International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp. 7509-7516
 https://dx.doi.org/10.37622/IJAER/11.11.2016.7509-7516

An Efficient Privacy Preserving Medical Image Retrieval Using ROI Enabled Searchable Encryption

J. Hyma
Assistant. Professor, Dept. of CSE Gitam University Visakhapatnam, Andhra Pradesh, India.

Dr. G. Lakshmeeswari
Assistant. Professor, Dept. of CSE GITAM University Visakhapatnam, Andhra Pradesh, India.

D. S. Sampath Kumar
Dept of CSE GITAM University Visakhapatnam, Andhra Pradesh, India.

Ayush Anand
Dept. of CSE GITAM University Visakhapatnam, Andhra Pradesh, India.

Abstract
In this paper, we propose a new idea of searchable medical image encryption method to provide secrecy or authentication when a database is stashed away on a host maintained by a third-party server. This project addresses the trouble of enabling content based image retrieval throughout encrypted medical image dataset. Medical image database is encrypted by the owner of the content before transmitting or before stacked away on to the server. These encrypted stored data along with patient information are made accessible for authorized users only. The authorized user can pose the query on the encrypted data base and able to retrieve the most relevant cluster of images from the database maintained by the third part server. We compare our proposed privacy preserving data mining technique with conventional technique in terms of precision and recall. The insights obtained through this research and comparisons will help to design real time algorithms appropriate for privacy aware third party server systems.

Keywords: Searchable medical image encryption, CBIR, Privacy preserving search, Feature extraction, encryption, Indexing.

INTRODUCTION

Hospitals with forward-thinking bring out tremendous amounts of data in all departments. Mainly medical images like scanning, x-ray, etc., are being progressively significant in innovative diagnosis and medical examinations through large assortment in radioscopy protocols and modalities, but an elaborated image interpretation is not simple at all times. By delivering enormously huge amount of imagery tomographic modalities like computed tomography, Magnetic Resonance Imaging (MRI) and Positron Emission Tomography (PET) can tend to an information overload and create a need for forward tools to support understanding images. CBIR (Content Based Image Retrieval) has been suggested as one of the capable tools to aid diagnosis and use the huge amount of perceptual data available.

The main aspire of medical image retrieval over ciphered database is to give something effective and precise search potentially throughout encrypted medical image data without decrypting them. Onward motion in this medical field can have applications in upholding the privacy of sensitive data hived away on third-party servers. Examples include Webmail and online storage services, where there are developing concerns that the service provider may not be confided with the information of personal data, and data encoding in a cipher language is necessary to preserve the privacy of the medical imagery from the third party service provider and potential cyberpunks.

With the arrival of the internet based computing paradigm and the growth of online storage services, the third party servers not only offer information for sharing, but also contain huge amount of secret data demanding limited access and privacy preserving. Secure management of secret data stored online is an increasingly important issue, which needs a balance between data privacy and accessibility. Technologies that can enable online data management with privacy preserving are going to be crucially important for internet based computing to reach its full potential.

Earlier data privacy protection for online personal data concentrates on access control and secure transmission to ensure that personal data can be transmitted securely to the third party host and unauthorized person cannot access the personal data. Once the data comes to the host, the host decrypts the personal data and operates on plaintext without secrecy in order to allow services to users such as search and data summarization. This makes the user's personal data vulnerable to untrusty third party service providers and malicious interlopers. For example, personal picture gallery can potentially be viewed by an executive if stacked away online in plaintext. Encrypted data stored online using traditional cryptographic ciphers directly make it hard for the host to process the data, and also for the users to get back

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp. 7509-7516
© Research India Publications. https://dx.doi.org/10.37622/IJAER/11.11.2016.7509-7516

information from the encrypted database. Hence, it is both desirable and essential to develop new technologies for data retrieval over encrypted databases that can preserve user's secrecy without sacrificing the accessibility and usability of the personal data.

As the numbers of digital medical images are rapidly increasing, they become a crucial part of today's personal medical image data collections. Storing and managing huge amount of medical image data online is a desirable option for comfort data access anytime anywhere. Motivated by these crucial technological trends, we propose in this report the problem of distance metric based image search of online medical image database, while minimizing data leakage and preserving data privacy against unauthorized access including third party service providers. Below given are some related works.

The emerging area of previous work to privacy preserving medical image retrieval is secure data mining, which aims at performing normal data mining tasks but keeping the data being processed secret. Previous work on information retrieval in the encrypted format concentrated on text documents. Song et al, Brinman et al, and Boneh et al researched Boolean search method to distinguish whether or not a particular search item is present in encrypted document. Swaminathan et al. proposed a framework for rank ordered search over encrypted text documents, so that text document can be retrieved back in the order of their relevance to the search item. In that secure text search, search methods can be applied to index based search of Multimedia information. However this type of search relies on having exact description of the data already available, and its search scope is limited to the given keyword set.

In contrast CBIR based search over an encrypted image database provides more flexibility, where by sample images presented as search items with similar visual content are identified in the database. Erkin et al. proposed a review of related cryptographic primitives and several applications of secure image processing in data analysis and personal data protection. However, applying these cryptographic primitives directly with the content based image retrieval is not an ideal solution. Elective image retrieval generally relies on estimating the resemblance of two items using the minimum distance between their visual features, such as color, shape and some additional important features. Generally these cryptographic primitives do not preserve the distance between image feature vectors after encryption. Accordingly scalability and efficiency are crucial for multimedia data retrieval but it can be difficult to attain using cryptographic primitives alone. Another work by Shashank et al. deals the problem of privacy preserving of the search image when searching over a public database where the images are not encrypted. By formulating the search item and response item in the right way during multiple times of communications between user and the third party server, the host is made unretentive to the actual search path and thus incognizant of the query content.

Compared with Shashank et al. work, this report focuses on the Content-based medical image retrieval over encrypted databases, where both query and database images are encrypted and also their privacy is protected. The methods proposed in this project enable efficient medical image retrieval in the encrypted domain, without multiple times of communications between user and the host. We confirm that the feasibility of our solution in medical images by analysis and simulation of different modality of medical images.

PROPOSED METHODOLOGY

Selective Searchable Encryption

In the area of medical image security, the terms" selective encryption" (or) "partial encryption" denote techniques which trade-off privacy for computational complexity. They are planning to preserve medical image content and carry out the security requirements for a particular medical image application. For example, in real time the encryption of an entire video stream using traditional ciphers requires more computation time due to large volumes of data involved. If we consider a dataset of medical imagery as discussed in the introduction, several requests of this type need to be answered concurrently which evidently puts server demands on the process of encryption. Hence a reduction of computational demand is desirable for these medical applications. In searchable encryption of visual medical image data, application based specific data structures are exploited to design more efficient encryption system as shown in figure [1].

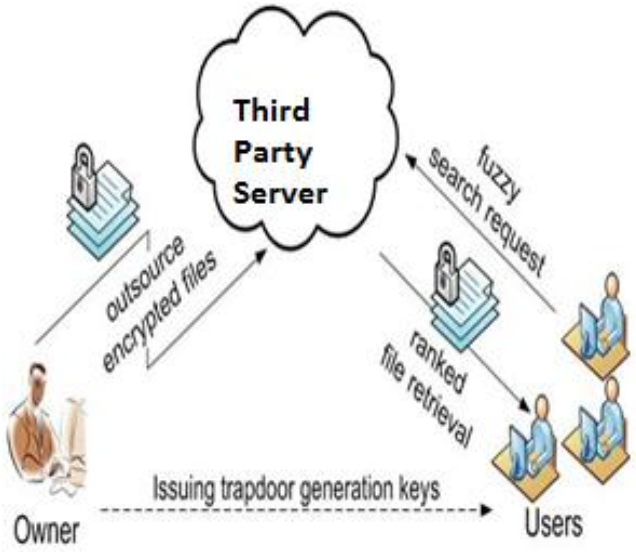


Figure 1: Searchable encryption

Intuitively, Searchable encryption seems to be a good idea in all cases since it is always desirable to decrease the computational complexity involved in various signal processing applications. However the privacy (or) security of such schemes is usually lower as compared to full encryption. The main reason to accept this drawback is significant savings in terms of power or processing time. Hence the environment in which searchable encryption should be applied needs to be examined thoroughly in order to decide whether its use is reasonable or not. In the following sections we discuss assumptions for the reasonable use of searchable encryption of visual image data in medical applications and therefore restrict the discussion to lossless image data formats.

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016) pp. 7509-7516
© Research India Publications. https://dx.doi.org/10.37622/IJAER/11.11.2016.7509-7516

Information Modeling and Processing Steps:

A similarity search problem requires a collection of objects like images, text documents, etc. that collection of objects characterized by a collection of similar features and those are represented as points in a high-dimensional attribute space. Given search items in the form of points in the space, we are required to find the most similar object to the search item. Our method is designed to not only for the similarity search, but also to prevent information leakage. In this paper, we consider a third party data storage system involving three different entities are owner of medical data, data user and the third party server.

Content owner has a collection of n medical images $M = (m_1, m_2, , m_n)$ that he wants to outsource to the third-party server in encrypted format while still keeping the potentiality to search through them for efficient data utilization reasons. Image owners will first build a secure searchable database by compressing all images from the database M before outsourcing image data to third party server. Then image owner encrypts all images using RSA encryption method. At last image owner stores the encrypted data M' on the server.

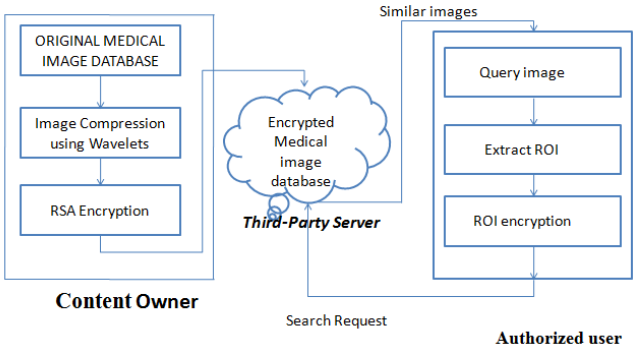


Figure 2: Schematic diagram of proposed method

Users of the content are the authorized ones to use the data which is stored on the server. We presume the authorization between the content owner and content user is appropriately done. For a given search image, an authorized user generates ROI of an image if needed and submits a search request in encrypted form of query image to the server. Upon receiving search request from image user the third party server is responsible to search relevant images and return the corresponding cluster of images from database to the image user. Here the noticeable point is the above discussed process has to be carried out on the encrypted database as similar as possible on the original database.

Third party Server stores the encrypted medical image data for image owner and processes the search of image users. After receiving the search or query, server compares with the images which are stored in the server to return most similar images according to the ranking obtained by the used distance criteria.

TECHNIQUES USED FOR PRIVACY-PRESERVING IMAGE RETRIEVAL

In this part we review earlier methods that served as candidate solutions for privacy preserving data mining in medical field. Some major steps with different techniques will be discussed here.

Wavelet based Image compression

When network storage space and bandwidth are limited, image has to be compressed. It is necessary to preserve the medical image data during transmission from unauthorized access. Hence to reduce the time for encryption and also to reduce the transmission cost, the medical image is first compressed anterior to encryption.

Wavelet based medical image compression involves the use of a new area of applied mathematics simply called "Wavelets". Wavelet compression is a set of a larger class of methods generally referred to as Wavelet based image compression. The first step in this technique generally involves a lossless transform based medical image compression to provide a sparse representation of an input medical image. The transformed medical data are then quantized in order to attain higher compression ratios.

Medical image compression is one of the most successful and useful application of22 discrete wavelet transformation. The discrete wavelet transform can be implemented using some specially designed filter banks. The following figure shows an example of lossless compression with the IWT.

$$X(a, b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} \psi(t - b|a)x(t)dt \quad (1)$$

Let us consider an image I(x,y) of size N×N. The samples of medical image are passed through LPF and HPF filter banks simultaneously and the outputs are down sampled by two along rows. Then the output samples can be further decomposed using the same filter banks and down sampled by two again along columns, giving the approximations LL and detail versions LH,HL and HH with each of size is N/2×N/2.

Approximation coefficients are called as low resolution or low frequency coefficients. The detail versions LH, HL and HH give horizontal detail versions, vertical detail versions and diagonal detail versions respectively. Multi level wavelet decomposition produce approximation and detail versions in each dimension. This type of decomposition can be repeated to increase the frequency resolution and low frequency coefficients decomposed with low and high pass filter banks and then down sampled. In this project, we have conducted experiments using single level decomposition based on Haar wavelet transformation.

In our research, global thresholding method is selected based on Bridge-Massart strategy. This will give effective image compression which can be stored in less space and transmitted more quickly. After compression of all images which are stored in original medical image database, we have to encrypt all images to maintain privacy of personal medical data. In this research, we present RSA encryption method to encrypt all medical images.

RSA Encryption:

RSA encryption is a public key encryption which uses prime factorization as trapdoor one-key function. Following steps shows the procedure of RSA encryption algorithm.

i. Generate two large and random primes p and q.
ii. Compute the modulus $n = pq$.
iii. Choose an odd public exponent e between 3 to n-1

i.e.; relatively prime to q-1 and p-1.

iv. Compute private exponent d.

v. (n,e) is the public key and (n,d) is private key.

The encryption operations exponentiation to the e^{th} power modulo n.

$$C = ENCRYPT(m) = m^e mod n \quad (2)$$

Here m is input medical image, C is resulting cipher image. The original medical image is encrypted with a private key using RSA traditional encryption algorithm. This method makes it possible to encrypt an image of any size with only one exponentiation.

The decryption operation in the RSA cryptosystem is exponentiation to the d^{th} power modulo n.

$$m = Decrypt(C) = e^d mod n \quad (3)$$

In this research, we consider RSA encryption is used to encrypt features from both the query image and database images. Despite that there are number of efficient encryption algorithms available, this report still helps us to understand how RSA is efficiently available in the future, it can help to solve the problem of privacy preserving data mining in the medical field.

After compression of all images, image owner encrypts the compressed medical image database with a private key, and sends all encrypted medical images to the third party security provider for the purpose of privacy preserving image retrieval.

Retrieval with Encrypted Query Image:

In the retrieval stage authorized user's wants to retrieve similar images to particular query image from the third party server. In order to get more similar images, user divides the query image in to two regions: ROI (Region of Interest) and the Region of Background (ROB). In the medical image intensity values of ROI contain important information. After segmented ROI from the query image user generates a secure encrypted image with the resulted ROI image in order to avoid information leakage. Then encrypted ROI image is submitted to the third party server. With the encrypted ROI image the third party server returns most similar images by searching on the encrypted database images.

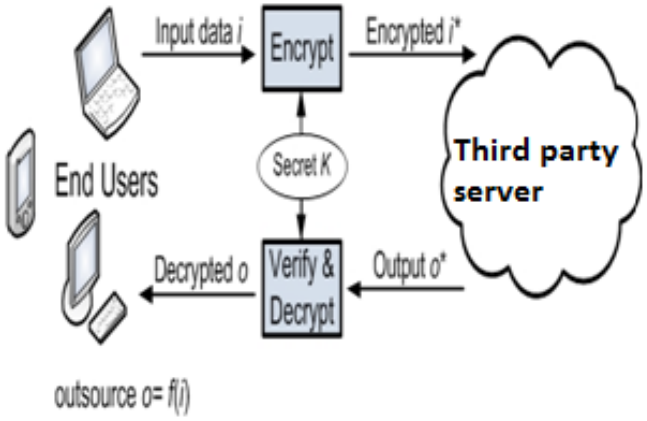


Figure 3: Content user to extract similar images

Once receiving a request from user, the third party server performs search operation on the hived away encrypted database. Then the third party gets a list of images corresponding to every component of encrypted feature vectors.

Euclidean Distance Metric:

In this research image categorization is performed by Euclidean metric or Euclidean distance. Euclidean metric is a measure of ordinary distance between two points, and is given by Pythagorean formula. By using this formula as distance measure, Euclidean space becomes a Euclidean metric space. The related norm is called the Euclidean norm.

Euclidean distance measure between two points' k and l is the length of the line connecting them. If k and l are two points in Euclidean n-space, then in Cartesian coordinates the distance from l to k or from k to l is calculate by following equation.

$$d(k,l) = d(l,k) = \sqrt{(l_1 - k_1)^2 + (l_2 - k_2)^2 + . + (l_n - k_n)^2} = \sqrt{\sum_{i=1}^{n} (l_i - k_i)^2} \quad (4)$$

After computing medical image distances, the third party server ranks all these medical images based on their distances with query encrypted medical image. Finally, the third party server transmits the most relevant encrypted medical images to the authorized user as search results.

By receiving the encrypted medical images given by the third party server, user decrypts these medical images with private key which is shared by data owner, and obtains decrypted medical images similar to query image.

RESULT ANALYSIS:

In this section, we compare two major types of data mining techniques namely encryption based privacy preserving and ordinary data mining techniques. Detail experiment results and quantitative analysis are provided in order of their retrieval accuracy and computational efficiency.

Security efficiency comparison:

Privacy preserving medical image search scenario considered in this research, the third party server stacks away only the encrypted medical images and performs data mining based on encrypted form of selected ROI query features. We assume the third party server as a semi antagonist i.e., it follows the protocols for execution requirement, but may use what it observes in the process of execution to infer additional information. Such a semi honest system is applicable to such scenarios as online service providers, who would like to know as much as possible about the content users for benefits like better targeted ads, but would not intentionally break the user's privacy. A content user who wants to utilize these online third party services computational power for easy authorized access, reliable storage and better organization of owner private medical dataset, but wants to reveal as a little bit information as possible to the third party server beyond what is exactly necessary for the third party server to provide necessary services.

Given that the database images are compressed by using wavelet compression technique to increase transmission speed

and then encrypted by using highly secure ciphers, the main security objective will be to minimize information leakage from the encrypted database and from the search process. Euclidean distance based image retrieval relies on comparison of different image metrics to capture semantic similarity between medical images. Stacking away raw images without any protection is never wise, because visual content can disclose important information about image content. Proposed algorithm will hide the visual content of an image and make it difficult for an adversary to probe the important content of encrypted medical images.

In the first stage of research, a number of experiments which are used to analyze the proposed wavelet based compression and RSA based encryption algorithms will be presented. To evaluate the proposed method some aspects were examined.

Security: In this research security means privacy preserving and robustness against various attacks. In our research used encryption algorithm that make them difficult to cryptanalysis.

Speed of transmission: By compressing all medical images from the given dataset we can increase the speed of transmission. Our proposed wavelet based compression algorithm will give better compression results in a lossless manner.

Compression ratio: Measures the ratio of compression between the uncompressed image size and the compressed image size is defined as,

$$CompressedRatio = \frac{SizeofCompressedImage}{SizeofUncompressedImage} \tag{5}$$

Correlation: Correlation gives the similarity between the reconstructed image and original image. Correlation is defined as,

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \tag{6}$$

Here, $I_1(r,c)$ is the intensity of pixel at (r,c) position of original image,$\bar{I}_1$ is the mean of original image defined as,

$$\bar{I}_1 = \frac{1}{MXN}\sum_{r=1}^{N}\sum_{c=1}^{M}\big(I_1(r,c)\big). \tag{7}$$

$I_2(r,c)$ is the intensity value of pixel at (r,c) position of reconstructed image,$\bar{I}_2$ is the mean of reconstructed image defined as,

$$\bar{I}_2 = \frac{1}{MXN}\sum_{r=1}^{N}\sum_{c=1}^{M}\big(I_2(r,c)\big) \tag{8}$$

M is the height of size; N is the width of image and r, c is row and column numbers at each pixel. Results were taken on some images and accuracies are displayed in below tables.

Table1: Comparison results of Compression and correlation

Original Image		Encrypted Image				Reconstructed Image		
Image Name	Image Size (bytes)	Image size (bytes)	Simulation time	Compression Ratio	Correlation	Image size (bytes)	Correlation	Simulation time
CT Image1	262144	65536	0.92	0.088	0.0064	262144	0.9976	0.79
CT Image2	160000	65536	0.92	0.088	0.0164	160000	0.9965	0.79
MRI Image1	250000	65536	0.92	0.088	0.0017	250000	0.9995	0.79
MRI Image2	65536	65536	0.92	0.088	0.0008	65536	0.9999	0.79

Search accuracy comparison:

Good search accuracy means that the most top ranked images have high relevance to the query medical image features. Due to the semantic gap between perceptual features, irrelevant images may be retrieved as similar results and degrade the search accuracy. A good privacy preserving search technique should give as best search accuracy as possible when compared to ordinary search without any protection.

We perform the metric based search experiments on Oasis medical database. These medical images are grouped by modalities into two categories with 100 images in each category of CT and MRI. Medical image data mining accuracy is evaluated using precision and recall. Precision and recall are defined as

$$Precision = \frac{No.ofsimilarimagesamongretrievedimages}{No.ofretrievedimages} \tag{9}$$

$$Recall = \frac{No.ofsimilarimagesamongretrievedimages}{No.ofsimilarimages}. \tag{10}$$

A higher precision at a given recall indicates best retrieval performance. Results obtained for proposed privacy preserving data mining and conventional data mining are given below.

Table2: Precision and Recall Percentages

Image Retrieval technique	Distance calculation technique	Delay(output) In seconds	Precision%	Recall%
CBIR	Euclidean distance	4-6	79.8	80
Encrypted ROI based retrieval	Euclidean distance	11-16	80	82

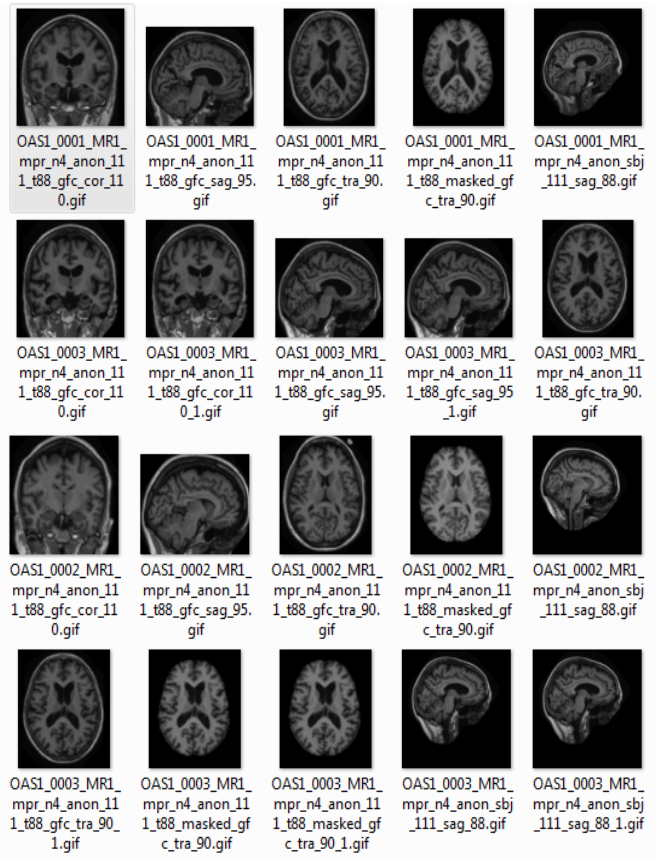
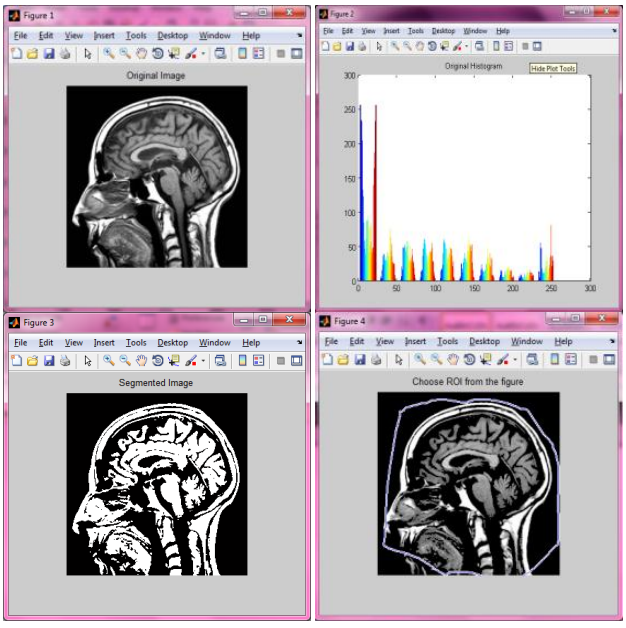


Figure 4: Some Input set of images uploaded

Above shown figure represents regarding upload of images by content user. It contains images of (.tif) tagged image file format with different sizes.

Following figures regarding outputs of proposed system. The retrieved results are depends upon the Euclidean metric of similar images from database which are stacked away in the third party server.



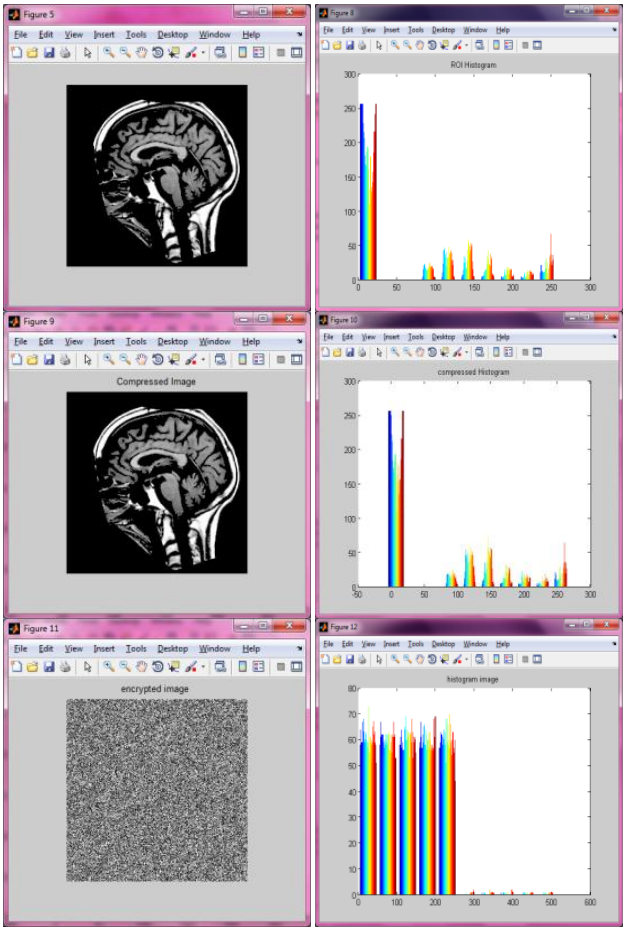
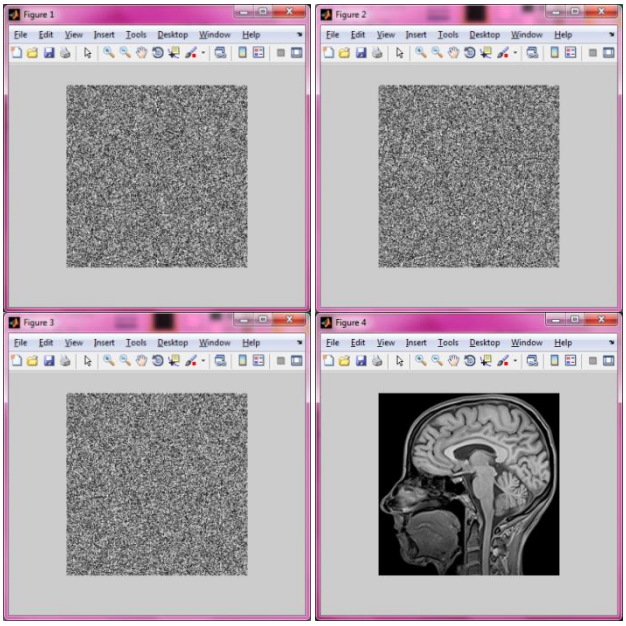


Figure [5]. (a): Original Image, (b):Histogram of original image, (c): Segmented output, (d):ROI selection, (e):Selected ROI, (f):Histogram of ROI image, (g):Compressed ROI Image, (h): Histogram of Compressed image, (i):Encrypted Image (query image for MRI dataset) and (j):Histogram of Encrypted image.



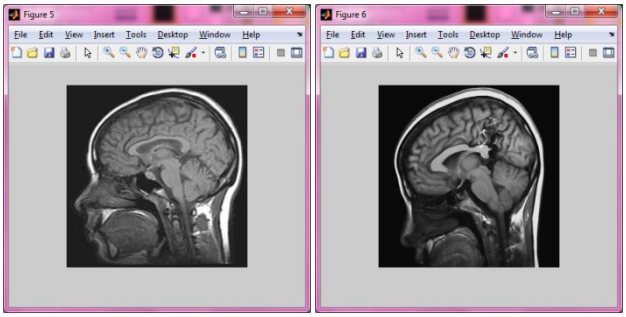
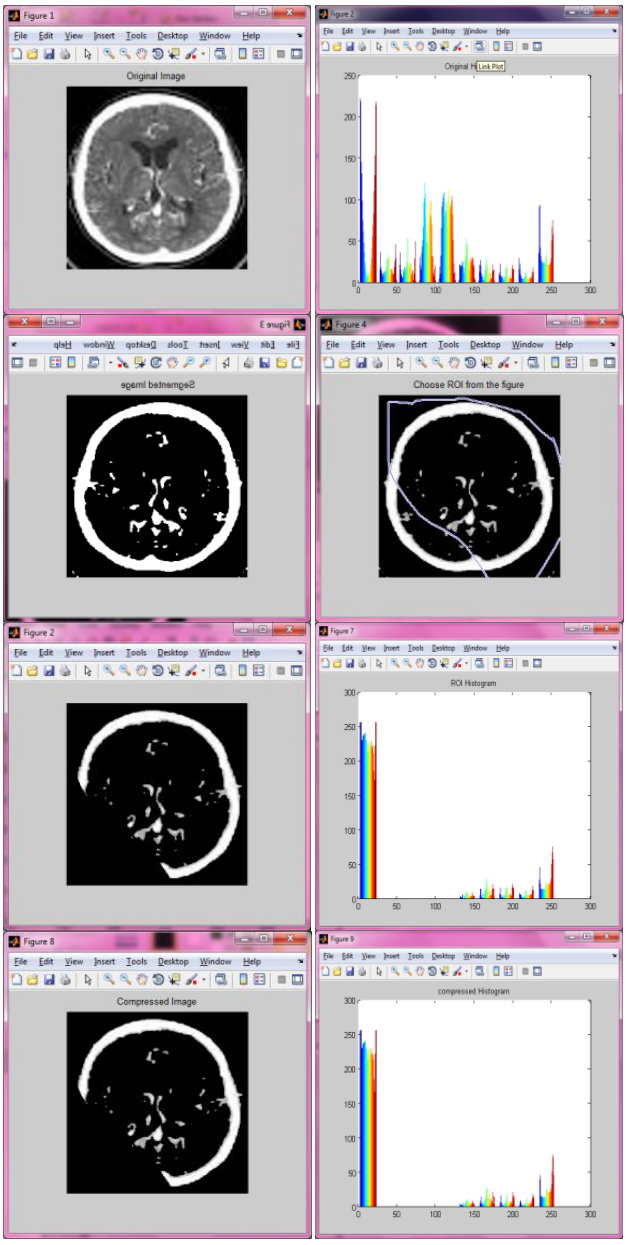


Figure 6: Most similar retrieved images. (a):Top most similar image in encrypted form, (b):2nd most similar image in encrypted form, (c):3rd most similar image in encrypted form, (d):decrypted top most similar image, (e):decrypted 2nd most similar image, (f):decrypted 3rd most similar image



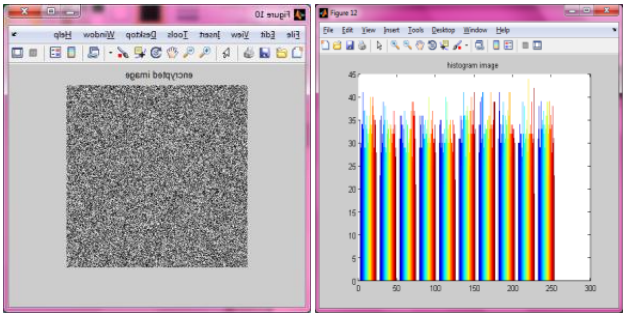


Figure 7: (a): Original Image, (b):Histogram of original image, (c): Segmented output, (d):ROI selection, (e):Selected ROI, (f):Histogram of ROI image, (g):Compressed ROI Image, (h): Histogram of Compressed image, (i):Encrypted Image (query image for CT dataset) and (j):Histogram of Encrypted image.

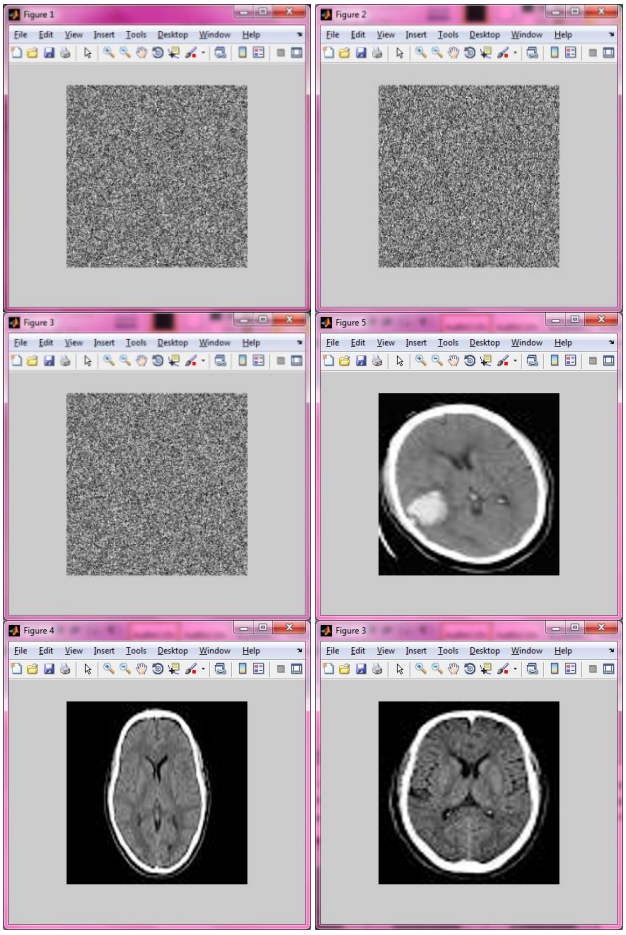


Figure 8: (a): Original Image, (b):Histogram of original image, (c): Segmented output, (d):ROI selection, (e):Selected ROI, (f):Histogram of ROI image, (g):Compressed ROI Image, (h): Histogram of Compressed image, (i):Encrypted Image (query image for CT dataset) and (j):Histogram of Encrypted image.

CONCLUSION AND FUTURE WORK:

In this research, we have analyzed the problem of privacy preserving medical image retrieval. This problem has many

real time applications such as secure third party online services that help manage personal image collection, and problem also challenging several research issues, such as achieving a best trade-off between efficiency and security for real time applications that demands high accuracy and least user involvement. We have reviewed two main types of retrieval techniques, namely techniques based on conventional medical image retrieval and techniques based on privacy preserving medical image retrieval. We have provided quantitative comparison of these two kinds of techniques in terms of precision and recall. We hope the study of comparison offered in this research can provide useful insights in designing security aware techniques for the problem of privacy preserving image search as well as other practical secure online host applications with various levels of security and accuracy retrieval requirements. As a future enhancement we can process the image with its extracted feature set and also work with other encryption algorithms that support partial homomorphic operations and thus provide searchable encryption.

REFERENCES:

[1]. D. Song, D. Wagner, and A. Perrig, ``Practical techniques for searches in encrypted data," in *Proc. IEEE Symp. Res. Sec. Privacy*, Feb. 2000, pp. 44_55.

[2]. Yi Zhu, Xingming Sun, Zhihua Xia, Li Chen, Tao Li and Daxing Zhang, 2014. Enabling Similarity Search over Encrypted Images in Cloud. *Information Technology Journal, 13: 824-831*.

[3]. R. Brinkman, J. M. Doumen, and W. Jonker, ``Using secret sharing for searching in encrypted data," in *Proc. Workshop Secure Data Manag. Connected World*, 2004, pp. 18_27.

[4]. United States Department of Health and Human Services. HIPAA: medical privacy—national standards to protect the privacy of personal health information. Available at: http://www.hhs.gov/ocr/hipaa/

[5]. D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, ``Public-key encryption with keyword search," in *Proc. Eur.*, 2004, pp. 506_522.

[6]. ByungRae Cha, NamHo Kim, JaeHyun Seo and JongWon Kim, "Idea Sketch of Searchable Image Encryption System on Streaming Media," SCTA 2012, Aug. 2012.

[7]. N. S. Jho and D. W. Hong, "Technical Trend of the Searchable Encryption System," ETRI Journal, Vol. 23, No. 4, Aug. 2008.

[8]. A. Swaminathan, Y. Mao, G-M. Su, H. Gou, A. L. Varna, S. He, M.Wu, and D.W. Oard, "Confidentiality Preserving Rankordered Search," Proc. of the ACM Workshop on Storage, Security, and Survivability, pp. 7-12, Oct. 2007.

[9]. Reese, G. (2009) Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly.

[10]. P.C. Cosman, R.M. Gray, R.A. Olshen, Evaluating quality of compressed medical images: SNR, subjective rating, and diagnostic accuracy, Proc. IEEE 82 (6) (1994) 919-932.

[11]. A. Bruckmann, A. Uhl, Selective medical image compression techniques for telemedical and archiving applications, Comput. Biol. Med. 30 (3) (2000) 153-169.

[12]. C. Wang, `` Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud," *IEEE Trans* on cloud computing, vol.1 no.1, 2013.

[13]. Huang HK. Teleradiology technologies and some service models. J Comp Med Imag Graph 1996;20(2):59-68.

[14]. Lou SL, Sickles EA, Huang HK, Hoogstrate D, Cao F, Wang J, Jahangiri M. Full-field direct digital mammograms: technical components, study protocols, and preliminary results. IEEE Trans Inform Technol Biomed 1997;1(4):270-8.

[15]. Huang HK, Lou SL. Telemammography: a technical overview. RSNA Categorical Course Breast Imaging 1999;273-81.

[16]. Stahl JN, Zhang J, Zeller C, Pomerantsev EV, Lou SL, Chou TM, Huang HK. Tele-conferencing with dynamic medical images. IEEE Trans Inform Technol Biomed 2000;4(2):88-96.

[17]. Zhang J, Stahl JN, Huang HK, Zhou X, Lou SL, Song KS. Real-time teleconsultation with high resolution and large volume medical images for collaborative health care. IEEE Trans Inform Technol Biomed 2000;4(2):178-85.

[18]. Stahl JN, Zhang J, Chou TM, Zellner C, Pomerantsev EV, Huang HK. A new approach to tele-conferencing with intravascular ultrasound and cardiac angiography in a low-bandwidth environment. Radio-Graphics 2000;20:1495-503

[19]. Yu F, Hwang K, Gill M, Huang HK. Some connectivity and security issues of NGI in medical imaging applications.

[20]. Digital Imaging and Communications in Medicine (DICOM). National Electrical Manufacturers Association(NEMA).Rosslyn,VA,http://medical.nema.org/dicom/2001.html, Part 15: Security Profiles, PS 3.15-2001; 2001.

[21]. J. M. Zain and A. R. M. Fauzi, Medical Image Watermarkingwith Tamper Detection and Recovery, Proc. 28th IEEE EMBSAnnual International Conference, pp. 3270-3273, 2006.