INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue3)
Available online at www.ijariit.com

A Trinity Approach for Secure Image Access and Retrieval in Cloud

T. E Bavisha
PG Scholar
Department of Information Technology,
Vivekanandha College of Engineering
For Women(Autonomous),
Tiruchengode, India.
bavesjey@gmail.com

M. Madlin Asha
Assistant Professor
Department of Information Technology,
Vivekanandha College of Engineering
For Women(Autonomous),
Tiruchengode, India.
madlinasha88.jesus@gmail.com

Abstract: Images plays an important role in human's day to day life and it consumes much more space for storage rather than other formats. Hence, the need for cloud storage outsourcing arises. The Privacy of user and transfer of images in the network is the main concern. For privacy-preservation purposes, sensitive images, such as medical and personal images are needed to be encrypted before outsourcing, which makes the CBIR technique on plaintext realm to be inoperative. To ensure user privacy, a keyword based technique is introduced to provide individuality for the users. User validation for accessing their images from the cloud is provided by generating an OTP. The cryptography and segmentation techniques are upholding image security during transfer. Additionally, the illicit publication of user images is recognized with the help of watermark extraction.

Keyword: User Keyword, One Time Password (OTP), AES 128 bit Encryption/Decryption, Watermark, Segmentation, Least Significant Bit (LSB) Steganography, and Locality Sensitive Hashing (LSH).

I. INTRODUCTION

The expansion of the imaging devices, like digital cameras, smartphones, and medical imaging tools, our planet has been witnessing an incredible development in quantity, availability, and importance of images. The requirements for efficient image storage and retrieval are strengthened by the rise of large-scale image databases. CBIR techniques confirm the potential of helpfulness in many applications. However, a large image database consists of millions of images. And CBIR services usually acquire high storage and computation complexities. Cloud offers an immense opportunity for the on-demand access to sufficient computation and resources for storage, which makes it a striking choice for the image storage and outsourcing.

We have used many insecure channels for transferring our images with the internet. However, on a certain point, it's not secure. Cryptography and steganography are two ways that use the information to convert it into a cipher data or conceal their existence correspondingly which might be used to transfer information in an obscured manner.

A. 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 of the internet and the digital world. Encryption techniques used for images convert 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. Advanced Encryption Standard (AES)

The number of repetitions of transformation rounds is specified based on the key size that converts the input (plain image) into final output (cipher image). The number of cycles for repetition will be 10 rounds. Each round consists of four similar but different stages, including one that depends on the encryption key itself. The Steps are as follows,

1. Add Subkey,
2. Byte Substitution,
3. Shift Row,

4. Mix Column.

For decryption, a set of reverse rounds is applied to transform cipher image back to the original image using the same key used for encryption.

C. One Time Password (OTP)

An OTP is a password that is valid only for one login session for any digital devices. The most important advantage of OTP in contrast with static passwords are that they are not vulnerable to replay attacks. The OTP generation is carried out with the help of random or pseudorandom numbers and also hash functions are used to make a prediction of successor OTP's difficult.

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:

1. User data are collected by the administrator with a keyword (like a nickname) 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.
2. An index table is created with the UID and the user images with the names after concatenation.
3. Administrator stores the encrypted index table and the encrypted database in a cloud server.
4. If the user searches for a particular image with the name after concatenation and the cloud server finds it available then, an OTP is generated and sent to the user's phone number through SMS service.
5. And is validated with the OTP database in a cloud server. If the OTP matches, the images are processed for transmission in the network. If the OTP validation fails then, the user asks to resend OTP.
6. The Watermark is added to the user image with his/her unique watermark bits and is divided into chunks using and is again encrypted using AES 128bit algorithm and is sent to the user. Sends key to the user.
7. The user decrypts the image using the key sent and frames the chunks into a whole image. And finally, when the cipher image is decrypted with the key given, 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.

II. 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 of keyword-based search techniques used in cloud discuss the various techniques available and it's working [10], [11].

A searchable encryption scheme enables the users to search over encrypted image collections. A plenty of methods has 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 the 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 an original image into a 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.

III. PROBLEM FORMULATION

A. System 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., $M = \{m1, m2, m3,..., m_n\}$, to the cloud server hence he registers to an administrator with a unique **keyword**.

Image Administrator – Collects user information and generates UID with the user given a 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 the cloud server. Administrator sends User ID to Watermark Certificate Authority.

Cloud Server: Stores administrator data and searching are carried out based on user request and invokes OTP generator. Embeds watermark bits to user images.

OTP Generator: If the user query for a particular image is found, an OTP is sent to user phone through SMS service. And it validates the OTP which is present by the user. If the user is valid, the image refinement process is carried out.

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

Image Refinement - The combination of segmentation and encryption of resultant image.

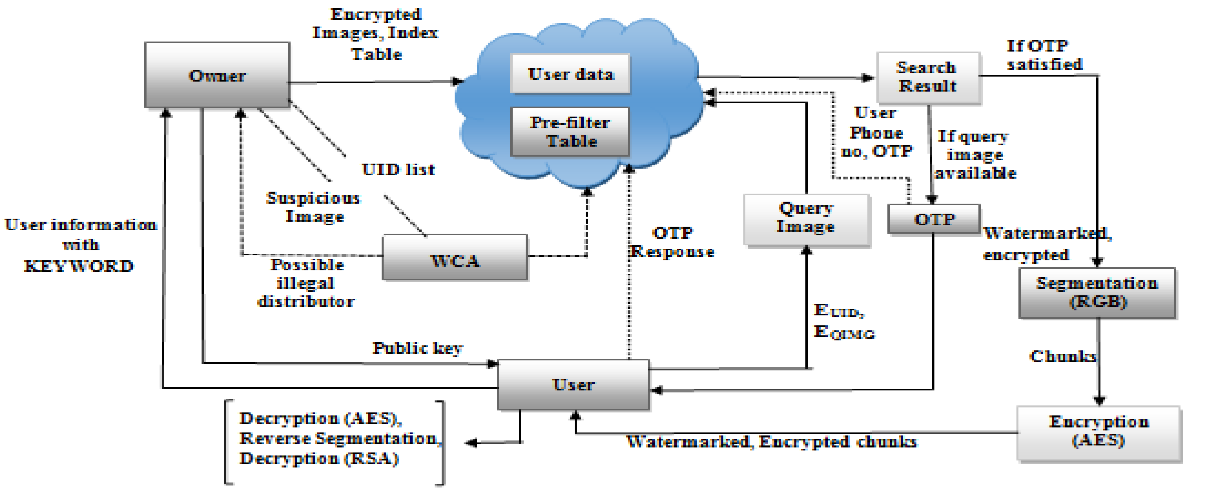


Fig.1. Framework of the trinity approach

B. Threat 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.

C. 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.

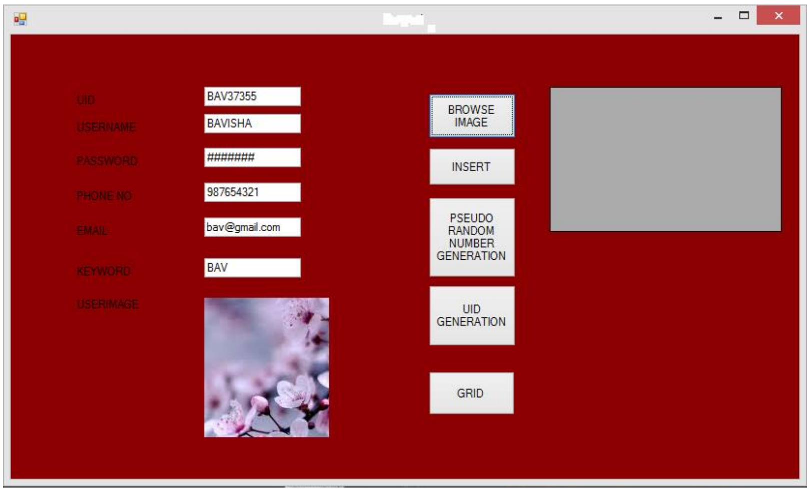
Data privacy **-** The image content and the trapdoor information have to be kept unknown to the cloud server.

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

IV. THE PROPOSED SCHEME

A. User 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.

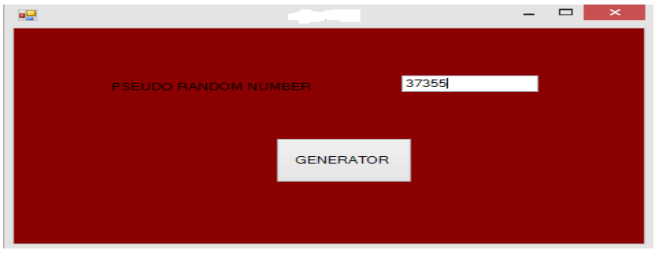


UID	BAV37355
USERNAME	BAVISHA
PASSWORD	########
PHONE NO	987654321
EMAIL	bav@gmail.com
KEYWORD	BAV
USERIMAGE	

Fig.2. User registration details

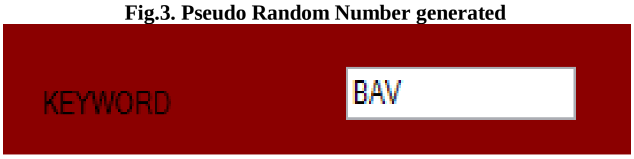
B. UID generation

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 a seed. For instance, the Fig.3 represents the pseudo random number generated for UIDGEN. Fig.4 represents the user given keyword.



PSEUDO RANDOM NUMBER 37355

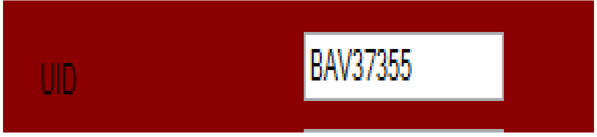
Fig.3. Pseudo Random Number generated



KEYWORD BAV

Fig.4. user given keyword

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

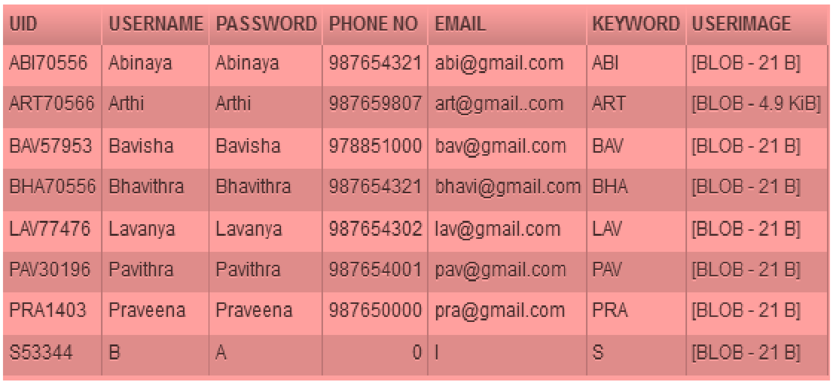


UID BAV37355

Fig.5. Generated UID

C. *Administrator*

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



UID	USERNAME	PASSWORD	PHONE NO	EMAIL	KEYWORD	USERIMAGE
ABI70556	Abinaya	Abinaya	987654321	abi@gmail.com	ABI	[BLOB - 21 B]
ART70566	Arthi	Arthi	987659807	art@gmail..com	ART	[BLOB - 4.9 KiB]
BAV57953	Bavisha	Bavisha	978851000	bav@gmail.com	BAV	[BLOB - 21 B]
BHA70556	Bhavithra	Bhavithra	987654321	bhavi@gmail.com	BHA	[BLOB - 21 B]
LAV77476	Lavanya	Lavanya	987654302	lav@gmail.com	LAV	[BLOB - 21 B]
PAV30196	Pavithra	Pavithra	987654001	pav@gmail.com	PAV	[BLOB - 21 B]
PRA1403	Praveena	Praveena	987650000	pra@gmail.com	PRA	[BLOB - 21 B]
S53344	B	A	0	I	S	[BLOB - 21 B]

Fig.6. User details in SQL database

D. *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.

E. *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,o_r,p_1,p_2) sensitive, when $p_1 > p_2$.

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”.

F. Encryption of user data

The advance encryption standard is used for the purpose of encryption in the proposed model. The AES algorithm is a symmetric encryption model used to encrypt the various forms of data in the different round information. The proposed model is using the 128-bit key length based encryption algorithm with the 128-bit block size and with 10-encryption rounds.

The user request is carried out with encrypted names (E_{UID}, E_{QIMG}). An OTP is generated if the requested image is available.

G. One Time Password (OTP) generator

Secure Hash Algorithm (SHA) is used for OTP generation. If the image is available, the cloud server invokes OTP generator and sends OTP to the user to enhance user privacy. OTP is sent to user mobile phone through SMS service. Maintains a database in cloud server hence, the recent OTP by the user can be validated. Fig. 7 represents the functioning of OTP in this proposal.

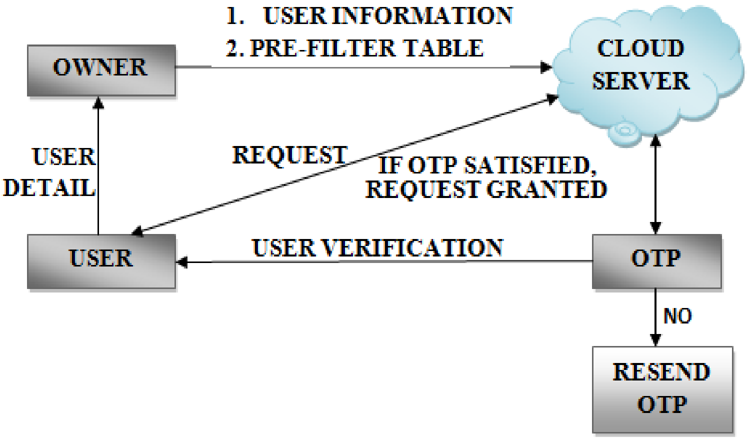


Fig.7. OTP Functioning

H. Image Refinement

1. Segmentation

Each image is classified based on its height and width. The segmentation is carried out based on their row and column initialization. Figure 9 represents the chunks images formed. The figure shown below is segmented as 4 rows and 4 columns.

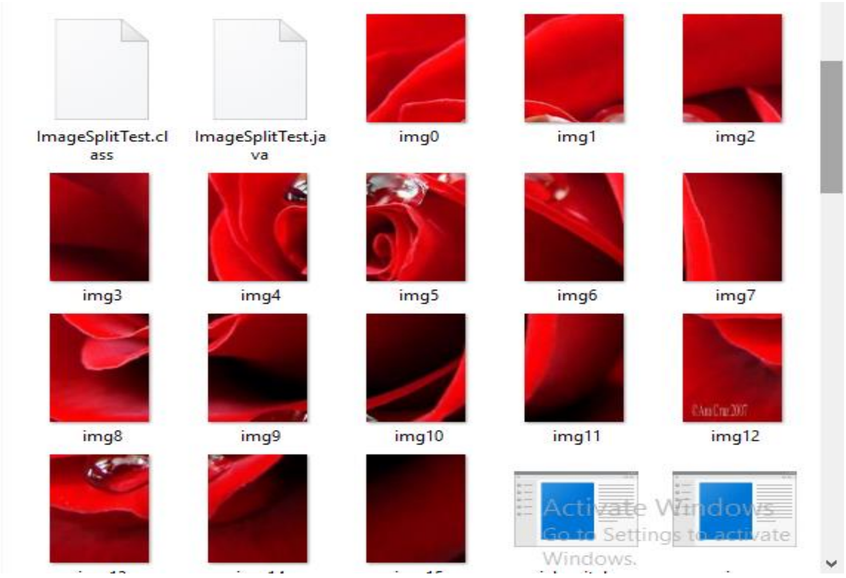


Fig.9. Chunks formed after segmentation process

2. *Encryption of chunks*

Subsequently, encrypt the image part using AES technique. Likewise, the whole process continues till all the chunks are decrypted. Thus image fragments are created. Each image part is the same size of original image. Fragments number depends on the range taken for splitting. Then the encrypted image parts are sent to the receiver. The encryption key is sent using mail to the user. Figure 10 shows the encrypted image.

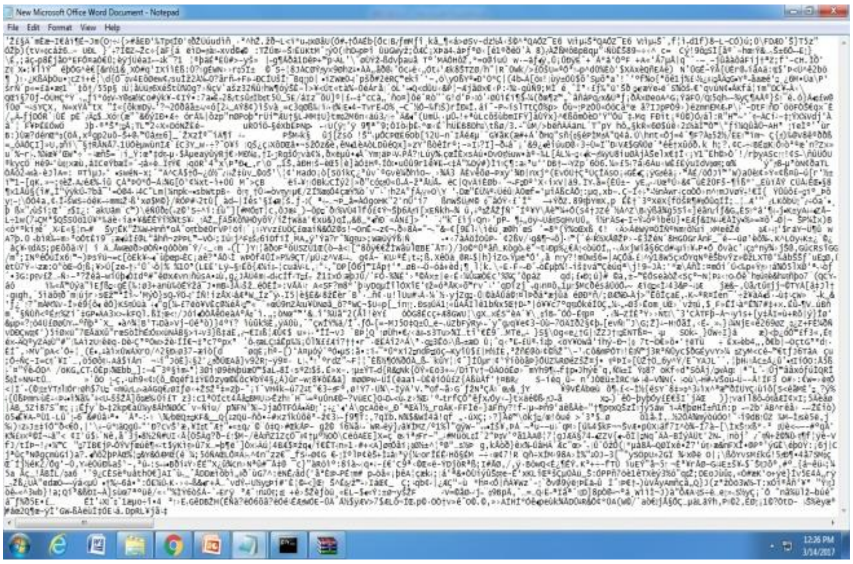

New Microsoft Office Word Document - Notepad
File Edit Format View Help
12:26 PM
3/14/2017

Fig.10. AES – 128bit encrypted image

I. *User side*

Decryption of image chunks takes place at the user side. Each chunk is decrypted by the AES key sent to the user. The process is continued until all image parts are obtained. Then, the image chunks are framed together with the help of segmentation key. Finally, the formed image is decrypted by using the private key generated by the user and the original image is obtained. Fig.11. User side framework.

J. *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 the 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.

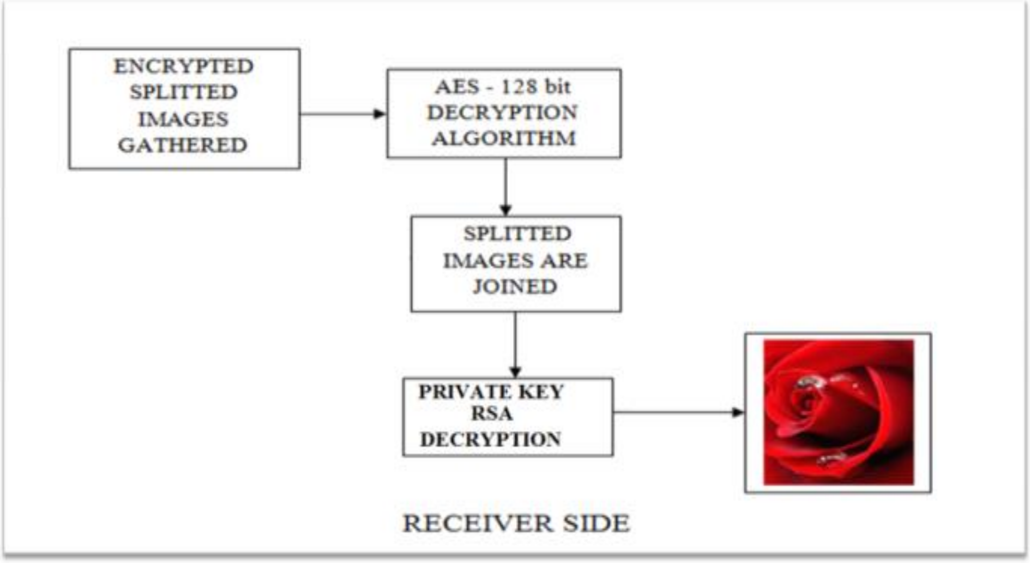

ENCRYPTED SPLITTED IMAGES GATHERED
AES - 128 bit DECRYPTION ALGORITHM
SPLITTED IMAGES ARE JOINED
PRIVATE KEY RSA DECRYPTION
RECEIVER SIDE

Fig.11. User side framework

CONCLUSION

The security of images is maintained by double time encryption with the help of AES-128 bit techniques. The use of Keyword based User image access and OTP validation scheme enhances user privacy. Search efficiency is attained as the index table is generated using Locality Sensitive Hashing technique. The segmentation of encrypted images provides more security during transfer. The illegal distribution of images is determined as the 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] Samreen Sekhon Brar, Ajitpal Brar, “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 an 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 UsingTrapdoor 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] MilindMathur, AyushKesarwani, “Comparison between DES, 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), and 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.