Memory Comparison between AES and DES Algorithms

We have generated a small module which is built in C# and .net. It shows the time difference taken by the two algorithms DES and AES converting plain text into an encrypted form. We have calculated the time taken by each algorithm in milliseconds of encrypted data.

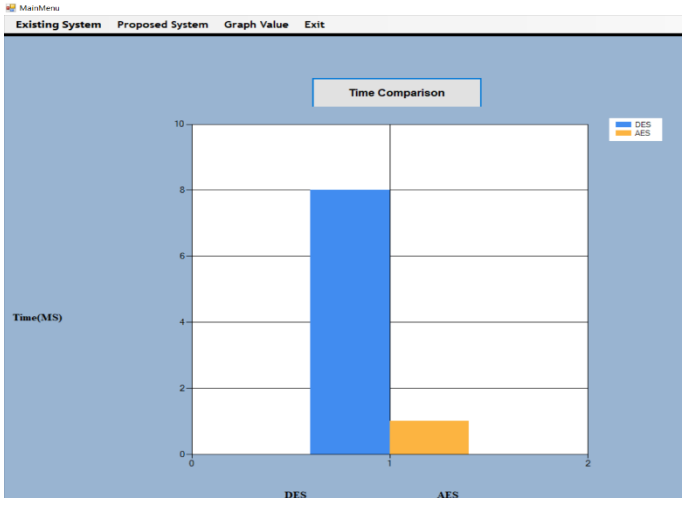

Fig.3:Time Complexity between Existing and Proposed System

Figure 4 shows generic scalability (memory usage & encryption performance) of the encryption algorithms. The analyses were derived from different researches. Bruce (2000) provides a comprehensive analysis of the performance of the five AES finalist showing approximated algorithm speed against on a variety of common software and hardware platforms. It is very difficult to compare cipher designs for scalability and even more difficult to design a cipher that is scalable among all platforms.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

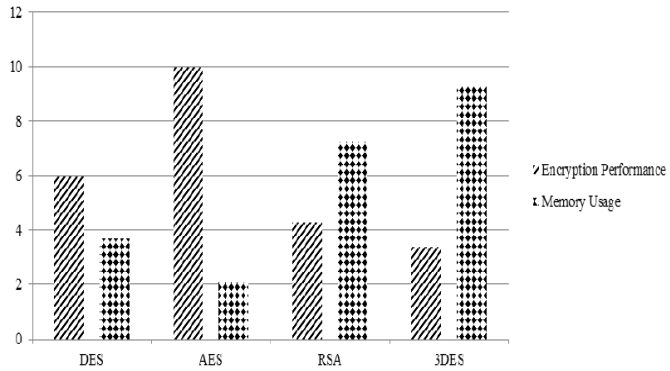

Fig.4:Generic Scalability (Memory Usage & Encryption Performance) of the Encryption algorithms

2. Time consumption of the trapdoor generation:

Similar to the index generation, the trapdoor generation incurs the calculations of bucket values, a splitting operation, and two matrix multiplications. The time complexity is $O(L\lambda l+l+l2)$. The time cost of the trapdoor generation is mainly dependent on the dimensionality of the visual descriptor [1], as illustrated in figure 5.

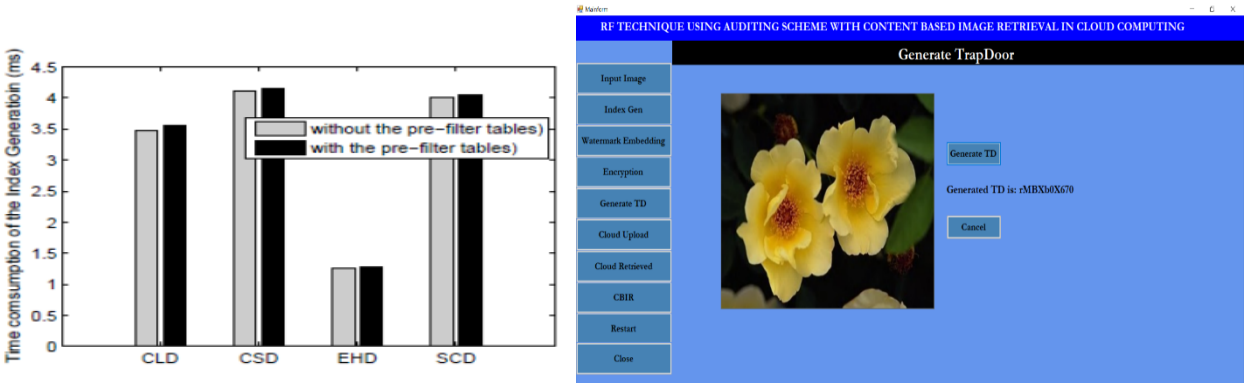

Fig.5: Time Consumption of the trapdoor generation, the data are averaged from 40 times of trapdoor generation

3. Performance Evaluation of Watermark Extraction Accuracy:

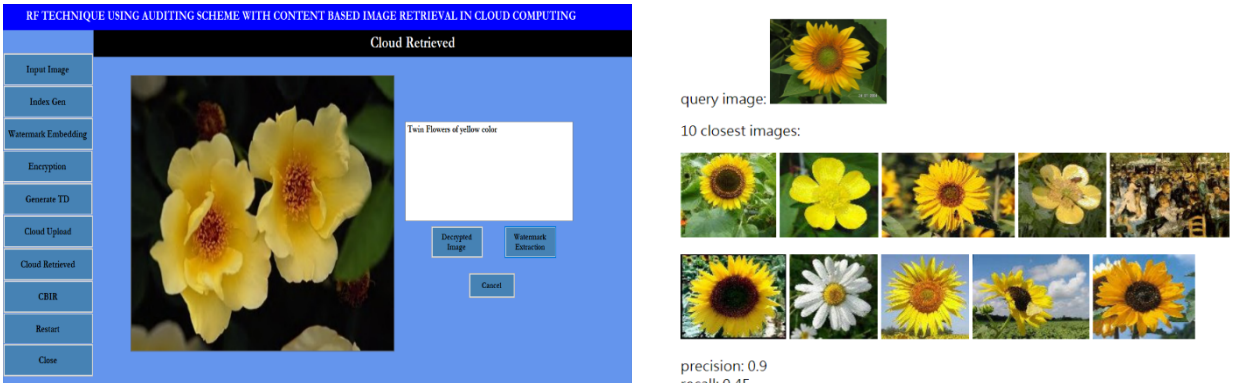

Fig.6:Accuracy result of watermark extraction (a) and (b)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Here in figure6, watermark extraction gives the accuracy result after performing experiments of precision and recall. Let us considered the following figures, where given the files of feature vectors already computed for the database and the reference to a query image, returns a list of images from the database in the order of the closest match to the query image.

1. Average of color and texture features are:
2. Compute color feature (Similarity)
3. Compute texture feature (Similarity)
4. Average of (normalized) color and texture feature.

4. Performance Evaluation of Relevance Feedback:

Relevance feedback is technique is used so that an input query image is matched with the dataset of images which are uploaded. Once the query image is matched with the one in image datasets then match result gives us information regarding refined result set, as shown in figure 7

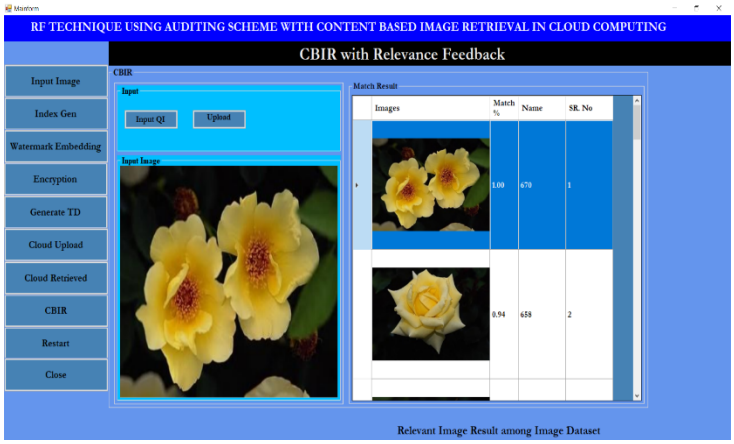

Fig.7:CBIR with Relevance Feedback

VI. CONCLUSION AND FUTURE WORK

The security of images is kept up by encryption with the assistance of AES calculations. The utilization of keyword-based user image gets to conspire upgrades user protection. Search proficiency is accomplished as the index is created utilizing a Locality-Sensitive Hashing method. We consider untrustworthy users in accessible encryption conspires and propose a watermark-based convention to decide the unlawful circulation of pictures.We proposed a methodology utilizing a Bayesian network as the relevant image adoption model is an incredible asset that is appropriate in the perspective of relevance feedback in image retrieval. To tackle the problem of imbalanced dataset causes the degradation in the retrieval results, a long-term learning approach based on random forest classifier is proposed. The long-term learning relevance feedback collects the user feedback, to train the random forest classifier, for improving the retrieval results.

VII. FUTURE WORK

As future work, there are still a few angles could be moved forward. Initially, the image access can be enhanced further to a higher level. Besides, the watermarking strategy can be framed to the better limit with better robustness and embedding capacity. One or more -clusters with the chosen relevant images belong to will be set as positive feedback information. The utilization of negative feedback will likewise be researched. High-speed image retrieval using CBIR is still a major challenge for researchers in academics and industry. Future work for long-term

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

learning relevance feedback is to use the indexing structures for the database to speed up the overall retrieval performance.

REFERENCES

1. Zhihua Xia, Xinhui Wang, Liangao Zhang 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, vol. 11, 2016, pp. 2594-2608.
2. Bavisha, M. Madlin Asha, "A keyword-based user privacy-preservation and copy-deterrence scheme for image retrieval in the cloud", in *International Journal of Innovation in Scientific and Engineering Research (IJISER)*, vol. 4, Issue JAN 2017/106.
3. Jing Xin, Jesse S. Jin, "Relevance feedback for content-based image retrieval using Bayesian Network", ACM-ICPS ACM International Conference Proceeding Series, pp. 91-94, VIP '05 Proceedings of the Pan- Sydney area workshop on visual information processing.
4. Lalit Kumar Saini, Vishal Shrivastava, "A survey of digital watermarking techniques and its applications", in *International Journal of Computer Science Trends and technology (IJCSTT)*, vol. 2, Issue 3, May/June 2014.
5. S. Banuchitra, Dr. K. Kungumaraj, "A comprehensive survey of content-based image retrieval techniques", in *International Journal of Engineering and Computer science (IJECS)*, vol.5 Issue Aug 2016, pp. 17511-17584.
6. Sonam Tyagi, Harsh Singh, "Digital watermarking techniques for security applications", in *International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems (ICETEESES-16)*
7. Puja Kumar, "Image retrieval relevance feedback algorithms: trends and techniques", in *International Journal of Scientific Engineering and Technology*, vol. 2 Issue No. 1, pp. 13-21.
8. Urvi H. Panchal, Rohit Srivastava, "A comprehensive survey on digital image watermarking techniques", in *Fifth International Conference on Communication Systems and Network Techniques 2015*.
9. Zhan Qin, Jingbo. Yan, Ki, Ren, Chang Wen Chen, Cong Wang, "Towards Efficient privacy-preserving Image Feature Extraction in cloud computing", in *22nd ACM International Conference on Multimedia*, 2014, pp. 497-506
10. Z. Xia, Y. Zhu, X. Sun, Z. Qin and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing", IEEE Transactions on Cloud Computing, vol. 99, 2015, pp. 1-10
11. Shivaji R. Lahane, Sonal H. Kunte, "Using watermark-based protocol, increase robustness and privacy of CBIR in cloud computing", in *International Journal of Advanced Research and Innovative Ideas in Education (IJARIIE)*, vol.3, Issue-4 2017, pp. 1853-1860
12. Nasir Memon, Ping Wah Wong, "A buyer-seller watermarking protocol", IEEE Transactions on Image Processing, vol. 10, no. 4, April 2001, pp. 643-649
13. Eu-Jin Goh, "Secure Indexes"; in IACR Cryptology ePrint Archive 2004
14. K. Belattar and S. Mostefai, "CBIR using relevance feedback: comparative analysis and major challenges", *5th International Conference on Computer science and Information Technology (CSIT)*, IEEE, pp. 317-325
15. Sakshi Shivhare, Vijay Trivedi and Vineet Richhariya, "Content-based image retrieval by using Interactive relevance feedback technique- A survey", in International Journal on Recent and Innovation Trends in Computing and Communication July 2015 (IJRITCC), vol. 3, Issue 7, pp. 4641-4646
16. Aarti Datir, Dipak Patil "Survey on different techniques of CBIR", in *International Journal of Science Technology Management and Research (IJSTMR)*, vol. 1 Issue 8, Nov 2016, pp. 29-34
17. Ajinkya sabale, Rohit Prajapati, Sameer Patahn, Sanket Prabhu, Sanjay Agrawal, "Third-party auditing of data on a cloud with fine-grained updates", in *International Journal of Engineering and Computer Science (IJECS)*, vol. 4, Issue 11, Nov 2015, pp. 14987-14992
18. Milind Mathur, Ayush Kesarwani, "Comparison between DES, 3DES, AES, RC2, RC6,and Blowfish", in *National Conference on New Horizons in IT-NCNHT* 2013, pp. 143-148
19. Galibarov Pavel, "Embedding, Extraction,and Detection of Digital Watermark in Spectral Images", Master Thesis accepted by *Council of Department of Information Technology* on Oct. 2003, pp. 1-51
20. Zhihua Xia,Xinhui Wang, Xingming Sun, Qian Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data", IEEE Transactions on Parallel and Distributed Systems, Vol. 27, no.2, Feb 2016.
21. K. Gopalakrishnan and Nasir Memon, "Protocols for Watermark Verification", IEEE Transaction on Multimedia and Security, pp. 66-70, Oct-Dec 2001.
22. B. S. Manjunath, Jens-Rainer Ohm, Vinod V. Vasudevan,and Akio Yamada, "Color and Texture Descriptors", IEEE Transaction on Circuits and Systems for Video Technology, Vol. 11, no. 6, June 2001
23. Nilesh Bhosle, Manesh Kokare, "Random forest-based long-term learning for CBIR", IEEE 2016 International Conference on Signal and Information Processing (IConSIP).