ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Privacy Preserving Personalized Data by Sobel Edge Detection in Hybrid Cloud

Archana S[1], Mariya Anthony Selvi A[2], Jothi V[3], Ragu G [4], Dr. R. Janarthanan [5]

B.E. Scholar, Department of CSE, T.J.S Engineering College, Chennai, India [1,2,3]

Assistant Professor, Department of CSE, T.J.S Engineering College, Chennai, India [4.]

Professor, Department of CSE, T.J.S Engineering College, Chennai, India[5.]

ABSTRACT: The industry of cloud gives a service paradigm of storage/computation outsourcing, which helps to reduce user's burden and reduce the cost for both the enterprises and individual users. A great number of images are captured by image sensors every day and the dramatically increasing number is drawing to people's concerns for big image data storage and privacy. To protect the image privacy, people are accustomed to store the image data in the private cloud of their own, as the private cloud, in general, is credible. But with the expansion of big image data, the storage space in the private cloud is not vast enough. Thus, the private cloud has to seek help to the public cloud which possesses abundant storage and computing resources. However, the public cloud is often not trusted.

KEYWORDS: Image storage, Secure Big image data service, private cloud, public cloud, Sabel Edge Detection, AES.

I. INTRODUCTION

Cloud computing is internet-based computing that gives shared computer processing resources and data to computers and other devices on user demand. It is the delivery of hosted services over the internet. Its services can be public, private or hybrid. The three main benefits of cloud computing are self-service provisioning, elasticity, pay per use. The three broad categories of cloud computing are Infrastructure as a Service, Platform as a Service and Software as a Service. CCD/CMOS image sensors are deployed in everywhere such as digital camera, Smartphone, traffic camera, satellite reconnaissance, astronomical observation, medical micro endoscopy and robot vision. To clear local storage & also to save local storage space, collection of images are stored in cloud. Cloud Storage has been broadly classified into two categories as Public Cloud and Private Cloud. It is necessary to let the hybrid cloud provide an efficient image service while maintaining the privacy. Thus, the private cloud has to seek help to the public cloud which possesses abundant storage and computing resources. However, the public cloud is often not trusted. As a result, the image data to be transmitted to the public cloud need to be encrypted. Meanwhile, compressing these encrypted image data appropriately before transmission is essential to reduce the consumption of communication resources. On the other hand, it is highly expected that not all the data in an image are stored in the public cloud and a hand of data in an image, in which people are the most interested, can be placed in the private cloud for easy looking-up. Therefore, our aim is to propose an efficient secure image service framework for users through the hybrid cloud.

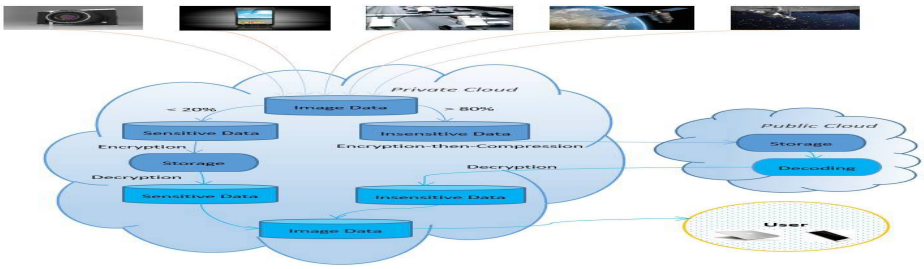


Fig.1 Secure big image data service framework

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

This section gives an idea about the basics of cloud computing and our proposed paper. In the following sections,section II explains the related works and section IIIexplains methodology, sectionIV explains our proposed system and the conclusion is insection V.

II. RELATED WORKS

Kumar and Makur applied the approach of to the prediction error domain and achieved better lossless compression performance on the encrypted grayscale/color images. Furthermore, Zhang designed an image encryption scheme via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently, compressed by discarding the excessively rough and fine information of coefficients in the transform domain. Recently, Zhang *et. al* suggested a new compression approach for encrypted images through multi-layer decomposition. Extensions to blind compression of encrypted videos were developed in despite extensive efforts in recent years, the existing ETC systems still fall significantly short in the compression performance, compared with the state-of-the-art lossless/lossy image and video coders that require unencrypted inputs. Meanwhile, reasonably high level of security needs to be ensured. If not otherwise specified, 8-bit grayscale images are assumed. Both lossless and lossy compression of encrypted images will be considered. Specifically, we propose a permutation-based image encryption approach conducted over the prediction error domain

III. METHODOLOGY

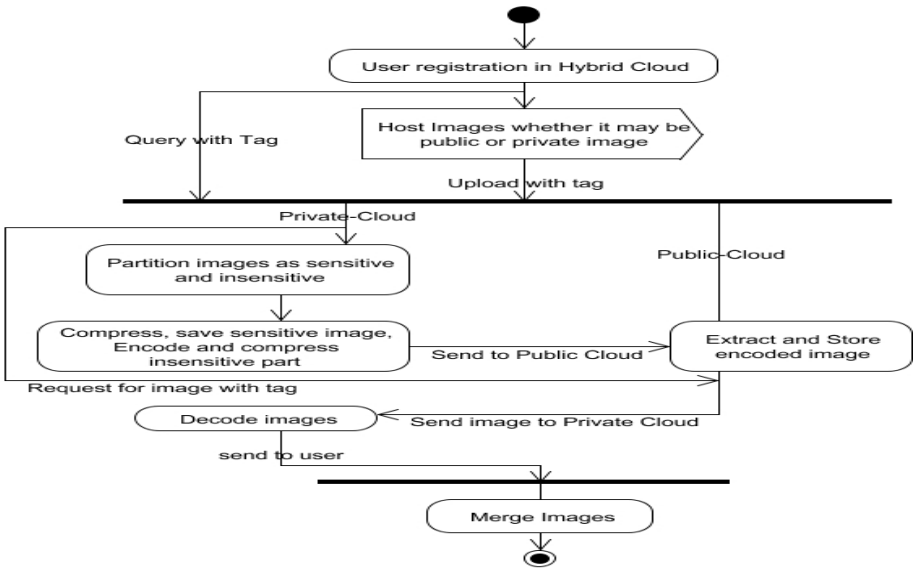


Fig.2 Activity Diagram

The user classes and characteristics involved in the working principle are as follows:

- Upload Images to hybrid cloud,
- Partitioning of image data,
- Coding and Decoding,
- Encryptionand private cloud storage,
- Compress and public cloud storage,
- Query and retrieval of images from hybrid cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

1. Upload Images to hybrid cloud

Initially, users have to create an account in hybrid cloud. Private cloud & Public cloud is internally tied up with each other. There is separate admin for private cloud & public cloud. User can directly access only private cloud. After login, user has to select an image and upload into cloud with tag. Tag is nothing but name of an image to identify correctly. Now, the image is received by the private cloud for processing and storage. User need not to apply any algorithm regarding security of that image.

2. Partitioning of Image Data

Images are arranged in pixels and image compression programs are generally used for compressing images, which is different from compressing the data. In most of the applications the user needs security. Therefore needs an encryption before compression. The pixels in an image are highly correlated to each other. Therefore the pixels can be predicted from their neighboring pixels. For this firstly the images are subdivided into blocks. For each block the transform coefficients are calculated. The resulting coefficients are then quantized and the output of quantize is used by symbol encoding techniques to produce the output bit stream which represents the encoded image. In image decompression model the reverse process takes place.

To make use of the public cloud's resources, the private cloud firstly partitions image pixels into two parts including sensitive data and insensitive data based on sensitivity identification approaches like Sobel edge detector. The sensitive data that are of great significance only account for a very small percentage (e.g., no greater than 20%) of whole image data. The remaining are insensitive data (or called insignificant data).

3. Coding and Decoding

The encoder divides the text in to four sub bands such as 00, 01, 10 and 11. Here the image is an encrypted one and performs down sampling. The 00n represents the sub image in the nth resolution level. And this sub image can be get from 00n+1, 01n+1, 10n+1 and 11n+1. This is called down sampling. Here the pixel locations are not shuffled. After the down sampling the low resolution image is obtained. Then each sub image is encoded independently. The decoding process starts from the 00 subimage of the lowest resolution level. Then the local statistics of the subimage 00 is derived. The decoder decrypts the 01n, 10n, 11n and then 00n-1 can be synthesized. Repeat the process till the target is obtained.

4. Encryption and private cloud storage

The sensitive data are straightway encrypted and stored in the private cloud side.Advanced encryption standard (AES) based algorithm is used here for image encryption. The primary purpose of encryption is to provide services to the people and to maintain the security of their information. There are four main objectives behind the use of cryptography which are confidentiality, data integrity, proof of identity and lack of ingratitude. AES is designed a secure symmetric image encryption technique and to ensure improvement in the encryption performance, mainly for images characterization with reduced entropy. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. It offers high security and can be realized easily in both hardware and software. The key stream generator has an important influence on the encryption performance.

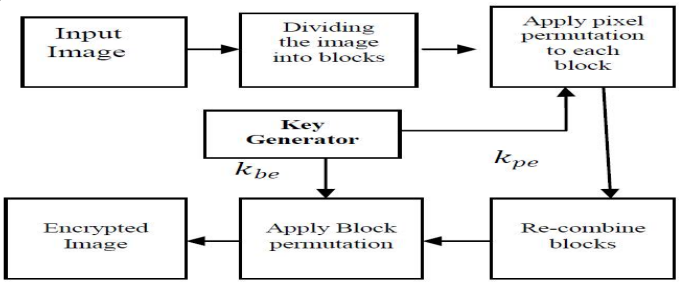


Fig.3Random permutation encryption process

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

5. Compress and public cloud storage

For the insensitive data, the instinctive idea is to compress them and then transmit the compressed result to the public cloud for storage and decompression. Yet, the public cloud is often semi-trusted or even malicious and therefore it is required that the public cloud can fulfill a privacy guaranteed decompression operation. In other words, prior to transmission, the insensitive data will be encrypted moderately. So, the insensitive part of an image is encrypted and compressed and send it to public cloud by private cloud.

6. Query and retrieval of images from hybrid cloud

Once users make a request for an image by asking tag of an uploaded image, the public cloud provides a privacy-guaranteed insensitive data reconstruction service. It decompresses the insensitive data and returns them to the private cloud. Now the private cloud decrypts the sensitive and insensitive data and assembles both to a complete image for the user. User can also check their uploaded history. It contains private images of user along with corresponding tag.

IV. PROPOSED SYSTEM

In order to secure image storage, it need to be stored in the trusted private cloud and are encrypted, to avoid theillegal user to directly access the data. For that, the appropriate compression must be exploited to reduce storagespace. However, the private cloud itself does not necessarilyown such storage and computation resources with the era ofbig image data. On the other hand, the public cloud possessesmore abundant storage and computation resources comparedto the private cloud. As a result, it is desirable that theprivatecloud can leverage the public cloud's resources to serve foritself.Yet, the publiccloud is often semitrusted or even malicious and therefore it isrequired that the public cloud can fulfill a privacy-guaranteeddecompression operation.

When a userrequests an image, the public cloud decompresses the insensitivedata and returns them to the private cloud which decryptsthe sensitive and insensitive data and assembles both to acomplete image.The proportion of the sensitive data is not more than 20% towell utilize the storage resources of the public cloud. However,this does not mean that a smaller proportion is better becauseof two reasons. One is that the sensitive data outperform theinsensitive data in terms of security protection level, therefore,for the security purpose, as many sensitive data as possibleshould be stored in the private cloud.

The other is that processingthe insensitive data is lossy. If too many data are partitionedinto the insensitive part, then some important information inthe image will be discarded.

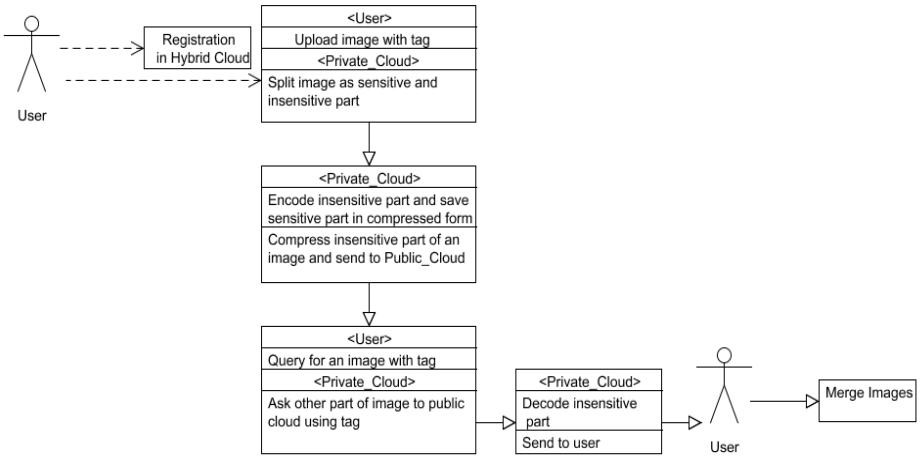


Fig.4 Collaboration Diagram

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

We give a specific realization based onthe techniques of Sobel edge detector, tent-logistic system andcompressed sampling. An image is first distinguished to obtainsensitive data set and insensitive data set with the help of Sobeledge detector. Then, the sensitive dataare encrypted in parallelin the similar way of the counter mode. The insensitive data areencrypted with the architecture of permutation-diffusion andare then subsampled by parallel compressed sampling technique.The encrypted sensitive data are stored in the privatecloud while the compressed measurements of the insensitive data are outsourced to the public cloud for storage. Such anoutsourcing means the private cloud saves abundant storagespace through outsourcing the greater than 80% data of animage to the public cloud.

Upon receiving the user's request,the public cloud decompresses the compressed measurementsand transmits the results that, in fact, are still encrypted insensitivedata to the private cloud which decrypts and assemblesthe sensitive data and insensitive data into a complete imagefor the user. The encryption of insensitive data can be againstciphertext-only attack while the encryption of sensitive datacan resist chosen-plaintext attack due the greater significanceof the sensitive data than the insensitive data. It is worth mentioningthat the proposed image service framework, as shownin Fig. 1, can be probably achieved using other more excellenttechniques and methods, which will be further studied infuture works. For example, the sensitive data can be furthercompressed before or after encryption, and the compressedmeasurements in the public cloud can also be considered tobe compressed for storage space savings.

1. Identification of Data Sensitivity

Sensitivity identification aims at extracting the sensitive datain an image. The sensitive data are the most interested regionfor users and limited to a very small proportion of an image.We choose the contour information of an imageas region of interest. The steep region in contour change ismore significant than the smooth region. To recognize thesecontour features, we can apply edge detection technique thatis a common image processing method. An edge detectionmethod of Sobel edge detector is adopted to identify thelocation of sharp intensity transitions in a target image, finallyacquiring a detection image for the target image. Implementingthis detection image recognizes the sensitive data for the targetimage.

2. Encryptionof Sensitive Data

Less than 20% encryption for sensitive data, on the one hand, we hope the computation resources in the private cloud to be efficientlyused. Because of the significance ofsensitive data, they need to be heavily encrypted to be againstsome potential attacks. Thus, we applythe idea of counter mode, which is a common block cipheroperation mode, as the counter mode has the advantage thatencryption and decryption can be fully parallelized. In additionto the parallelism, it can resist chosen-plaintext attack under anappropriate keystream generator. Here, this generator is constructedby using the tent-logistic system.

3. Encryptionof Insensitive Data andSub-sampling

The insensitive data with the amount exceeding 80% in animage will be compressed and then delivered to the public cloud for storage and decoding. However, the data need to beencrypted prior to transmission, the computation resources in the public cloud side can be utilized to fulfill thedecoding work. Thus, the private cloud performs the encryption then compression work before transmitting the insensitivedata to the public cloud. Encryptionmust affect the compression performance and thereby it isalways making a tradeoff by maximizing the compressionperformance only under two lightweight encryption schemesincluding permutation-only operation and diffusion-only operation.It is possible to enhancethe security without affecting the compression performance by use of the permutation-diffusion architecture.

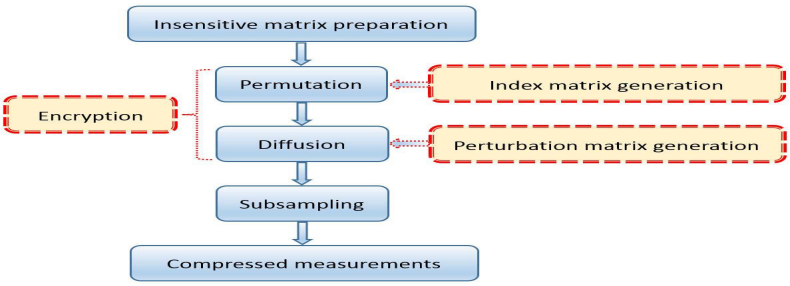


Fig.5Insensitive data encryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

After implementing permutation-diffusion encryption, we sub-sample each column using a measurement matrix to achieve the compression effect. Although the compression performance of compressed sampling has been found not excellent enough, it possessessome outstanding advantages of its own that are concluded as the following several aspects. First of all, the insensitive data can be extremely sparse, which is very suitablefor compressed sampling. The texture change in the insensitivedata block is less apparent than that in the sensitiveblock. As a consequence, the corresponding nonzero elementsafter sparse transform have less number and the sparsity isstronger. Second, one can adopt a very small sampling rate topromote the compression performance, since the insensitivitymeans the insignificance, as claimed by the insensitive blockitself. Third, for security guarantee purpose, the permutationdiffusionarchitecture can be utilized, which is not onlycompatible with parallel compressed sampling, but also reinforcesthe compression performance. Moreover, the proposedcompression scheme is robust and can offer progressive imagereconstruction service.

The robustness means on one hand, itcan sustain the occurrence of packet-loss in the transmissionchannel between the private cloud and the public cloud. Onthe other hand, once partial data are returned by the publiccloud, the private cloud is still able to provide progressiveimage service for users, as long as the reconstructed imagequality is acceptable. Lastly, what we want to emphasize isnot maximum compression but enough compression (sub-sampling).The compression data are sent to the public cloud forstorage and decoding while maintaining the privacy. Whenrequired, the data are decoded by the public cloud and the returned back to the private cloud.

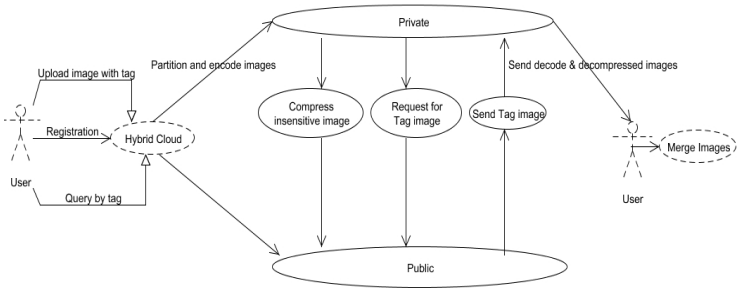


Fig.6 Use-case Diagram

4.Reconstruction of Insensitive Data

After generating the compressed measurements, the privatecloud outsources them to the public cloud for storage anddecoding. Upon receiving the request from the private cloud,the public cloud exploits insensitive data reconstruction servicein parallel. The public cloudis assumed to be semitrusted, i.e., can honestly fulfill thereconstruction service as specified, but is curious about theinsensitive data. The privacy is achievable, as proved by the next section, thereforethe public cloud cannot acquire meaning knowledge fromthe insensitive data. If the greater computation savings isrequired in the private cloud, then a linear encryption complexityis achievable at an expense of removing the permutationencryption.

5. Assembling of Image Based on User Request

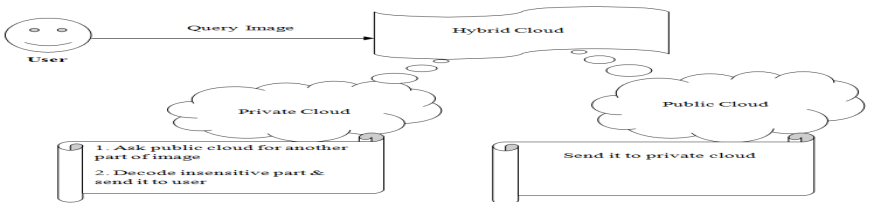


Fig.7 Architecture Diagram for Query Image

If receiving a request for some image from a user, the privatecloud exploits three steps to serve for the user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

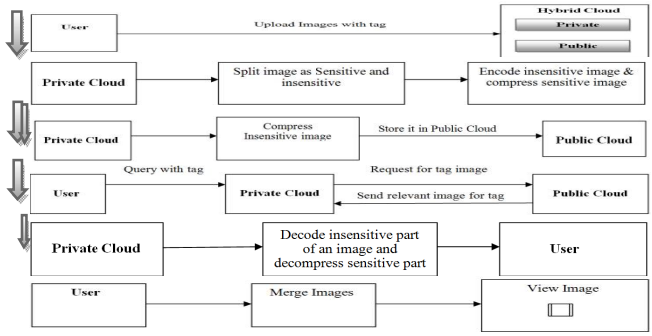
Vol. 7, Special Issue 4, April 2018

Step 1: Decrypts the sensitive data

Step 2: Decrypts the insensitive data. The public cloud providesthe reconstruction service, which then performs inverse diffusionand inverse permutation operations

Step 3: Regroup the image.The above two data sets are then regrouped intoa complete image according to the correspondingbinary sensitivity indicator.

DATA FLOW DIAGRAM



V. RESULT AND CONCLUSION

It proposes the detailed overviewof efficient secure service framework for big image data with the help of the hybrid cloud. The sensitive data are securely stored in the private cloud while the insensitive data are encrypted-then sub sampled and stored in the public cloud. This framework can save at least 80% space for the private cloud. The public cloud is responsible for at least 80% the insensitive data's storage and decoding. The security is verified through key space analysis, visual analysis, and key sensitivity analysis. With respect to the insensitive data outsourcing, encryption reliability is also demonstrated. In this paper, we do not consider the further compression coding of measurements and in future work, we will optimize compression rate to obtain better image service quality.

ADVANTAGES

- Provide secure image service for the users.
- The proposed framework can save larger than 80% space for the private cloud.
- It has a privacyguaranteed decoding scheme in the public cloud.

CONSTRAINTS IN IMPLEMENTATION

The proportion of the sensitive data is no more than 20% to well utilize the storage resources of the public cloud. However, this does not mean that a smaller proportion is better because of two reasons. One is that the sensitive data outperform the insensitive data in terms of security protection level, therefore, for the security purpose, as many sensitive data as possible should be stored in private cloud. The other is that processing the insensitive data is lossy. If too many data are partitioned into the insensitive part, then some important information in the image will be discarded.

ACKNOWLEDGEMENT

I take this opportunity to convey my deep and sincere thanks to our Head Of the Department Mr.Dr. R. Janarthanan. I alsoextendmy deep gratitude to the project coordinator Mrs.T.Karpagam and also to my guide Mr. G. Ragu for their valuable help and support inpresenting the project. I express my sincere gratitude toall the staffs of Computer Science & EngineeringDepartment and my beloved family members and friends who helpedme with their timely suggestions and support.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

REFERENCES

[1]. M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, 2004.
[2]. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos Soliton. Fract.*, vol. 21, no. 3, pp. 749–761, 2004.
[3]. Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2002, 2015.
[4]. L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 19, no. 10, pp. 3653–3659, 2014.
[5]. Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, 2016.
[6]. Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Process.-Image Commun.*, vol. 28, no. 3, pp. 292–300, 2013.
[7]. P. Refregier and B. Javidi, "Optical image encryption based on input plane and fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.
[8]. X. Peng, L. Yu, and L. Cai, "Double-lock for image encryption with virtual optical wavelength," *Opt. Express*, vol. 10, no. 1, pp. 41–45, 2002.
[9]. N. Zhou, Y. Wang, and L. Gong, "Novel optical image encryption scheme based on fractional Mellin transform," *Opt. Commun.*, vol. 284, no. 13, pp. 3234–3242, 2011.
[10]. W. Chen, "Optical multiple-image encryption using three-dimensional space," *IEEE Photonics J.*, vol. 8, no. 2, p. 6900608, 2016.