International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3861-3866

Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage

G. Preethi and N.P.Gopalan

Bharathiar University, Research and Development Centre, Coimbatore, India.
National Institute of Technology, Department of Computer Applications, Trichy, India.

Abstract

The healthcare organizations utilize the outsourcing amenities have been facing critical challenges for scrutinize the significant data. These data are needed to processed and effectively analyzed by better performance. Traditional processing scheme has no longer able to process the huge data. They were not at all having a security system for medical images.. In order to achieve the scalability, data security issues to combine the image compression using symmetric key homomorphic encryption in cloud computing. The existing techniques are available to provide data security with the help of steganography and contrast enhancement. This technique has some drawback of image quality due to various noises. The proposed technique is used to protect the data by inserting images into the data an efficient Reversible Data Hiding (RDH). This is securing the private image and documents in the cloud storage. The Experimental result shows the good image quality and improved cloud storage capacity. The image quality having acceptable PSNR values is 72 dB and over. This paper has an enhancement of data security with the healthcare data, confidential data in the cloud environment.

Keywords: Data Hiding, Image Security, Reversible Data Hiding, Symmetric key, Compress and Uncompress of Image Recovery.

INTRODUCTION

The growing field of information technology provides the database outsourcing has become essential for nowadays. There are different types of clouds namely public cloud, private cloud, and hybrid cloud. These clouds are used accordingly to their own purposes. Rapid growth of technologies the healthcare generate varieties of data in various organizations. The promising technology is cloud computing which can provide the related resources such as storage, process, analyzing the data, data security and platforms are delivered as services [10]. Many organizations have to keep data in their own cloud for future use. The cloud service provider gives a guarantee for protecting data from unauthorized people. Even though the organizer's or user to store the information in a better way. The Healthcare data is more confidential as well as to provide better quality services. The patient's information and clinical information are shared in a secured way. Safety, quality, and efficiency of patient care are reducing healthcare cost in Electronic Medical Records (EMR) and Electronic Health Records (EHR) to the grand vision of healthcare digitization. The digitized documents are supported both present and future care received by the patient from the same or other clinicians, is the primary purpose of the HER [9]. The Electronic Health Record provides communication between patient and clinician. The clinical reports and scan images are stored in a cloud database. This allows the sharing of images and access by other users in anywhere in the world. This is an advantage of cloud computing even though still there are prospective risks in privacy-preserving system. There are lots of approaches available to secure the confidential data and images for preventing from unauthorized users over the cloud storage such as contrast enhancement techniques, Histogram equalization, Morphological enhancement, secret image sharing etc. In this paper proposed the image encryption techniques using symmetric key steganography for data security in cloud storage.

RELATED WORK

The data is embedded into image and transfer from one position to another position. Some noises are included when the receiver extracts the image and has some issue with the quality of the image. These problems are avoiding Kalker and Willems suggest the method is RDH. The receiver has the image to extract in a reversible manner [2].

The public domain cloud system has a potential for security and privacy when using a mobile device. This author presents an efficient image protection method for private images in the cloud by using steganography technique. The results are shows that the enhance image security of private images also increased the cloud storage capacity [1].

The author J. Tian used a novel method of data embedding into the image using a steganography. This paper proposed a method for enlarging an image and to create some space between the two pixels. In the pixel data are embedded into it. At the final stage of receiver extract space and get the image in a secure way. The original images are restored back without any change of original size of an image. This has some limitation of creating a space between the pixels because the enlarged image doesn't have the quality of image [3][14].

The following author V.Sachnev, H.J.Nam etc, introduced data hiding method, which has the combination of differential and Wavelet transform. To enlarge the image used to selecting the two-pixel point from the cover image to draw the histogram [4][13]. In the histogram, peak points are calculated and the data is embedded into it. The data are extracting by encryption technique and restore the original image. This also

has some limitations of image quality and processing was very low in this method.

The new approaches were introduced by X. Zhang that is an image compression via the LSB technique. The chosen image partitioned into major two parts of A and B. In the first part of A has compressed image and create some space for embedded the image into it. The part B image is extracted in a reversible manner [5][15]. This approach has some problem of creating space and converts the LSB part A into part B in reverse order without encryption key to sharing the image.

A. Markandey and S. Moghe etc used the image encryption techniques to maintaining the private security in the cloud server. They suggest to allocate a memory space for an image in the cloud server and then to encrypt the image. Allocating memory space is not familiar for all the clients. This approach concentrates only to secure the images, not for the confidential data [6][11][12]. These security systems were worked in server side. There is no guarantee of client- side encryption on this approach.

OUR CONTRIBUTION

The data hiding with an image has a high security in cloud storage. The confidential data to encrypted using the symmetric key of large factorization and then the cover image has split into the matrix form of compressed and uncompressed cells in it. These cells are extracted without changing their data content or image quality using Reversible Data Hiding techniques.

PROPOSED METHOD

The proposed new way is an encryption using image inserted into the text and providing the reversible data hiding through the symmetric key. Initially, the given data is divided into two parts that's LSB and MSB. The LSB stands for Least Stored Bytes and Most Stored Bytes, the uncompressed data are stored in the LSB of cloud storage. The data have to insert into the image for encryption with a symmetric key in the form of compressed images. The unauthorized reader has to open only the image file without their knowledge of data hidden into it. The images are split into the number of cells each cell contain the compressed data with the cover of the images. The unauthorized users are well known encrypts, the compressed image on the three cells of images able to view in the form of uncompressed it's indicated by 1 and the other compressed parts are indicated by 0 which can't display to the user. These cells are created by a randomized approach of the matrix using the similarity of tic-tac-toe technique in AI. The matrix has been expanded to 3 x 3, 5 x 5, 7 x 7, etc [7][16], matrices dependence on the length of hiding data and images. The receiver has a key to decrypt the image, and then the uncompressed image shows the hidden data to the user. The following diagram shows the compressed images in the block indicate 0 and the unauthorized users can track the image of data which is the form of uncompressed images in the block indicate 1.

Definition 1:

$O_i = \{ \forall\, C_{ij} \in I_{ij}, Uc_{ij} \leq C_{ij} \}$ and $D_i = \{ \forall\, DC_{ij} \in T_{ij}, DUc_{ij} \leq DC_{ij} \}$, where 1≤ i≤ n and 1≤ j ≤ m. The original image is compare with data whether both compression and uncompressing are same or not. The images are embedding to the text message and it will extract from the cover of image. The hidden information is shows to the authorized users otherwise the compressed cell image shows to the user with the help of comparing height and width of the pixels.

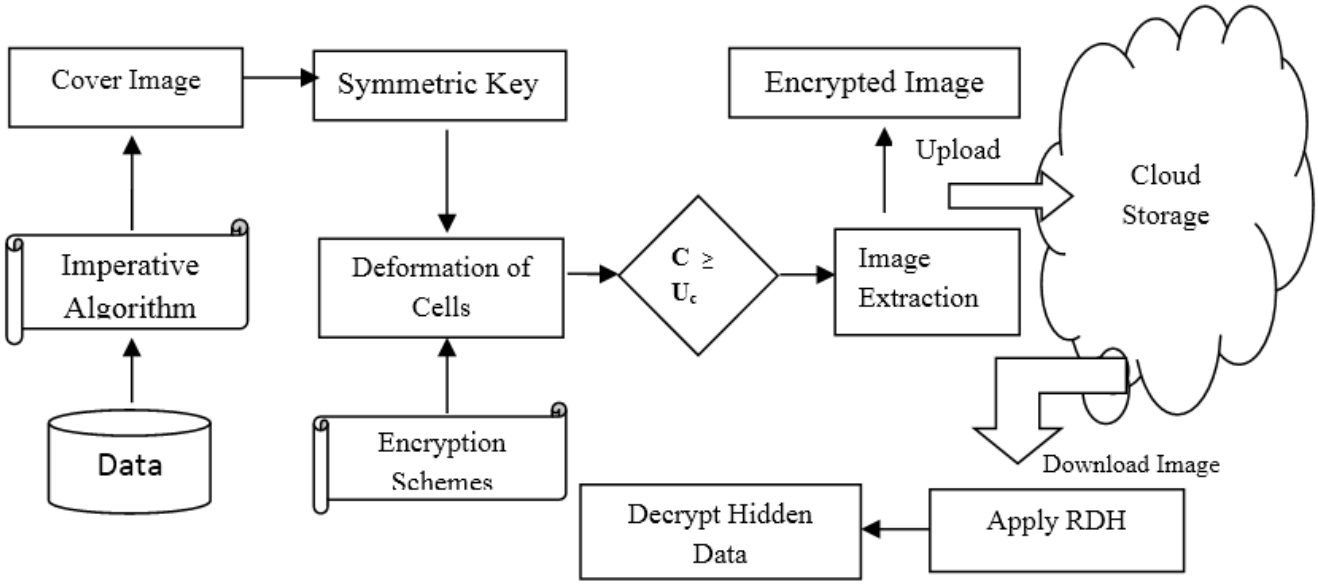


Figure 1. Architecture of Proposed System

Definition 2:

$$CI = \{ I_{ij}^{c} \mid I_{ij}^{c}, I_{ij}^{c} = (H_{ij}, W_{ij}, C_{ij}) \} \; and$$

$$HT = \{ H_{ij}^{uc} \mid I_{ij}^{uc}, I_{ij}^{uc} = (H_{ij}, W_{ij}, C_{ij}) \}$$

Where i = 1,2…n and j = 1,2,…m. Coved Image (CI) and Hidden Text (HT). The number of row (n) and number of column (m) are compared in the compressed image and uncompressed image. If the definition is true the cell are randomly allocate to compress or uncompress. This techniques show in the following diagram.

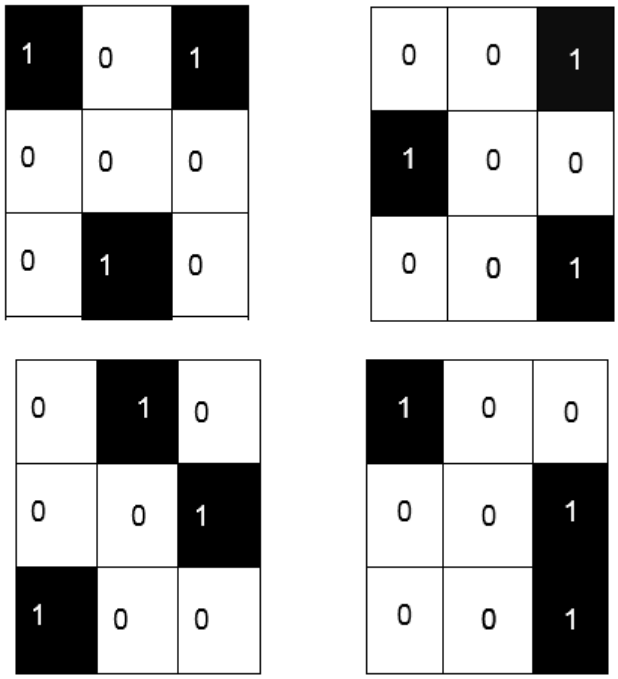


Figure 2. Compressed and Uncompressed deformation of 3 X 3 connect

Image Embedding to the confidential data:

The procedure is used to cover up the designated image underneath the confidential data. In the proposed system has to identify the LSB of cells in the cover image is indicate the compressed images. The given below image has $I_{ij}^{c} = (230, 267, 14)$ and the $Uc_{ij} = (cell_{no}, Cell_{height}, Cell_{width}, 065)$. The uncompressed cell has a pattern to differentiate the original compressed image. The hacker well known about encrypts to hack the image to identify the hidden message. The proposed system has to differentiate cells to be filled by the patterns or colors. Even though the uncompressed cells do not shows the complete image or hidden data to the user. This is added the advantage of the proposed system. Our scheme has been identifying the partitioned image in the form of n x m without any overlapping of cell in the image. The hidden data could not affect in any way by the proposed system. The identified uncompressed cells are transform (1) RGB color model [8] into YIQ coordinates of C_Y, C_I, C_Q color matrix transformation from the equation (3).

$$\begin{bmatrix} C_Y \\ C_I \\ C_Q \end{bmatrix} = \begin{bmatrix} 0.326 & 0.512 & 0.142 \\ 0.578 & -0.263 & -0.329 \\ 0.215 & -0.482 & 0.321 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 123 \\ 267 \\ 14 \end{bmatrix}$$

Finally, the RGB color image is retrieved as follows

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} C_Y \\ C_I \\ C_Q \end{bmatrix} * \begin{bmatrix} C \\ M \\ Y \end{bmatrix}$$

The CMY color model represents the black color as an entity column vectors. In the above equation, YIQ is representing the brightness, hue, and purity of the pattern or color. The Y parameter incorporated the colors of red, green and blue intensities in the standard luminosity curve. In the black and white image contain very less Y signal only. As well as the, I contain the orange and cyan hue information provides the flesh-tone shading approximate bandwidth is 0.0015 GHz. Finally, the parameter Q has the green and magenta hue information provides the approximate bandwidth 0.0006 GHz. Then n x m block value is equal to the cover image underneath the hidden data, where $U_c = 1024_{hcells} X 1024_{vcell} X\, N_{bytes}$. The proposed scheme has the ability to hide the data into the image with help of compressed and uncompressed cells in the confidential image and data. The image size is expanded until the size of data. The hidden data has been stored in the cloud storage very securely.

Image Extraction from the Secret Hidden Data:

The proposed method used to extract the hidden data from the covered image. Initially, the user downloads the image which image wants to extract and know the hidden data from the cloud storage. We use the random approach to identify the uncompressed and compressed cells in the covered image. The uncompressed images have RGB color without any changes on it. The extracted cells have different YIQ color model to be filled by the pattern or color chosen by the user. The brightness, hue and purity luminance are providing the YIQ color model at each and every cell in the cover image.

Step 1: download the cover image wants to extract the hidden data.

Step 2: To obtain the symmetric key for extract the image.

Step 3: Convert image into the matrix form of encrypted image, matrix is M

Step 4: Matrix has n number of rows and m number of columns.

Step 5: Obtain the tic-tac-toe technique to identify the alternate cells in the split image, a01 to a20.

Step 6: Compute the following factors:

$$[n_1, m_1, x_1, U_c, C] = gsvd\ (A_{11}, D_m)$$

Similarly

$$[n_2, m_2, x_2, Uc, C] = gsvd\ (A_{12}, D_m)$$

Obtain the decrypted symmetric key matrix image Dm is same as the encrypted symmetric key matrix.

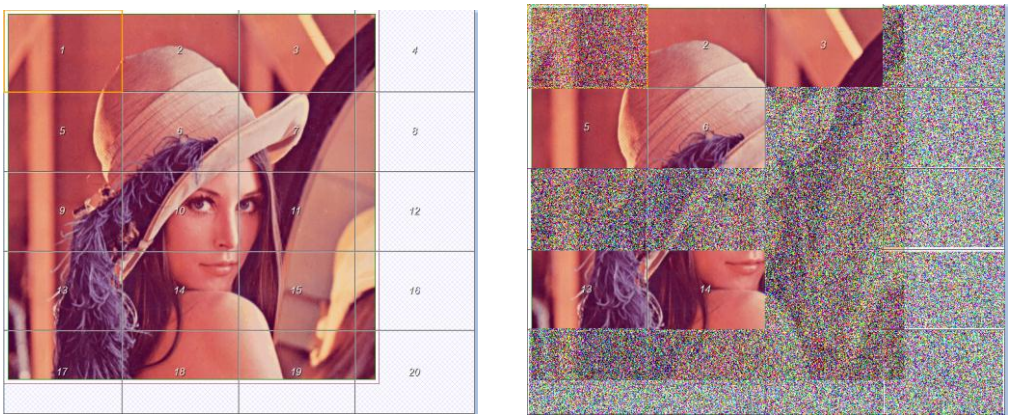
Step 7: Extracted U_c cell from each row in the image pixel to count the number of uncompressed cell U_c and each time to compare the compressed cell count C.

Step 8: Each cell bits draw out from the cover image pixel and repeat until the cells are reache (5)

Step 9: The identified U_c are transformed from RGB color model into YIQ

Step10: Count the Uc and C ce (6) n repeat else stop the process.

Step11: Repeat the Step 7 and Step 9 until the complete cover image pixels are processed.



(a) (b)

Figure 3. (a) Original Image (b) Compressed Cells and Uncompressed Cells using RDH

EXPERIMENTAL RESULT:

The image decomposed into a number of cells. The compressed image and uncompressed cells are highlighted using a proposed RDH using bilinear scaling transformation. The various tests are applied in the image and size of their image shown in table 1. The cover image divided into a number of cells approximately 3 x 3, 5 x 5, 7, x 7 etc pixels from the original image. In the image has compressed and uncompressed cells in the form of horizontal or vertical decomposition based on the user preferred algorithm such as Bilinear, Lanczos, Hermite of set scaling parameters the results shown in the Figure 3 (a). The uncompressed cells in image have the color model of YIQ to differentiate the original RGB color model cells shown in the Figure 3 (b). The proposed method is used to encrypt the cell and process the symmetric key RDH for giving the security of hidden data. This process is described detail in above. The compressed and decompress cells results are obtained in various levels that shown in table 2. In this paperwork has set the parameter Uc, C and $\alpha = 0$ or 1. These parameters are used to compute the extracted images whether having same color or pattern of YIQ color model for differentiating the compressed and uncompressed cells. The encryption has an image with the hidden data to be extracted by a symmetric key of both sender and receiver. The large number of factorization key is used in the encryption as well as decryption with the same as to cell extraction from the cover image. The proposed system to be obtained by applying the symmetric key encryption in the cover image then the RDH is performed to extract the hidden data. Our experiment results show the security of data against from all kind of encrypts, cryptanalytic, and brute force attacks. The homomorphic encryption systems perform only the subtraction and addition, in order to avoid this limitation our proposed system performed the Exclusive-or (XOR) symmetric key homomorphic encryption scheme. The extracted cell of compress and uncompress in the image is used this technique for getting more secure of private image, confidential data in the on-demand services. Our result has proved the encryption of image data hiding is excellent and gives the clear analysis report of the experiments.

The image hidden data is having a secure cryptosystem with the symmetric encryption plays significant responsibility against the brute force attack for having high cloud security system. The proposed system has a fast encryption and decryption using large factorization key to make infeasible of attackers. Our algorithm used a key size is divided into a matrix to increase the time complexity. The compressed and uncompressed cells are already stored in the form of a matrix.

However, we found that the correlation between the compress and uncompress image to reduce the key size and increase more secure from the unauthorized or from the attackers. The proposed system preformed the statistical analysis between the histograms and correlation of encrypted the image has reconstructed of the image with an original image get back. The False Rejection Rate is very near to zero for the original image and encrypted image. The efficiency of False Rejection Rate is 0.0153% and False Acceptance Rate is 96.75%. This means a proposed system has perfect encryption and decryption of compress cell and uncompress cell for RDH. The time complexity has to reduce at 0.326 sec for both processing to get the hidden data image which includes the encryption and decryption for cloud-stored images. The proposed method was executed in MATLAB 7.0 shows the performance which is measured on 3.0 GHz. Intel Core i3 processor with 4 GB of RAM running Windows 7.

The PSNR value is calculated by the formula,

$PSNR_i = 10 (In (x)/ In (10)) [M^2_{fluc} / M_{SE}]$

Where i = 1,2, … n, n > 0 and M_{fluc} is the maximum number of fluctuation in the cover image input. However, the Peak Signal to Noise Ratio to be calculates the cell difference of two images. The equation (7) is used to calculate the PSNR values for cover image and confidential data. The Mean Square Error (M_{SE}) value is calculated by the formula

$$M_{SE} = \frac{\sum_{r,c}[Image1(r,c) - Image2(r,c)]^2}{r * c}$$

Here, calculating difference between the first and second image row and column of regression points. The average points of all error values are identified and measure by the equation (8).

Table 1: Dissimilar key Image Name and Size

Cover Image Name	Cover Image Size
Lena.tif	768k
Lena.jpg	136k
Harbor.tif	488k
Plam.tif	800k
Magickingdom.tif	18k
Orangebuilding.jpg	(7)
Panda.jpg	153k
ZebraColor.jpg	89.1k

Table 2: Performance of Proposed Method Using RDH in Image Encryption

Confidential Data Size	Reduce Size of Image for Fitting Confidential Data	Embedded Cover Image Quality	Uncompressed Data Length (%)	Number of Changing Cell Rate	PSNR of Cover Image (dB)	Mean Square Error (MSE)	Maximum Fluctuation Time (R)
652k	116k	High	16k	48	0.009	7.3280×10^{-48}	0.5
109k	27k	High	5k	28	0.321	7.1203×10^{-28}	0.3
365k	123	Medium	17.4k	28	58	6.7872×10^{-28}	1.3
760k	40k	High	44.4	18	48.23	7.2038×10^{-18}	1.9
10k	8k	Low	3	6	93.12	4.0021×10^{-6}	0.001
182k	18k	Medium	7.1	28	42	6.9601×10^{-28}	0.6
126k	27k	High	9	18	0.02	8.3631×10^{-18}	0.001
79k	10.1k	High	15	6	33	4.3086×10^{-6}	1.1

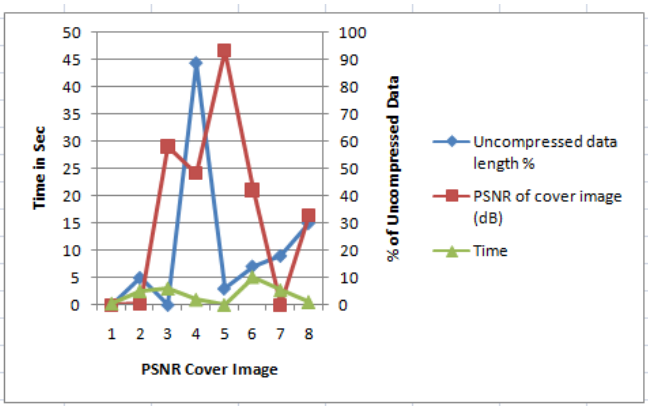


Figure 4. Time Complexity of Cover image and Uncompressed Data Encryption

CONCLUSION

The proposed image encryption method has very secure and privacy of hidden data over the cloud storage. We use the image extraction of compressed and uncompressed cell using RDH. The differentiation of image shows of pattern in alternative cells and compressed cell having RGB color model to protect from hackers in the cloud. Moreover the proposed system reduces the memory space in cloud to extract split cells in order to avoid the overlapping of hidden data and image. The important data, images to be stored very securely so the images are encrypted and the image size is reduced and preserve the cloud storage capacity. This has double security system of data in the cloud. The result of data has no change and increased the security of images while share in cloud. The health care data and images are shared in the way of proposed system in secure manner. In future work, we plan to increase the symmetric key size for encryption of hidden data to provide secure services in the client side.

REFERENCES

[1] Helei Cui., Xingliang., and et al., 2017, "Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing", IEEE Transaction on mobile computing, Vol. 16, No. 5, pp. 1315 – 1329.

[2] Mirza Abdur Razzaq., and Mirza Adnan Baig., 2017, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking", IJACSA, Vol 8, No. 5, pp. 224-228.

[3] Mohammed Abdul Hameed Jassim Al-Kufi., et al., 2017, "An Algorithm Based on GSVD for Image Encryption", Mathematical and Computational Applications, pp. 1 – 8.

[4] Hassan Hajjdiab., Mohammed Ghazal., and Ashraf Khalil.,2017, "Random Image Matching CAPTCHA System", Electronic Letters on Computer Vision and Image Analysis, Vol. 16(3), pp. 1-13.

[5] Marwan, M., Kartit, A., and Ouahmane, H., 2017, "Security in Cloud-Based Medical Image Processing: Requirements and Approaches", ACM ISBN 978-1-4503-4852-2, pp. 354-360.

[6] Wen-Chuan Wu and Shang-Chian Yang., 2017, "Enhancing Image Security and Privacy in Cloud System Using Steganography, pp. 321-322.

[7] Dongmei Li., Xiaolei Dong., and Zhenfu Cao., 2016, "Secure and privacy-preserving pattern matching in outsourced computing", Security and Communication Networks, pp. 3444 – 3451.

[8] Raid Khalid Hussein., and Ahmed Alenezi., et al., 2016, "A Framework to Secure the Virtual Machine Image in Cloud Computing", IEEE International Conference on Smart Cloud, pp.35 – 40.

[9] Marwan, M., Kartit, A., and Ouahmane, H., 2016, "Cloud – Based Medical Image Issues", IJAER, Vol. 11, No. 5, pp. 3713 – 3719.

[10] Yassin, Ali A., Abdullah, A., and et al., 2015, "Cloud Authentication Based on Encryption of Digital Image Using Edge Detection, International Symposium on Artificial Intelligence and Signal Processing, pp.1-6.

[11] Markandey, A., Moghe, S., 2014, "An Image Encryption Mechanism for Data Security in Clouds", 2014 IEEE GHTC – SAS, pp. 227-231.

[12] Andrews Sobral., and Antoine Vacavant., 2014, "A comprehensive review of background subtraction algorithms evaluated with synthetic and real videos", CVIU 122, pp.4 – 21.

[13] Ritika and Sandeep Kaur, 2013, "Contrast Enhancement Techniques for Images – A Visual Analysis", IJCA, Vol. 64, pp. 20 – 25.

[14] Jyotika Kapur., Akshay., J. Baregar., 2013, "Security Using Image Processing", IJMIT, Vol 5, No. 2, pp. 13 – 21.

[15] Shini, S. G., Tony Thomas., and Chithraranjan, K., 2012, "Cloud Based Medical Inage Exchange – Security Challenges", Elsevier, Procedia Engineering 38, pp. 3454 – 3461.

[16] Somaya AI-Maadeed, Afnan Al-Ali., and Turki Abdalla, 2012, "A New Chaos-Based Image-Encryption and Compression Algorithm", Journal of Electrical and Computer Engineering, Vol 2012, pp. 1-12.