A KEYWORD BASED USER PRIVACY-PRESERVATION AND COPY-DETERRENCE SCHEME FOR IMAGE RETRIEVAL IN CLOUD

[1]T.E. Bavisha, [2]Ms.M.MadlinAsha

[1]PG Scholar Department of Information Technology, Vivekanandha College of Engineering For Women(Autonomous) Thiruchengodu,India.

[2]Assistant Professor Department of Information Technology, Vivekanandha College of Engineering For Women(Autonomous) Thiruchengodu,India.

[1]bavesjey@gmail.com [2]madlinasha.jesus88@gmail.com

Abstract: An Image plays an important role in human life and it consumes more storage space than other formats. Hence, the need for cloud storage outsourcing is demanded. Privacy of users and image transfer in network is a main concern. To ensure 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 furthermore, the illegal publication of user images is traced with the help of watermark-based protocol.

Keyword: Double RSA Encryption/Decryption, Watermark, User Keyword, locality Sensitive Hashing (LSH).

1. INTRODUCTION

1.1 Cryptography

Cryptography is the study of techniques for secure communication and its application in the presence of third parties. In day-to-day life, encryption is an important tool in many areas of engineering, medicine, communication, image and video processing. Hence the security of digital images has become important due to the rapid development on the internet and the digital world. Encryption techniques used for images covert the images into another one that is harder to understand and completely non-accessible for the third party. And during decryption the original images are retrieved.

B. Rivest-Shamir-Adleman (RSA)

The steps involved in RSA double key image encryption algorithm is described below:

- Select two prime numbers p and q. (prime number is a number divisible only by that number and 1)
- Calculate N value, by multiplying p and q.
- Note $ø(N)=(p-1)(q-1)$
- Selecting at random encryption key e, where $1<e<ø(N)$, $gcd(e,ø(N))=1$
- Solve the following equation to find decryption key d, $e.d=1 \mod ø(N)$ and $0≤d≤N$
- Publish their public encryption key: $KU=\{e,N\}$
- Keep secret private decryption key: $KR=\{d,p,q\}$
- From the sender side, to provide the authentication we use the key as ep, it can be calculated as the form similar to the calculation of e, like $ep.dp=1 \mod ø(N)$ and $0≤d≤N$.
- The receiver side we provide the authentication by using the private key as dp, by randomly.

Contribution – This paper protects the privacy of image users and security for images both during storage and access against curious outsiders. The main contributions are listed as follows:

- User Data’s are collected by the administrator with a keyword(like a nick name) and generates an Id with the keyword given and concatenates the keyword with the user image name .Sends the result of concatenation and UID to the user.
- An index table is created with the UID and the user images with the names after concatenation.
- Administrator stores the index table and the encrypted database in a cloud server. The cloud server.

- The user searches for a particular image with the name after concatenation and the UID in encrypted form.
- The Watermark is added to the user image with his/her unique watermark bits.
- The user decrypts the image using the private key, a watermarked original image is obtained.

The rest of this paper is framed as follows. Section II introduces the related works. Section III gives a brief introduction to the system model, threat model, and design goals. The Proposed scheme is explained in Section IV. Section V gives conclusions.

2. RELATED WORKS

Secure trapdoor generation without leaking content of the user data is described by developing the fine-grained multi-keyword search schemes over encrypted cloud knowledge[5], [7]. A survey and review on keyword based search techniques used in cloud discusses about the various techniques available and it's working [10], [11].

A searchable encryption scheme enables the users to search over an encrypted image collections. A plenty of methods have been proposed under various threat models to achieve the search functionalities, like similarity search [18] [20], dynamic search [21], [22]. However, some of these schemes are feasible to retrieval of an image.

A two factor authentication for enhancing security of users by generating one time password [16] is explained by Neha Vishwakarma and Kopal Gangrade. The watermarking techniques have been widely discussed in buyer – seller scenarios [23] – [26].

The security of images during transfer is enhanced with the concept of splitting [12] – [15] the whole image into chunks as referred as segmentation. The conversion of original image into hidden format (i.e. cipher image) is chosen with the comparison and survey [1], [6], [9] and [17] among different varieties of encryption [3] algorithms in cryptography.

3.PROBLEM FORMULATION

3.1System model

The system model proposed in this paper consists of seven different entities:the image user, the administrator, cloud server, OTP generator, Watermark Certificate Authority(WCA) and image refinement, as explained in Fig.1.

Image User wants to outsource his collection of n images, i.e., M = { m1,m2,m3,..., mn }, to the cloud server hence he registers to an administrator with an unique keyword.

Image Administrator – Collects user information and generates UID with user given keyword and encrypts his images after renaming Image and creates index table using encrypted data's to enhance search efficiency. Administrator sends user data to cloud server. Administrator sends User ID to Watermark Certificate Authority.

Cloud Server - Stores administrator data and searching is carried out based on user request.

Watermark Certificate Authority (WCA) - Itsresponsibility is to generate watermarks for the authorized users and executes adjudication through the extraction algorithm.

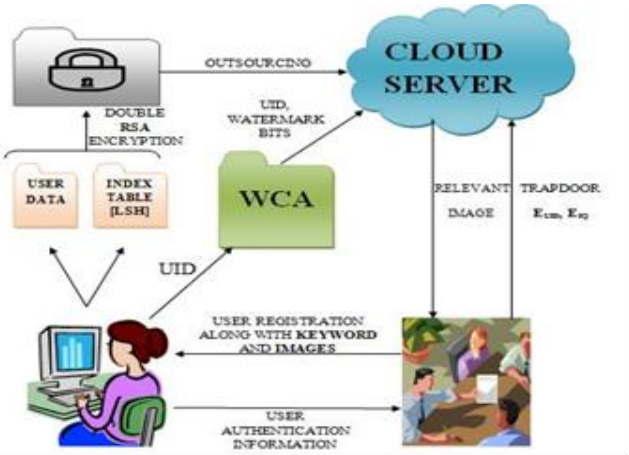


Figure 1: Framework of the keyword based user privacy-preservation and copy-deterrence scheme for image retrieval

3.2Threat model

In our scheme, the administrator, image users, and cloud server could provoke security complications. In this proposal, three security problems are mainly considered.

User privacy - The user access means can be obtained and used by an unauthorized person. Thus, the user privacy has to be maintained properly.

Data privacy - The cloud server keeps and analyzes the data communication so as to access fragile information. Thus, the privacy of image and trapdoors needs to be properly protected.

Copyright - The illegal distribution of images has to be determined and preserved.

3.3 Design goals

Efficiency – The use of linear search scheme is a bit inefficient and computationally impractical for a massive database. The proposed approach aims to attain a better efficiency than linear approach by developing encrypted index table.

Security - Based on the threat model, the security requirements are achieved in the proposed scheme by the following:

User privacy – The user registration information or his keyword needs to be kept unknown to the cloud server.

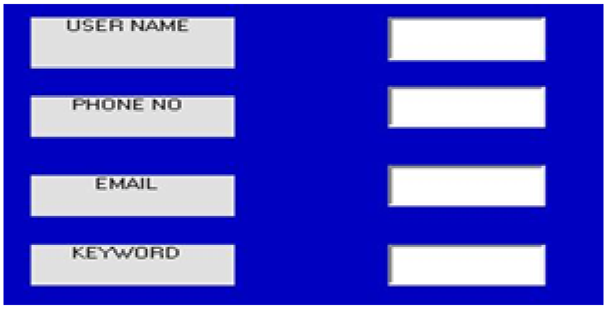
Data privacy - The image content and the trapdoor information have to be kept unknown to the cloud server.

Copyright – The watermark based protocol needs to be able to depict the illegal distribution.

4. THE PROPOSED SCHEME

4.1User Registration

Register's to the administrator along with the keyword and their images. The keyword the user gives is checked with the administrator database for any existence and is processed. Fig.2. illustrates the details given by the user for registration.



USER NAME

PHONE NO

EMAIL

KEYWORD

Figure 2: User registration details

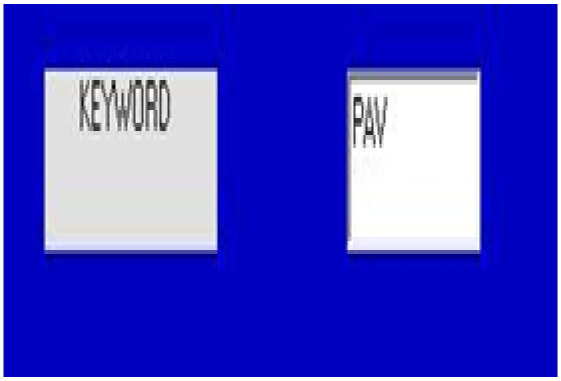
4.2 UID generation

A pseudo random number is generated and is concatenated with the keyword given by the user.A pseudorandom number generator is an algorithm which is used for the generation a sequence of numbers. The pseudorandom number sequence generated will not be truly random, because it is completely determined by a small set of initial values, called seed. For instance, the Fig.3 represents the pseudo random number generated for UIDGEN. Fig.4 represents the keyword given by the user.

PSEUDO RANDOM

77475

Figure 3: Pseudo Random Number generated

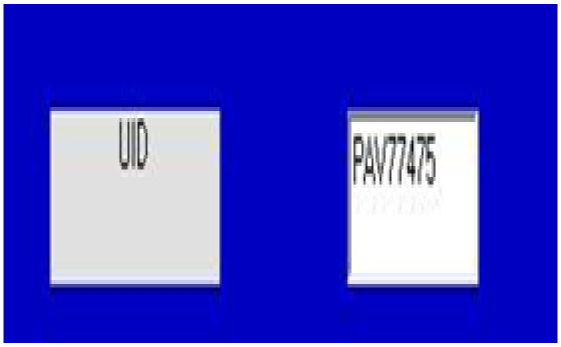


KEYWORD

PAV

Figure 4: Keyword given by the user

The final UID generated by the concatenation process is represented in Fig.5.



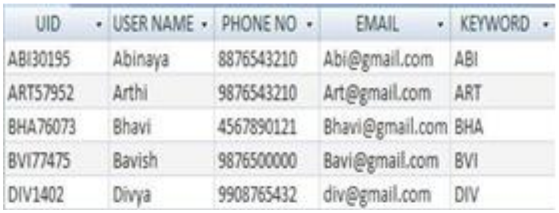
UID

PAV77475

Figure 5: Generated UID

4.3 Administrator

The user data's given for registration is stored in administrator database which will resemble as shown in Fig.6.



UID	USER NAME	PHONE NO	EMAIL	KEYWORD
ABI30195	Abinaya	8876543210	Abi@gmail.com	ABI
ART57952	Arthi	9876543210	Art@gmail.com	ART
BHA76073	Bhavi	4567890121	Bhavi@gmail.com	BHA
BVI77475	Bavish	9876500000	Bavi@gmail.com	BVI
DIV1402	Divya	9908765432	div@gmail.com	DIV

Figure 6: User details in database

4.4 Image Renaming

The image name is concatenated with the user given keyword so that the user and data privacy can be achieved efficiently.Table.1 represents the image renaming process.

Table.1 Image renaming representation

IMAGE NAME	IMG_2649
KEYWORD	PAV
RENAMING IMAGE	PAVIMG_2649

The user will already know the image renaming process, it is carried out as an important process by the administrator for privacy concern.

4.5 Index generation

The administrator generates an index table with the help of Locality Sensitive Hashing (LSH) technique. In LSH technique, hashes the input items so that the items which are similar can be mapped together in a single bucket. This technique is more in common with clustering and search based on nearest neighbor method. A hash function family H

$= \{ h : T \rightarrow V \}$ is known as (c,cr,p1,p2) sensitive, when p1> p2.

Based on the name of the images and the UID, the index table is generated. Sample Index table is shown in Table.2. Bucket creation which is carried out with the help of clustering and is carried out by using "Specific Keywords".

Table 2: Bucket creation using LSH technique

UID	IMAGES		
PAV 77475	PAV IMG_2649	PAV IMG_1826	PAV IMG_2089
BHA 76073	BHA ROSE	BHA IMG_765	BHA 1234

4.6 Encryption of user data

The Double RSA approach is used to convert the original data into a cipher data, where the content is hidden from being accessed. The encryption by the administrator is done with the private key (x) and public key (xp).

$$H = M^{x} \bmod N \qquad (1)$$

$$E = H^{xp} \bmod N \qquad (2)$$

The equations (1) and (2) can be combined and written as,

$$E = (M^{x} \bmod N)^{xp} \bmod N \qquad (3)$$

Where H denotes the cipher data, M denotes the message to be encrypted, N = pq, E is the encrypted image, x denotes sender's private key, xp denotes sender's public key. The public key is sent to the user to generate his own private key.

4.7Trapdoor generation

The receiver can generate his own private key (y) with the help of sender's public key (yp).

$$M = E^{y} \bmod N \qquad (4)$$

$$D = M^{yp} \bmod N \qquad (5)$$

The equations (4) and (5) can be combined and written as,

$$D = (Ey \bmod N)yp \bmod N \qquad (6)$$

Hence with the help of generated private key, the UID and the image name (i.e. renamed image name) is encrypted using this private key. The user request is carried out with encrypted names (EUID , EIQ).

H. User side

Finally, the received image is decrypted by using private key generated by the user and the original image along with the watermark is obtained.

4.8 Watermark-based protocol

In the embedding process, the watermark bits generated are embedded into the least-significant bit (LSB) of the image.

If an unauthorized copy of image is found, the image owner will submit both the unauthorized copy and the corresponding original version to WCA which then extracts the watermark by WatermarkExtra.

The extracted watermark is used to identify the illegal user.

5. CONCLUSION

The security of images is maintained by encryption with the help of Double RSA techniques. The use of Keyword based User image access scheme enhances user privacy. Search efficiency is attained as the index table is generated using Locality sensitive Hashing technique. The illegal distribution of images is determined as watermark based protocol is used. Overall, the images and their contents are secure against cryptography attacks. The privacy of images, users, and copyright for images are highly achieved.

As future work, there are still some aspects could be improved. Firstly, the image access can be enhanced further to a higher level. Secondly, the watermarking technique can be framed to better capacity.

REFERENCES

[1] SamreenSekhonBrar, AjitpalBrar, “Double layer image security system using Encryption and Steganography,” I.J. Computer Network and Information Security, 2016, 3, 27-33.

[2] NookaSaikumar, R. Bala Krishnan, S. Meganathan, N. R. Raajan, “An Encryption Approach for security Enhancement in images using Key Based Partitioning Technique,” 2016 International Conference on Circuit, Power and Computing Technologies[ICCPCT].

[3] M. Madlin Asha, Dr.J. Jennifer Ranjani, “Secure Image Retrieval using Pyramid Histogram of Oriented Gradient Descriptor”,.

[4] C.-Y. Hsu, C.-S. Lu, and S.-c. Pei, “Image feature extraction in encrypted domain with privacy-preserving sift,” Image Processing, IEEE Transactions on, vol. 21, no. 11, pp. 4593–4607, Nov 2012.

[5] Mrs.M.Anandhi, S.Karthi, “Secured Data Transmission in Cloud Using Trapdoor Encryption”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016.

[6] Verma O.P., Agarwal R., Dafouti D., “Performance analysis of data encryption algorithms”, ICECT, vol. 5, pp. 399-403, IEEE, 2011.

[7] Muhammad Sajid Khan, Chengliang Wang , Ayesha Kulsoom, ZabeehUllah, “Searching Encrypted Data on Cloud” , IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013.

[8] Gary C.Kessler, “An Overview of Cryptography: Cryptographic”, HLAN, ver. 1, 1999-2014.

[9] Milind Mathur, Ayush Keasarvani” Comparison betweenDES, 3DES,RC2,RC6, BLOWFISH and AES”,NCNHIT vol.1 143-148,2013.

[10] Ms. Jabeenakkalkot, ms. S. Shanmugpriya, “A survey on keyword-based search mechanism for data stored in cloud”, IJCSMC, Vol. 5, Issue. 5, May 2016.

[11] VimmiMakkarSandeepDalal, “ Techniques of keyword search over cloud data A Review”, International Journal of Computer Applications & Information Technology Vol. 3, Issue I June-July 2013.

[12] A.D. Jepson and D.J. Fleet, “Image Segmentation”, 2007.

[13] R.Yogamangalam, B.Karthikeyan, “Segmentation Techniques Comparison in Image Processing”, International Journal of Engineering and Technology (IJET), ISSN : 0975-4024, Vol 5 No

1 Feb-Mar 2013.

[14] SD Yanowitz, AM Bruckstein ,"A new method for image segmentation" on Computer Vision, Graphics, and Image, 1989.

[15] M Celenk ,"A color clustering technique for image segmentation" on Computer Vision, Graphics, and Image Processing, 1990.

[16] Neha Vishwakarma, Kopal Gangrade, "Secure Image Based One Time Password", International Journal of Science and Research (IJSR), Volume 5 Issue 11, November 2016.

[17] Aarti Devi, Ankush Sharma and Anamika Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption," in International Journal of Computer Science and Information Technologies, Vol. 6, No. 3, 2015.

[18] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Proc. of 28th International Conference on Data Engineering. IEEE, 2012, pp. 1156–1167.

[19] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proc. of INFOCOM. IEEE, 2012, pp. 451–459.

[20] Z. Xia, Y. Zhu, X. Sun, and L. Chen, "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking," Journal of Cloud Computing, vol. 3, no. 1, pp. 1–11, 2014.

[21] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. PP, no. 99, p. 1,2015.

[22] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security. Springer, 2013, pp. 258–274.

[23] S. Katzenbeisser, A. Lemma, M. U. Celik, M. Van Der Veen, and M. Maas, "A buyer– seller watermarking protocol based on secure embedding," Information Forensics and Security, IEEE Transactions on, vol. 3, no. 4, pp. 783–786, 2008.

[24] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proceedings of the 11th ACM workshop on Multimedia and security. ACM, 2009, pp. 9–18.

[25] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," Information Forensics and Security, IEEE Transactions on, vol. 5, no. 4, pp. 920– 931, 2010.

[26] Zhihua Xia, 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 Transaction on Information Forensic and Security, vol. , No. 11 , September 2016.