JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Improved Privacy Preservation Through RPSM Method in Cloud

*[1] Priyanka Valmiki, [2]Dr. Arvind Kaurav [3]Prof. Nehul Mathur*
*[1]M.tech Studen, [2]Professor, [3]Assistant Professor*
*[1,2,3] Department of Electronics and Communication (EC)*
*[1,2,3] Bhopal Institute of Technology, Bhopal (M.P.), INDIA,*

***Abstract :*** This paper present a novel approach to target cyber-crimes and cyber-attacks. There are different platforms available, in which cyber-attacks are performed. Due to these attacks users important information are leaked such as personal documents and other private documents. In this method perform image encryption and decryption technique that is based prime number key. This proposed method use random pixel shifting method for image encryption. In this method image pixels are shifted on different place on the basis on formula that's worked on homogenous equation. In this thesis work also discuss the different attacks on encrypted image such noise attacks. The proposed novel approach shows better result as compare other method in terms of encryption and decryption of secure image. There are different result parameters are available to check the quality of encrypted and decrypted image such as peak signal to noise ratio (PSNR), mean square error (MSE), and structure similarity index measurement (SSIM)..

***Keywords— Preservation, Random Pixel Shifting Method (RPSM), peak signal to noise ratio(PSNR), mean square error (MSE), and structure similarity index measurement (SSIM).***

## I. INTRODUCTION

Cloud is the new computing platform in which provide different IT services for Clint. Cloud provide a shared control pools of configurable system that may be quickly provisioned with lowest management effort, usually over the internet Cloud computing. Now a day's most of cloud services providers are known as CSP or third party services provider. They are providing different type of cloud services that is used in the real world such SaaS, IaaS and PaaS.

Cloud computing suppliers offer their "services" consistent with completely different models, they are- IaaS:- is one of the famous platform of cloud services. In the IaaS CSP provide real time hardware support to clients such as high speed hardware, Big data storage and high speed RAM. PaaS:- vendors are the providers of developed atmosphere for the app developers. Within the PaaS models, cloud suppliers give a computing platform, generally likewise as OS, programming-language implementing setting, database, and web server. SaaS:- model, Cloud users don't administer the cloud infrastructure where the appliance runs. Cloud applications dissent from completely different applications in their measurability, which can be obtained by cloning tasks. onto multiple virtual machines. There are different types of clouds mentioned as follows:-.

**Private Cloud-** They can be said as cloud infrastructure which is operated only for one organization, either managed internally or by a third-party, or hosted either internally or outwardly.

**Public cloud-**A cloud is named as a "public cloud" once the administrations are rendered over a system that is open for open utilize. A cloud is named as a "public cloud" once the services are rendered over a network that is open for public use Open cloud administrations are moreover free.

Now let's focus on the information given about cloud storage. Cloud storage is a model of computer info storage throughout that the digital info holds on to logical pools. These cloud storage suppliers are accountable to keep the data out there, and additionally the physical atmosphere being protected and running.

There are different places available there cloud computing use for various economic solutions by giving alternative services like cloud storage, computing resources, digital watermarking and many more. There is great demand for sharing private information on the internet for various purposes. An appropriate methodology for protecting communicated or keeping information involves utilization of cryptographic techniques. A cipher text is an encrypted message which is the method of turning cipher text again into plain text is cryptography. In a cloud data, location is dynamic and depends on various factors such as network, speed and availability of storage location. In such a scenario standard information security which is meant to protect the data at a known location fails due to location uncertainty of user's data.

## II. LITERATURE SURVEY

The literature survey discusses some very new techniques carried out by many researchers related to the field of the Cloud Privacy-preserving Images Processing. There are many methods introduced of Privacy-preserving Image Processing in the Cloud in the last decade.

Bo Zhang et.al. [2023], A three-party computation (3-PC) privacy-preserving image retrieval scheme based on additive secret sharing techniques for cloud computing scenarios, using CNN as image feature extractor to improve retrieval accuracy, constructing hierarchical clustered index trees to improve search efficiency, and designing a series of security protocols to ensure the security of images, network models, feature extraction and search processes. Our scheme achieves a balance between security, accuracy and efficiency without loss of retrieval accuracy. The experimental evaluation results demonstrated the effectiveness and efficiency of our framework. We intend to extend this work in two directions in the future, one is to outsource feature extraction and index building to cloud servers to further reduce the computational overhead of data owners, and the other is to further improve retrieval efficiency [01].

Yuandou Wang et.al. [2023], Digitized histopathology glass slides, known as Whole Slide Images (WSIs), are often several gig pixels large and contain sensitive metadata information, which makes distributed processing unfeasible. Moreover, artefacts in WSIs may result in unreliable predictions when directly applied by Deep Learning (DL) algorithms. Therefore, pre-processing WSIs is beneficial, e.g., eliminating privacy-sensitive information, splitting a gig pixel medical image into tiles, and removing the diagnostically irrelevant areas. This work proposes a cloud service to parallelize the pre-processing pipeline for large medical images. The data and model parallelization will not only boost the end-to-end processing efficiency for histological tasks but also secure the reconstruction of WSI by randomly distributing tiles across processing nodes [02].

Qihua Feng et.al. [2022], Image retrieval systems help users to browse and search among extensive images in real-time. With the rise of cloud computing, retrieval tasks are usually outsourced to cloud servers. However, the cloud scenario brings a daunting challenge of privacy protectionas cloud servers cannot be fully trusted. To this end, image-encryption-based privacy-preserving image retrieval schemes have been developed, which first extract features from cipher-images, and then build retrieval models based on these features. Yet, most existing approaches extract shallow features and design trivial retrieval models, resulting in insufficient expressiveness for the cipherimages A novel paradigm named Encrypted Vision Transformer (EViT), which advances the discriminative representations capability of cipher-images. First, in order to capture comprehensive ruled information, we extract multi-level local [03].

Faliu Yi et.al. (2021) - The emergence of cloud computing, large amounts of private data are stored and processed in the cloud. On the other hand, data owners (users) may not want to reveal data information to cloud providers to protect their privacy Moreover, decryption of big data such as images requires enormous computation resources, which is unsuitable for energy-constrained devices, particularly Internet of Things (IoT) devices. Data privacy in most popular applications, such as image query or classication, can be preserved if encrypted images can be directly classied on the cloud or IoT devices without decryption. This paper proposes a high-speed double random phase encoding (DRPE) technique of encrypting images into white-noise images. DRPE-encrypted images are then uploaded and stored in the cloud [04].

Zhijian Liu et.al. (2020) - The privacy-preserving edge-cloud inference framework, Data Mix, to bring the best of the resource-hungry edge devices and the privacy invasive cloud servers together for the model inference. We propose to delegate most of the model computations to the cloud and carefully design a mixing and de-mining operation to protect the privacy of the data transmitted to the cloud. Our framework is ecient, accurate and privacy-preserving: extensive experiments on two computer vision datasets and a speech recognition dataset demonstrate that Data Mix can greatly reduce the local computations on the edge with negligible loss of accuracy and no leakages of private information [05].

Qi Gu et.al. (2020) - Content-Based Image Retrieval (CBIR) techniques have been widely researched and in service with the help of cloud computing like Google Images. However, the images always contain rich sensitive information. In this case, the privacy protection becomes a big problem as the cloud always can't be fully trusted. Many privacy-preserving image retrieval schemes have been proposed, in which the image owner can upload the encrypted images to the cloud, and the owner himself or the authorized user can execute the secure retrieval with the help of cloud. Nevertheless, few existing researches notice the multi-source scene which is more practical. In this paper, we analyze the difficulties in Multi-Source Privacy-Preserving Image Retrieval (MSPPIR). Then we use the image in JPEG-format as the example, to propose a scheme called JES-MSIR, namely a novel JPEG image Encryption Scheme which is made for Multi-Source content-based Image Retrieval [06].

Zhihua Xia et.al. (2019) - Content based image retrieval (CBIR) techniques have been widely deployed in many applications for seeking the abundant information existed in images. Due to large amounts of storage and computational requirements of CBIR, outsourcing image search work to the cloud provider becomes a very attractive option for many owners with small devices. However, owing to the private content contained in images, directly outsourcing retrieval work to the cloud provider apparently bring about privacy problem, so the images should be protected carefully before outsourcing. a secure retrieval scheme for the encrypted images in the YUV colour space. With this scheme, the discrete cosine transform (DCT) is performed on the Y component [07].

Haohua Du et.al. (2019) - Privacy has become one of the major concerns in cloud video surveillance. Privacy protection of the surveillance videos strive to protect users' privacy information without hampering regular security tasks of the surveillance, meanwhile retains the system's high accuracy and efficiency. The current state of the art in protecting the video privacy is mainly realized through Privacy Region Protection, which only protects the privacy regions while keeps the non-privacy regions visually intact so that processing in the cloud is still feasible. However, the problem of determining the privacy regions has been ignored

and not properly addressed. a novel notion - concept graph, and with the aid of that, we develop our system – PatronuS to determine the privacy regions subject to satisfying both privacy and security requirements.

Z. Qin et. al, [2014] - In the last decade the social media growth rate remarkable. Standard multimedia social networks e.g. Flicker, generally utilize user image information to build user behaviour models, social preferences, etc., for the aim of effective advertising, higher user retention and attraction, and many of others. Data utilization practice deteriorates users' personal privacy and it increases the legislation pressures and criticism. The projected system allows an interested party to perform a range of image feature detection tasks, as well as visual descriptors in MPEG-7 normal, whereas protective user privacy concerning image contents. We implement a paradigm system supported somewhat homomorphism encryption theme and also the benchmark Caltech 256 information. The experiment shows that our system will guarantee effective image feature detection while not giving up user privacy.

Cong Wang et. al, [2013] - Large-scale image data sets are being exponentially generated lately. Alongside such information explosion is that the invasive trend to source the image management systems to the cloud for its verdant computing resources and edges. The thanks to defend the sensitive data whereas facultative outsourced image services, however, becomes a significant concern. To face the problems and troubles of outsourced challenges For handling these challenges, we tend to propose outsourced image recovery service (OIRS), a unique outsourced image recovery service style that exploits all entirely and completely different domain technologies and takes security, efficiency, and design quality into thought from the terribly starting of the service flow. Specifically, we tend to elect to design OIRS below the compressed sensing framework that is considered for its simplicity of unifying the standard sampling and compressing the image acquisition. Owners of data got to offer compressed image samples to cloud to reduce the storage overhead. Additionally, in OIRS, information users will harness the cloud to firmly reconstruct pictures while not revealing info from either the compressed image samples. We begin with the OIRS design for distributed information that is that the typical application situation for compressed sensing, and so show its natural extension to the overall information for substantive tradeoffs between potency and accuracy. Analyzing the protection privacy of OIRS and conducting a comprehensive experiment to show the system potency**.** For completeness, we additionally discuss the expected performance speeding of OIRS through hardware inbuilt system design.

Chao-Yung Hsu et. al, [2012], "Image feature extraction in encrypted domain with privacy preserving SIFT,"
Privacy has received considerable attention however remains mostly neglected within the transmission community. Wherever the server is resource-abundant, and is capable of finishing the chosen task, think about a cloud computing situation there. Visible of the particular actual fact that scale-invariant feature transform (SIFT) has been wide adopted in various fields, this paper is that the initial to focus on the importance of privacy-preserving SIFT (PPSIFT) and to take care of the matter of secure SIFT feature withdrawal and illustration within the encrypted domain. We show through the safety analysis supported the discrete logarithm drawback and RSA that PPSIFT is secure against cipher text solely attack and familiar plaintext attack. Experimental results obtained from completely different case studies demonstrate that the planned homomorphic encryption-based privacy-preserving SIFT performs comparably to the initial SIFT which our technique is helpful in SIFT-based privacy-preserving applications

Chun-Shien Lu et. al, [2011] - Privacy has received a lot of attention however is still for the most part neglected within the multimedia system community. Contemplate a cloud computing state of affairs, wherever the server is resource-abundant and is capable of finishing the designated tasks, it's visualized that secure media and search recovery with privacy-preservation **are** seriously taken care of In sight of the actual fact that scale invariant feature transform (SIFT) has been wide adopted in numerous fields, this paper is that the initial to address the trouble of secure removal of a SIFT feature and illustration within the encrypted domain. In SIFT all the operations need to be affected to the encrypted domain, **we** tend to propose a homomorphic encryption-based secure SIFT methodology for privacy conserving feature extraction and illustration supported Paillier cryptosystem. Particularly, homomorphism comparison be a for SIFT feature detection however remains a difficult issue for homomorphic encryption methods. To conquer this downside, we investigate a quantization-like secure comparison strategy during this paper. In this, homomorphic encryption based SIFT program performed a better result. We think that this work may well be a necessary step towards the privacy-preserving multimedia retrieval, wherever privacy can be a significant concern

M. Armbrust et. al, [2010] - Cloud computing has the potential to transform an outsized a part of the IT business, making software system further more attractive. They have not be troubled concerning over provisioning a service whose quality does not meet their predictions, sothey waste valuable resources, therefore missing potential customers and revenue. The firms having big tasks can get results quickly as victimization 1,000 servers for one hour values no quite victimization one server for 1,000 hours.
**T. Sikor, et. al, [2001],** The MPEG-7 visual usual below development denote content-based descriptors that allow users or agents (or search engines) to give similarity in pictures or video supported visual criteria, and may be accustomed with efficiency identify, filter, or browse pictures or video supported visual content. Moving on the specifications, MPEG-7 specifies object form or object motion choices, color, texture and many more. As we see further more it also the information of aim, methodologies, and broad details of the MPEG-7 normal development for visual content description [23]

## III. PROBLEM FORMULATION

### *A. Spatial Domain*

The A digital image is a grid of pixels. A pixel is the smallest element in an image. Every image element corresponds to anybody worth known as image element intensity. Now the intensity of a picture varies with the placement of a picture element. Let I be a picture and (x,y) be the location (or coordinate) of any picture element. Now the image is represented as a function of location: I(x, y), wherever x and y are integers. Thus a picture I(x, y) could be a matrix of pixels. Spatial refers to area in a picture; this area

could be a 2d plane (xy-plane). Here the concept of image plane itself is referred and strategies in spatial domain are based on directly adjusting the value of the pixels. Spatial domain processes are represented as:

$$I_1(x, y) = T[I(x, y)]$$

Where $I_1$ is modified image and the value of a pixel with coordinates $(x,y)$ in $I_1$ is the result of performing some operation $T$ on the pixels in the neighborhood of $(x,y)$ in the original image $I$.

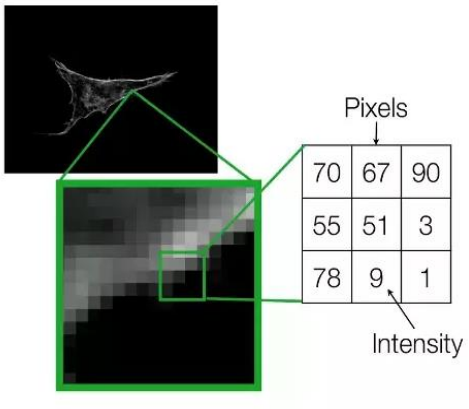


Fig.1 Pixel Information representation

*B. Frequency Domain*

Image enhancement in the frequency domain is simple. We tend to merely work out the Fourier remodeling of the image to be increased, multiply the result by a filter (rather than convolve within the spatial domain), and do reverser process to reform image. The thought of blurring a picture by dropping its high frequency parts or sharpening a picture by increasing the magnitude of its high frequency parts is intuitively simple to know. However, computationally, it's usually more economical to implement these operations as convolutions by little spatial filters within the spatial domain.

*C. Key Dependent*

Positioning Recognized security notions for coding schemes like IND-CCA seek advice from scenarios where encrypted plaintexts do not depend upon the key. For a few situations like encrypting a tough disk, storing the secret decoding key such a security model is not enough. The question of secure encoding within the presence of key-dependent messages arises, and marked progress in recent years can be understandable in such scenario which has been created for MACs and signature schemes, situations with key-dependent messages appear much less understood. In Both MACs and signature schemes provide data integrity, so a signature of a backup of a hard disk can also be used. Using a signature scheme allows a user to prove to another party whether or not the hard disk has been modified without revealing the secret key. On the other hand, MACs are symmetric, so the secret key must be revealed in order to prove that the hard disk has been tampered with

*D. Number of Images*

When we talk about the real time word, number of images is huge. That why we required a fast encryption - decryption method and user friendly method. If the method is complex and not easy to use, the user will not adopt this method. So they try to develop method on the basis of large number of image as well as easy to use.

*E. Number of Stages*

Combined image encoding concept involves the places or the stages where manipulation and SCAN strategies are done. Entire encoding method involves 2 stages where the multiple pictures to be encrypted are applied to phase manipulation block. When we talk about the 1st stage, Fourier transform (FT) is applied to induce phase and magnitude of all input images. Stages of all the pictures are disorganized to get changed image once applying Inverse Fourier transform. In the second stage, these changed pictures are disordered by using SCAN methodology. SCAN methodology finally provides encrypted image by rearranging the pixels positions of changed pictures

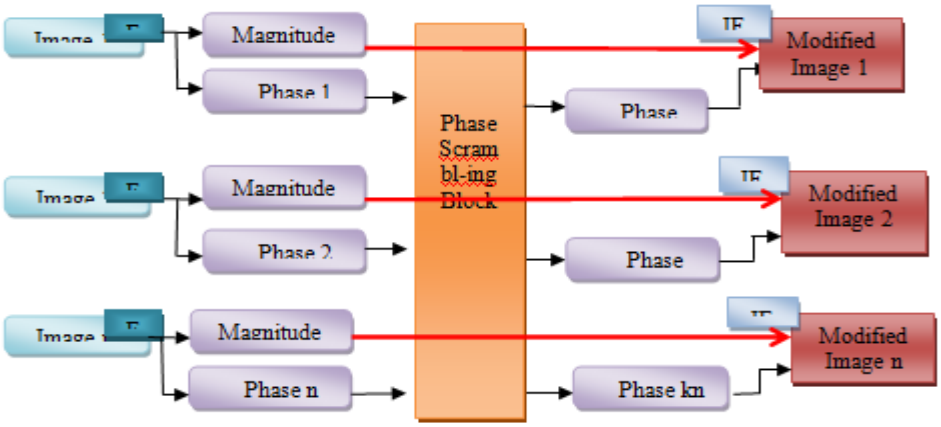


Fig. 2 Block Level Structure of Multiple Multimedia data (Image) encryption

## IV. PROPOSED METHOD

For privacy preservation a framework is been suggested for retrieval of pictures in large-scale, storage outsourcing, search, and dynamically updated repositories. Here the framework is made of two things: privacy preserving that is been executed in the outsourcing server and an image encryption component which is been executed on client devices. We base this framework on anew encryption scheme specifically designed for images, Random Pixel shifting method that is based on Gyrator transform while protecting the privacy of both image owners and other users issuing queries.

For the enhancement of previous problem use the following methodology. In this method use some terminology: a repository (Image Data Server) is a collection of images which is stored in the infrastructure of a cloud provider; the cloud server, or just cloud. The cloud server is based third type of cloud services that IaaS infrastructure that acts as a server both for storage and computation over images. In the proposed system both client and servers provide use this server, and its easily used and access by any place by using mobile phone, tablet. In the proposed method more than one users are use this services, they also upload there different images to secure cloud. Each and every user having own secret key, user id and password, with the help of this log in in the system, when upload any image on cloud server, it create a key for encryption of image, when user want to decrypt this image, require a decryption key without decryption key, it is not possible to decrypt image. If one user wants to share a secret image with different user, it can easily do just simply send the image with decryption key. Other user applies decryption with user's decryption key and decrypts this image.

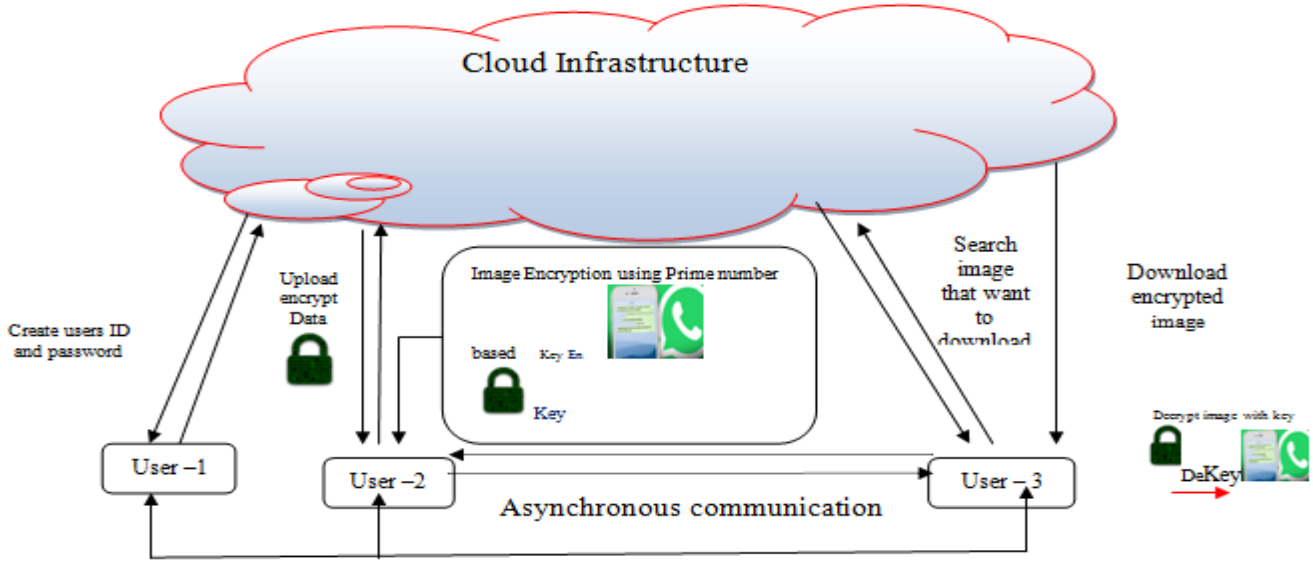


Fig. 3 Block diagram of Proposed Method

*A. Block diagram*

In the proposed system there are two important parts user or client and service provider server. Personal Images are easily transferred from one place to cloud and one user to other user.

In the above figure 3 shows the block diagram of proposed work. First user create log in ID and password with the help of create a new user sign process and send request to admin. After admin approval user convert its personal image into encrypted form and send to the server. In the above figure 3 shows the user 2 process of send and receive the secret data using random pixel shifting method encryption and decryp tion method. User can also send and receive this encrypted image to different user using any public and private channel. User's data already is in encrypted form so user can communicate data with other with any tension. Because in random pixel shifting method based on prime number and there is no limit of prime number. In the similar process user can easily download the encrypted image and decrypt it, with the help of decryption. Remember without prime number based decrypt key user cannot decrypt the personal data. That is the major advantage and drawback of this method. If user forget the encryption key decryption is not possible because it's based on second order homomorphic equation.

## V. SIMULATION AND RESULT

In this chapter discuss the simulation, result, data base and result parameters for the analysis of proposed method. For the implementation of proposed algorithm use Matrix laboratory. Matrix laboratory is a well-known tool for such kind of algorithm implementation related to data encryption and decryption. MATLAB contain a rich function family of computer vision tool box functions, image accusation tool boxes and large image processing library.

### *Result Parameters and Simulation tool*

The result of proposed method for privacy preserved secure data encryption and decryption shown in this section, simulation of our proposed method and result calculation. For the implementation proposed work simulate with the help the MATLAB R2013a (8.1.0.602) software and simulate our whole proposed methodology in graphical user interface (GUI). The performance of the proposed algorithm is tested for different data file size that is shown in GUI windows. Basic configuration of our system is: Processor: Intel (R) Quad Core (VM) i3 – 3110 Central Processing unit @, 2.40 GHz 64 b OS. MATLAB based simulation result shows good timing value for different file size images are compare to other method that is shown in table 5.1. These criteria can be evaluated by PSNR in dB, Mean square error (MSE), encryption time E(t), decryption time D(t) For calculate the similarity of the encrypted image and decrypted image calculate the structural similarity index measurement (SSIM) of the both images. Performance of our proposed method are quantitatively measured by PSNR, MSE, and SSIM values defined by:

*A.Encryption Time*

The time taken when image are encrypt. It is calculate by the total time taking of the encryption algorithm. In the proposed Work use random pixel shifting method.

E(t) = Time consumption in encryption

*B. Decryption Time*

The time taken when image are Decrypt. It is calculate by the total time taking of the Decryption algorithm. In the proposed Work use random pixel shifting method.

D(t) = Time consumption in decryption

*C. Peak Signal to Noise Ratio (PSNR)*

The PSNR is computed as:

$$PSNR = 10\, log_{10}\left(\frac{S^2}{MSE}\right) \qquad 5.3$$

Where *S* is that the size of actual image.
The PSNR is higher for an excellent worth image and lower for a poor quality image. This parameters is use to analysis the quality degradation of image. In this proposed research work on the basis of our image size 255x255, we mentioned PSNR and MSE are as follows.

*D. Mean Square Error (MSE)*

The MSE measures the standard amendment between the upload image (X) and downloaded image (Y) and is given by:

$$MSE = \frac{1}{N}\sum_{j=0}^{N-1}(X_j - Y_j)^2 \qquad 5.4$$

$X_j$ Shows the upload image
$Y_j$ Shows the download image
The MSE has been extensively used to quantify image quality and once used alone; it doesn't correlate powerfully enough with sensory activity quality. It ought to be used, therefore in conjunction with alternative quality metrics and perception. MSE is an important parameter for quality check of the image. The output value of MSE try to low or under 50. MSE more refined form is RMSE.

*E. Structural Similarity Index Measurement (SSIM)*

SSIM is the image Q.A. parameter with the help of this we can check and analysis the quality of the image. SSIM value in between 0 and 1, zero shows poor result above then 0.8 shows good result. Ideal SSIM value is 1.

$$SSIM\ (x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad 5.5$$

Comparison of proposed method with other methods.

***Data Set***

The standard data set images are shown in below. There are five different images are used as input image that is shown in below. There are three different type of images are shown in below in fig 4(a), 4(b),4(c),4(d) and 4 (e). These are images used to calculate the different prarameters of proposed method with different size of input data. In the below figure 4 shows the five different type of image, they are collect by berkeley university. **[2]** In the reference number 17 researchers also used same data set for cloud based image processing

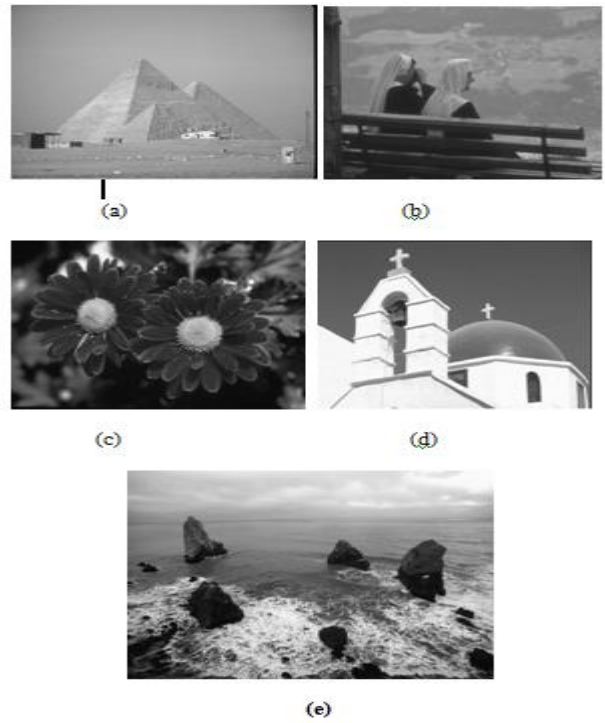


Fig. 4 Shows the Berkeley Image Data Set (Gray Scale) [2]

In the below figure 4 shows the test image 1 output. In this standard image perform encryption and decryption and other performance parameter. In the process of encryption and decryption calculate the five different parameters they are PSNR. MSE. E(t), D(t) and SSIM, the resultant value of these parameters respectively 31.2684, 48.5556 ,9.12, 9.53 and 0.85. In upstairs outcomes evidently see that all the outcome strictures for standard image are worthy, SSIM is 0.85 shows good resultant value, similar that PSNR, MSE, encryption and decryption all are shows good result.

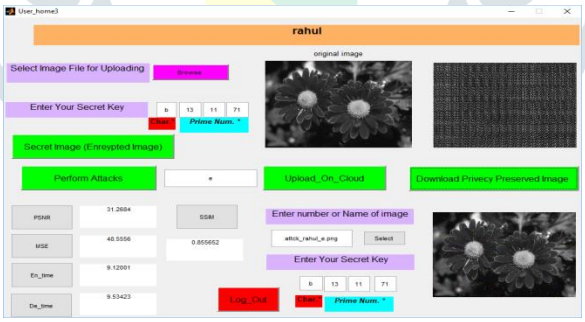


Fig. 5 Tested output of standard image 1

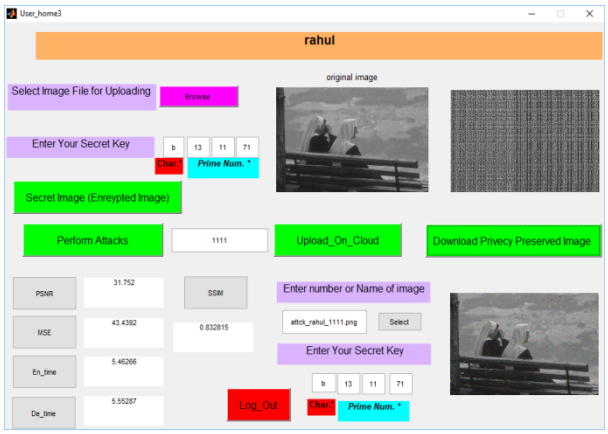


Fig. 6 Second Test Image Output Of Standard Data Set

In the above figure 5 shows the test image second output. In this standard image perform encryption and decryption and other performance parameter. In the process of encryption and decryption calculate the five different parameters they are PSNR. MSE. E(t), D(t) and SSIM, the resultant value of these parameters respectively 31.75, 43.4392 ,5.46266, 5.55287 and 0.83. In the above results clearly see that all the result parameters for standard image are good, SSIM is 0.83 shows good resultant value, similar that PSNR, MSE, encryption and decryption all are shows good result. SSIM of download decrypt image is above 0.8, it's a good outcome.

In the below figure 6 shows the test image third output. In this standard image perform encryption and decryption and other performance parameter. In the process of encryption and decryption calculate the five different parameters they are PSNR. MSE. E(t), D(t) and SSIM, the resultant value of these parameters respectively 31.75, 43.4392 ,5.46266, 5.55287 and 0.83. In the above results clearly see that all the result parameters for standard image are good, SSIM is 0.83 shows good resultant value, similar that PSNR, MSE, encryption and decryption all are shows good result. SSIM of download decrypt image is above 0.8, it's a good outcome.

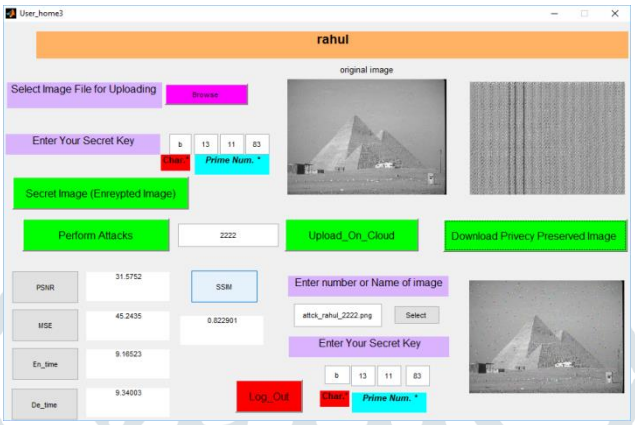


Fig. 6 Third Test Image Output Of Standard Data Set

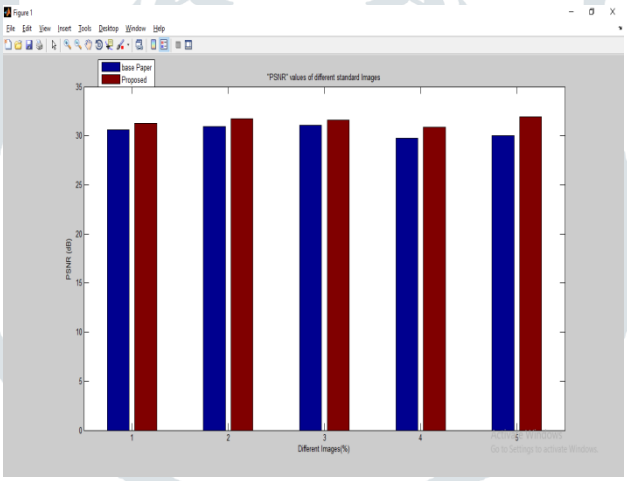


Fig. 7 Graphical comparison of PSNR

In the above figure 7 shows the graphical representation of PSNR. In the above bar graph compare the result of five different images. In all the image PSNR of proposed method is higher as compare to previous method. In the X axis (horizontal axis) shows the different images and in the Y axis shows the peak signal to noise ratio in decibel (dB). In the above figure shows the PSNR based comparison in the next figure 5.11 shows the comparison of proposed with previous method on the basis of SSIM.

In the below figure 8 shows the graphical representation of SSIM. In the below bar graph compare the result of five different images. In the entire image SSIM of proposed method is higher as compare to previous method. In the X axis (horizontal axis) shows the different images and in the Y axis shows the value of SSIM

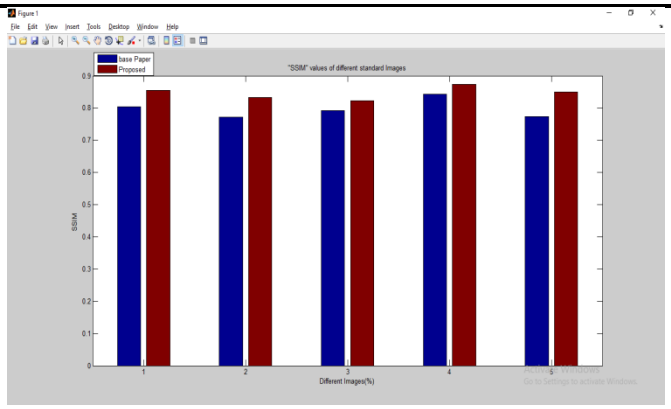


Fig.8 Graphical Comparison of SSIM

## VI. CONCLUSION

The conclusion of proposed method is mentioned here. The proposed based on random pixel shifting method shows better result for privacy preserve secure image encryption and decryption in public channel. The proposed method mainly focus the privacy preservation of the images as compare to other previous method most of the methods are based on third party based encryption and decryption. Now a day's cybercrime are increase rapidly. So the third party CSP are not very secure, the solution of this problem is our proposed method, in this method encryption and decryption done at user end cloud and private channel are only use for encrypted data send and receive. The proposed method is less complex as compare to previous methods. The main advantage of proposed method is random number based secure key. As we know that Random number are infinite, so it's difficult of crack by hackers.

## REFERENCES

[1] Bo Zhang , Yanyan Xu, Yuejing Yan1 and Zhiheng Wang, "Privacy-preserving Image Retrieval Based on Additive Secret Sharing in Cloud Environment" July 31st, (2023)

[2] Yuandou Wang, Neel Kanwal , Kjersti Engan , Chunming Rong, Zhiming Zhao "Towards a privacy-preserving distributed cloud service for preprocessing very large medical images" 12 Jul (2023)

[3] Qihua Feng, Peiya Li, Zhixun Lu, Chaozhuo Li, Zefang Wang, Zhiquan Liu "EViT: Privacy-Preserving Image Retrieval via Encrypted Vision Transformer in Cloud Computing" 31 Aug (2022)

[4] Hang Cheng , Qinjian Huang, Fei Chen , Meiqing Wang And Wanxi Yan "Privacy-Preserving Image Watermark Embedding Method Based on Edge Computing" February 22, (2022)

[5] Chiranjeevi Karri , Omar Cheikhrouhou , Ahmed Harbaoui , Atef Zaguia and Habib Hamam "Privacy Preserving Face Recognition in Cloud Robotics: A Comparative Study" Volume 10, 15 July (2021).

[6] Faliu Yi, Ongee Jeong And Inkyu Moon "Privacy-Preserving Image Classification With Deep Learning and Double Random Phase Encoding" Volume 9, October 11, 2021

[7] Zhijian Liu, Zhanghao Wu, Chuang Gan, Ligeng Zhu and Song Han "DataMix: Ecient Privacy-Preserving Edge-Cloud Inference" (2020)

[8] Qi Gu, Zhihua Xiaa and Xingming Suna "MSPPIR: Multi-Source Privacy-Preserving Image Retrieval in cloud computing" 30 Sep (2020)

[9] Zhihua Xia, Lihua Lu, Tong Qiu1, H. J. Shim, Xianyi Chen and Byeungwoo Jeon "

[10] A Privacy-Preserving Image Retrieval Based on AC-Coefficients and Color Histograms in Cloud Environment" vol.58, no.1, pp.27-43, (2019 )

[11] Haohua Du, Linlin Chen, Jianwei Qian, Jiahui Hou, Taeho Jung, Xiang-Yang Li "PatronuS: A System for Privacy-Preserving Cloud Video Surveillance" 2019

[12] Liu Qin, Zhan, et al. "Privacy-Preserving Image Processing in the Cloud." *IEEE Cloud Computing* (2018).

[13] Zheng, Yifeng, et al. "Privacy-preserving image denoising from external cloud databases." *IEEE Transactions on Information Forensics and Security* 12.6 (2017): 1285-1298.

[14] H. Esfahani et al., "Cloudbuild: Microsoft's Distributed and Caching Build Service,"Software Engineering in Practice (SEIP 16), 2016.

[15] M. Jeevitha Lakshmi S. , Umapriya , R. Ramya M., SivaSindhu. "Secure Transformation Based Approach for Outsourced Image Reconstruction Service" International Journal of Scientific and Research Publications, Volume 5, Issue 3, March 2015 ISSN 2250-3153.

[16] Z. Qin et al., "Privacy-preserving outsourcing of image global feature detection, "Proceedings of the Global Communications Conference (GLOBECOM 14), 2014.

[17] H. Wang et al., "Security protection between users and the mobile media cloud," IEEE Communications Magazine, 2014.

[18] Z. Qin et al., "Towards efficient privacy-preserving image feature ex-traction in cloud computing," Proceedings of the 2014 ACM on Multimedia Conference (MM 14),2014.

[19] C. Wang et al., "Privacy-assured outsourcing of image reconstruction service incloud," IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, 2013, pp.166–177.

[20] C. Lin, C. Lee, and S. Chien, "Digital Video Watermarking on Cloud Computing Environments," Proceedings of the Second International Conference on Cyber Security (CyberSec 13), 2013.

[21] C. Modi et al., "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, 2013, pp. 42–57.

[22] C.-Y. Hsu et al., "Image feature extraction in encrypted domain with privacypreservingSIFT," IEEE Transactions on Image Processing, vol. 21, no. 11, 2012, pp.4593–4607.

[23] S. Pandey et al., "An autonomic cloud environment for hosting ECG data analysis services," Future Generation Computer Systems, vol. 28, no. 1, 2012, pp. 147–154.

[24] K. Ivanova et al., "Features for art painting classification based on vector quantization of mpeg-7 descriptors," Data Engineering and Management, Springer, 2012.

[25] C.-Y. Hsu et al., "Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction," Proceedings of SPIE (SPIE 11), 2011.

[26] M. Naehrig et al., "Can homomorphic encryption be practical?," Proceedings of ACM Cloud Computing Security Workshop (CCSW 11), 2011.

[27] M.K. Khan, J. Zhang, and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification," Future Generation Computer Systems, vol. 27, no. 4, 2011, pp. 411–418.

[28] M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol.53, no. 4, 2010, pp. 50–58.

[29] W. Lu et al., "Secure image retrieval through feature protection," Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP 09),2009.

[30] Z. Erkin et al., "Privacy-preserving face recognition," Proceedings of PrivacyEnhancing Technologies Symposium (PETS 09), 2009.

[31] Pranay Yadav, Shilpi Sharma, Sweta Maurya "Internet of Things based Air Pollution Penetrating System using GSM and GPRS" 2018.

[32] Pranay Yadav, Shachi Sharma, Prayag Tiwari, Nilanjan Dey, Amira S. Ashour and Gia Nhu Nguyen "A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max" 2018.

[33] Sandeep Tiwari; Nitesh Gupta; Pranay Yadav "Diabetes Type2 Patient Detection Using LASSO Based CFFNN Machine Learning Approach" 2021.

[34] Pranay Yadav, Prof. Nitesh Gupta, Sandeep Tiwari "Diabetes Type2 Patient DetectionUsingLASSOBased CFFNN Machine LearningApproach" 2020.

[35] Abigail Fernandes, Pranay Yadav , Omkar Nalawade, Sanket Joshi , Renitta Jobby "classification and applications of lantibiotics from Gram-positive bacteria" 2023, Pages 411-425.