International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

An Efficient E^2C^2 Visual Cryptographic Technique to Secure Medical Images in Cloud Environment

Bincy Jolly, Senthilnathan T

Abstract*: Secure storage and easy retrieval of data is major concern for patients when medical data is stored over cloud platform. The unique features of cloud environment are high performance, data availability and security among which security of data stored in cloud environment is sensitive it can be easily attacked by intruders. Concerning medical images, while storing data, proper secure authentication method should be applied in order to avoid misuse of medical data. When this medical image is retrieved, the clarity of retrieved image should be high in order to determine the exact cause of sickness. This paper focuses on proposing a secure storage and retrieval of medical images stored in cloud with visual cryptographic technique using AES algorithm. The experimental results show that the proposed system is able to store images securely and retrieve medical images with high clarity.

***Keywords* : medical image, cloud storage, visual cryptography, AES algorithm.**

I. INTRODUCTION

As an evolution of anytime anywhere computing, the data collected every day is exposed in one way or other way. Therefore, the chances of unauthorized access of data is high. Recognizing this factor Moni Naor and Adi Shamir introduced a new concept called Visual Cryptography [1] which is a technique providing image is encrypted into shares in a manner decryption is possible only if required number of corresponding shares are stacked together. Since decryption is performed using human visual system, this idea ignored the utilization of key while exchanging data [2].

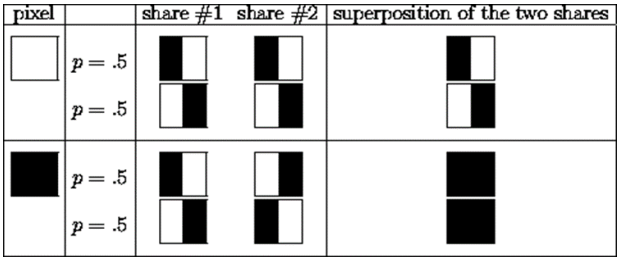


Fig. 1.Naor and Shamir Visual Cryptography 2-out of -2 Scheme

Cloud Computing provides platform for accessing, storing and retrieving data through several servers compared to remote host over internet [3].

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Bincy Jolly, Department of Computer Science, CHRIST (Deemed to Be University), Bengaluru, India. Email: bincy.jolly@mca.christuniversity.in.
Senthilnathan T*, Associate Professor, Department of Computer Science, CHRIST (Deemed to Be University), Bengaluru, India. Email: senthilnathan.t@christuniversity.in, +91 9865555222

The advantages of storing medical images over cloud network includes limitless storage, data portability and migration [3].

The threats of cloud environment comprise DoS attacks and legal issues [4].In modern healthcare information system medical image processing acts as the back bone [3]. The emergence of cloud computing enhanced the storage and transmission of patient's health records. Medical pictures stored over cloud network can reduce the burden of keeping records manually [5]. The patients might not be willing to disclose their sickness information hence necessary care should be taken while handling medical data in cloud [6].

To enhance security data is stored in encrypted format [7]. Encryption of data is usually performed by means of cryptography. The two types of cryptography include symmetric cryptography where the sender and receiver share identical key and asymmetric cryptography in which the sender and receiver share different key [8]. Advanced encryption standard algorithm is a symmetric key algorithm that encrypt image of block size 128 bits. The cipher key lengths can be 128, 192 or 256 bits [9].

II. RELATED WORK

In [10], the author studied on the methods for medical images to be stored securely in databases such as cloud using visual cryptography. The drawbacks of existing system are image interference problem, lack of proper encryption methods, outdated watermarking systems and so on. Initially the input image is selected and a discrete wavelet transform is performed which divides the image into its shares then an optimal threshold value is obtained for all the shares using modified cuckoo search. The secret image to be embedded is converted into a binary message. Then extraction process is performed. The extracted image will be having dual shares. These dual shares will give the original image.In [11], the author proposed model the input image is a plain image in which a function has been applied to obtain the secret key. The secret key is used to shuffle the pixels on the plain image based on an algorithm and it produce the ciphered image which can be stored or transmitted. The ciphered image is operated on the function to obtain the key and decryption is performed. This system was used on RGB images. The advantage of this approach is that there was no pixel expansion during encryption and decryption resulting no change in the size of the image.

In this paper[12] proposes a BIOMETRIC based Visual Cryptography scheme to address the authentication issues. The methodology proposes the finger print image which is obtained from the user is Steganographed with PIN

NUMBER of the user and the Steganographed image which in turn is divided into two shares. One share is stored in the bank database and the other share is provided to the customer. Hash code is generated for the customer share and it is stored in the bank database. One Time Password (OTP) is used every time to ensure the trusted submission of shares. This has the earliest method of sharing secret codes and message. This proposed approach is aimed to made several implementations to increase the data security and user authentication is the arena of visual cryptography. The proposed approach is aimed to provide visual cryptography with encrypted data transfer [13].

Objective of the paper[14] is to Reconstruct lossless secret image. This methodology proposes a (2, n) XFPVCS to share a binary secret image for n participants. The experiments show that the proposed encryption method has following advantages. The algorithm is a systematic approach for pixel-expansion-free (n, n) XFPVCSs. It provides an adjustable visual quality of meaningful shares.

This paper[15] is based on secure storage of documents on cloud using visual cryptographic technique. The technology used is SDSUVC which eliminates the traditional encryption techniques as traditional visual cryptography is prone to generate noisy data due to pixel expansion. The benefit of this approach includes less storage requirement in cloud and time take is comparatively less for retrieval of original document.

Using two-out-of-two visual cryptography a digital record is split into two records. To ensure security each split is stored at different cloud locations. This work explains the concept of multi cloud environment and the storage of data in multi cloud environment which reduces the data vulnarabilities and security risks involved in a single cloud system.[16].

Proposed the storage of document in cloud that is encrypted using AES. An order preservation encryption(OPE) key is generated which is used to authenticate the user. This generated key is matched with the users OPE and the user is verified. Decryption is done using the same generated key. This ensures security, efficiency and accuracy to the document[17].

Proposed a method to reduce pixel expansion during the process of visual cryptographic share generation using XOR operation by preserving the image quality. the method consisted two phases including a share generation phase and a hiding phase. Shares are generated using XOR operation avoiding the pixel expansion. Then the generated shares are hided using another image using steganography which gives additional security to the original image[18].

Proposed a method to perfectly restore the color images using Two in One Image Secret Sharing Scheme (TiOISSS). The extension of TiOISSS for color images was performed to improve the quality and construct the image perfectly. The RGB components were extracted for share generation. The extracted components were permuted three times by attaching a key to improve the security. During decryption the authenticity is checked using the keys [19].

Proposed a method to protect medical images stored in cloud using Reversible Data Hiding by improving image quality and cloud capacity. The data along with a cover image is split into matrix format and is encrypted using a symmetric key. The cells are decrypted using Reversible Data Hiding Techniques [20].

Analyzed various watermarking techniques and joint encryption algorithms used to secure biomedical images. Hence the detailed summary of different technique of watermark and joint encryption is presented in this paper [21].

Proposed an information hiding technique based on RSA encryption and Discrete Cosine Transform based on patient's medical images. Once the data is processed it can be transferred electronically. This method is prone to lossy compression according to experimental results[22].

Proposed a visual secret sharing scheme that reduces the pixel expansion during share generation of binary images. The gray scale image is converted into binary blocks of three shares of each share having two halves. Combination of any two half shares can generate the exact bit and repeating this step the whole image can be generated. The quality of the generated image is maintained [23].

Proposed a secure record retrieval system that reduces the time for communication between the user and server. Provides secure storage of medication details of a client stored in a cloud database. Since it uses half toning the color image as an input generates color halftone image. Confidentiality maintenance is done by embedding a cover image along with a secret image [24].

III. PROPOSED METHOD

The purpose of proposed work is to create a secure storage and retrieval for medical images in cloud environment. The AES algorithm is considered as the most secured and less time consuming encryption algorithm as it is found six times faster when compared to triple DES. The block size of AES algorithm is 128 bits and it supports key lengths of three different types 128, 192 and 256 bits. The generation of cipher comprises different rounds which is depended on the length of key used. A key having bit-length 128 take 10 rounds, 192-bit key takes 12 rounds and a 256-bit length key takes 14 rounds.

The basic operation in visual cryptography[25] is the original image is transformed into n shares. The vital factors for any (k, n) VCS are the following:

- m - The amount of subpixels into which each pixel is separated into. As m value increases, it is estimated that the resolution of the pixel is reduced.
- α - The relative difference. It is for the loss in contrast. Higher value gives higher resolution quality of image.
- k - The least number of shares needed to re-construct the image. More the k value clearer the reconstructed image.
- n - The total number of shares generated from image. The factors that affect visual cryptography is shown in Fig. 2.

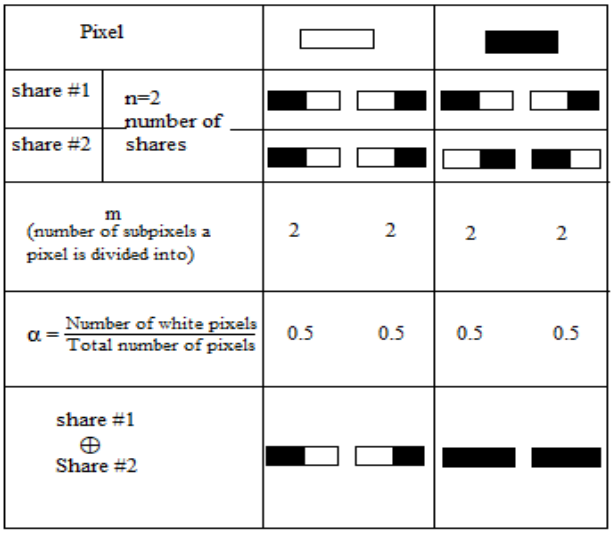


Fig. 2. Factors affecting visual cryptography

Since the data used to secure is medical image, the clarity of the reconstructed image is mandatory, hence n-out-of-n visual cryptographic scheme is used as the n number of shares generate clearer reconstructed image. The Proposed method is shown in Fig. 3.

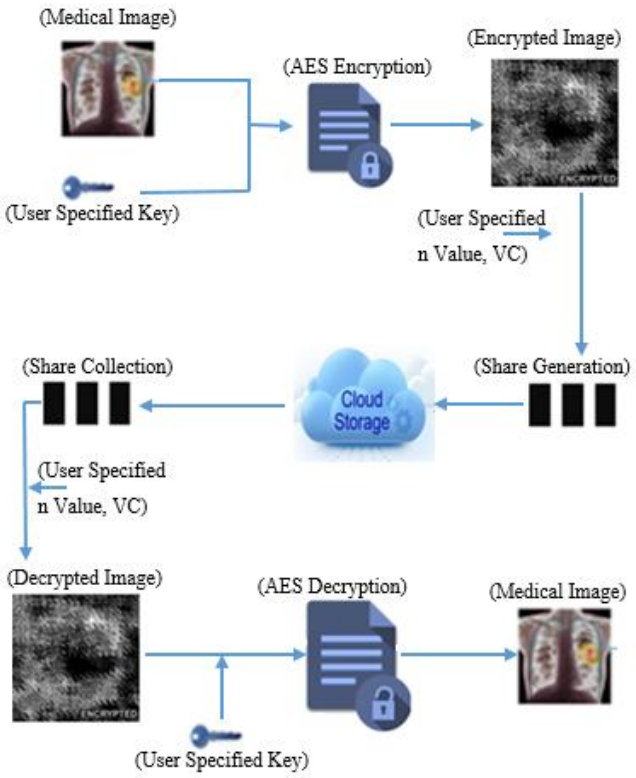


Fig. 3.Proposed method

The proposed method contains the following phases

(i) Encryption phase
(ii) Expansion
(iii) Collection
(iv) Construction/ Decryption phase

(I) *Encryption Phase*

The proposed method uses 256-bit length key, hence the algorithm has 14 rounds. The AES encryption technique uses the following four transformations in each rounds. Sub Bytes Transformation: sub byte transformation can be considered as a nonlinear transformation done on each byte of state. This step uses a substitution table(S-Box). The table consists of all the possible permutation values. Shift Rows: in this transformation, bytes in the particular row of the state is cyclically shifted. The first row remains the same and is not shifted. The second row gets shifted by one byte, third by two bytes and final row by three bytes. Mix columns transformation: it is operated at the column level. Each column of the state is transformed into a new column. AddRoundKey: the round key is added by performing bit wise XOR operation. Then the output is passed to the expansion phase.

```
Algorithm_encryptAES (user specified key, Medical
        Image)
{
        Transform the image pixel as matrix
        Submit the input matrix to the AES S-Box
        While(round<=14)
        {
        Do
                {
                Sub Bytes Transformation
                Shift Rows Transformation
                Mix columns transformation
                AddRoundKey transformation
                }
        }
}
```

(II) *Expansion Phase*

The expansion phase consists of share generation using n-out-of-n visual cryptography technique. The n value is taken from the user for this phase. This phase makes use of the combined effect of AES algorithm and visual cryptography. The RGB pixels from the original image is extracted and is stored in a global Matrix M, where M consists of values from 1 to 255. The resultant image is then divided into n shares. The AES algorithm and shares are bounded together to obtain the resultant shares.

```
Algorithm _generateShare
{
        Do
        {
                extract RGB pixels
                Generate globalized Matrix
                Generate n shares
                Bind with AES for resultant shares
        }
}
```

(III) *Collection Phase*

Collection phase consists of transfer, cloud storage and cloud retrieval of shares. In this phase the shares are stored in a cloud environment. AWS S3 buckets are used for storage. Each share is stored at S3 buckets of different regions.

The collection of shares is happened by retrieving the image shares from specified regions of S3 bucket.

```
Algorithm_Collection()
{
    shareStorage
    {
        Set environment variables
        Configure AWS secret access key
        Configure AWS secret access ID
        For i=1 to n
        {
            do
            Specify image path
            Store i^th share
        }
    }
    shareCollection
    {
        Set environment variables
        Configure AWS secret access key
        Configure AWS secret access ID
        For i=1 to n
        {
            do
            Specify image path
            Collect i^th share
        }
    }
}
```

(IV) *Construction Phase*

In this phase the collected shares are reconstructed together to obtain the original medical image. It has four phases Add round key, Inverse Shift rows, Inverse Substitute Bytes and Inverse Mix column. This phase can be considered as reverse of encryption phase. Encrypted shares are given as input along with user specified key. The round keys are given in reverse order which is followed by the Inverse shifting of rows. Then inverse substitution of pixel positions is performed with the use of key value. The last step is inverse Mix column. These processes are applied to all the encapsulated shares to obtain the original medical image.

```
Algorithm_decryptAES (user specified key, shares)
{
    Do
    {
        AddRoundKey transformations
        Inverse Sub Bytes Transformation
        Inverse Shift Rows Transformation
        Inverse Mix columns transformation
    }
}
```

IV. EXPERIMENTAL RESULTS

A sample image is taken and analyzed on the basis of n-out-of-n visual cryptographic scheme, in which all the n shares are needed to reconstruct the image. Security of the proposed algorithm as well as quality of the reconstructed image is taken into account for the analysis. Fig. 4. illustrates the encryption and decryption process of the proposed method.

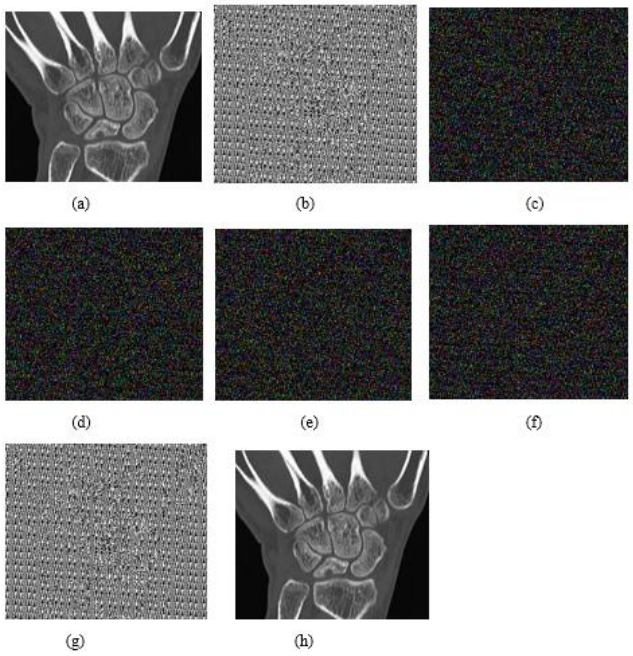


Fig. 4. (a) Original image (b) Encrypted image after AES (c) Share 1 (d) Share 2 (e) Share 3 (f) Share 4 (g) Decrypted image using AES decryption (h) Reconstructed image

(i) MSE, PSNR and SSIM analysis

The PSNR analysis is used to compute the peak signal to noise ratio in decibels. This value is used as a visual quality measurement of the reconstructed image. MSE value is used to compute the mean square error between the original and reconstructed image. Lower the value of MSE, higher the quality of reconstructed image.

Table- I: MSE, PSNR, SSIM values

Image scheme analyzed	**4-out-of-4 VC scheme**
MSE	0
PSNR (in decibel)	Infinity
SSIM	1

Even though the memory size of reconstructed image is slightly greater than the original image, the dimensions of the reconstructed image is same as original image which shows that there is no pixel expansion. The values of the MSE and PSNR indicates that the reconstructed image is of good visual quality. The SSIM value indicates that there is no structural difference between the original and reconstructed image.

(ii) Key space analysis

Key space is the set of all possible keys that can be used in an encryption scheme. An effective encryption scheme should have a key space that is large enough to withstand brute force attack. A symmetric key algorithm with key length *n* will have a key space of 2^n. An encryption key of length 256 bit which has a keyspace of 2^{256} is used in the proposed method. Therefore, the proposed method has a strong resistance to brute force attacks.

(iii) Key sensitivity analysis

An ideal cryptosystem should be sensitive to the input encryption key provided into the system. This sensitivity is addressed with respect to two aspects:

a) The difference in cipher images C1, C2 when the same plain image is encrypted with keys K1and K2, provided there should be only slight difference between the keys K1and K2.

b) The difference in deciphered images D1, D2 when the same cipher text is decrypted using keys K1 and K2, provided there should be only slight difference between the keys K1and K2.

Fig. 5. shows the key sensitivity of the proposed algorithm with respect to encryption and decryption.

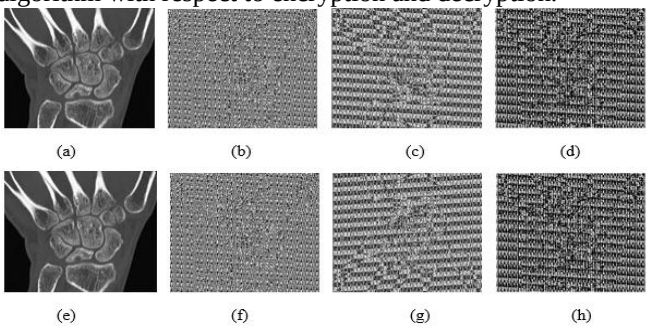
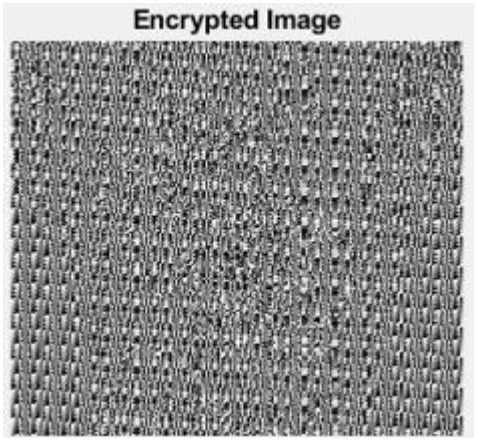


Fig 5 (a) Original Image (b)Cipher image C1 using K1 (c)Cipher image C2 using K2 (d) Difference Image [C1 – C2]

Fig 5 (e) Reconstructed Image (f) Deciphered image D1 using K1 (g) Deciphered image D2 using K2 (h) Difference Image [D1 – D2]

(iv) Histogram analysis

The manner by which the pixels are scattered in a picture can be found by performing histogram examination. Fig 6 illustrates the cipher image histograms from the encrypted image obtained after AES encryption of the sample medical image. A secure encryption method gives a uniformly distributed histogram for the cipher image. From the results it is clear that the histogram of the encrypted image is uniform such that the no information about the original image can be breached.



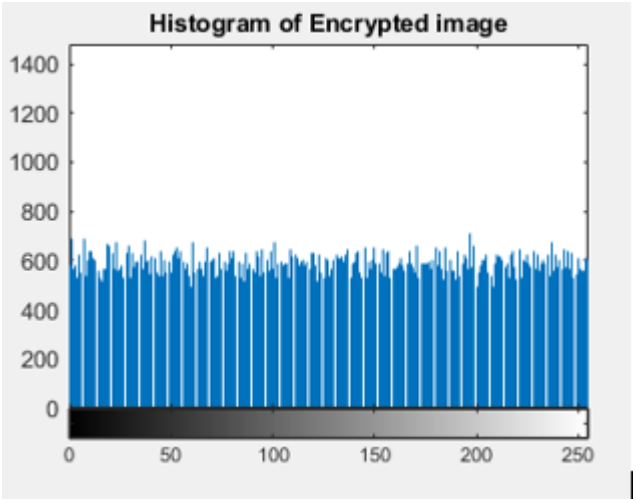


Fig. 6. Histogram Analysis of Encrypted image obtained after AES

V. CONCLUSION

In this paper, an efficient method for securely storing and retrieving medical images using AES and n-out-of-n visual cryptography is proposed. The primary objective of image encryption is to transfer an image securely over a connected malicious network so that no unauthorized user should be able to decrypt the image. In relation to medical images, the quality of the reconstructed image should be maintained for proper diagnosis. The process mentioned in this paper is tested with different parameters that ensures security and perfect restoration of the image. The authenticity of encrypted image is analyzed using keyspace analysis and the confidentiality of the generated shares are tested using key sensitivity analysis. The image quality is measured using various quality matrices. The combined effect of AES and visual cryptography makes the proposed algorithm is much more secure and resistant to external attacks. As a future work the time complexity taken for the completion of entire process can be reduced.

REFERENCES

1. M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptology EUROCRYPT, 1994, Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12
2. Rizwan Shaikh Sinhgad , Shreyas Siddh Sinhgad ,Tushar Ravekar ,Sanket Sugaonkar Sinhgad, “Visual Cryptography Survey”, International Journal of Computer Applications (0975 – 8887) Volume 134 – No.2, January 2016
3. Aparna Lanjekar, Apurva K. Thakur, Yaminee Koli , Jayashree Katti ,” Electronic Medical Reports Security in Cloud Storage Environment based on Visual Cryptography”, International Journal of Computer Applications (0975 – 8887) Volume 179 – No.6, December 2017
4. Santosh Kumar and R. H. Goudar,” Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey”, International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012
5. Fatma E.-Z. A. Elgamal, Noha A. Hikal, F.E.Z. Abou-Chadi, “Secure Medical Images Sharing over Cloud Computing environment”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 5, 2013
6. A.M. Vengadapurvaja, G. Nisha, R. Aarthy, N. Sasikaladevi,” An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security”, 7th International Conference on Advances in Computing & Communications, ICACC-2017, 2224 August 2017, Cochin, India

7. El Maraghy M, Hesham S and Abd El Ghany M.A, "Real-time Efficient FPGA Implementation of AES Algorithm", IEEE International SOC Conference (SOCC), page 203-208, Sept 2013.
8. M.Sambasiva Reddy and Mr.Y.Amar Babu, "Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, page 3341-3347, July 2013.
9. Sneha Ghoradkar and Aparna Shinde," Review on Image Encryption and Decryption using AES Algorithm", International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Advanced Communication Technologies (NCETACT-2015), 2015
10. Dr. S. Saravana Kumar, Charan R, Manikandan S, Suresh, Thennarasu B M, "Secure Visual Cryptography for Medical Image using Modified Cuckoo Search", International Journal of Pure and Applied Mathematics,Volume 119 No. 7 2018, 757-763
11. Quist-Aphetsi Kester, "A Visual Cryptographic Encryption Technique for Securing Medical Images", International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June (2013)
12. Mrs. A. Vinodhini, M. Premanand, M. Natarajan, "Visual Cryptography Using Two Factor Biometric System for Trust worthy Authentication", International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 1 ISSN 2250-3153.
13. P.Saranya, Dr.M.Vanitha," User Authorization with Encrypted Visual Cryptography Using High Definition Images", International Journal of Pure and Applied Mathematics,Volume 118 No. 8 2018, 429-433
14. Pei-Ling Chiu, Kai-Hui Lee, "An XOR-based Progressive Visual Cryptography with Meaningful Shares", IEEE International Conference on Computer Communication and the Internet (ICCCI), 2016
15. K. Brindha, N. Jeyanthi," Secured Document Sharing Using Visual Cryptography in Cloud Data Storage", Bulgarian academy of sciences cybernetics and information technologies, Volume 15, No 4 ,2015
16. Mbarek Marvan, Ali kartit, Hassan Ouahmane,"Protecting Medical Images In Cloud Using Visual Cryptography Scheme", International Conference of Cloud Computing Technologies and Applications (CloudTech) , 2017
17. Priyanka.K, Mrs.V.Mercy Rajaselvi M.E, "secured document search and retrieval using visual cryptography scheme in cloud environment", International Journal of Computer Technology & Applications,Vol 7(3),458-464,2016
18. Vandana Purushothaman, Sreela Sreedhar, "An improved secret sharing using xor-based visual cryptography", Online International Conference on Green Engineering and Technologies (IC-GET), 16864747,2016
19. R. Sathishkumar and Gnanou Florence Sudha, "Authenticated Color Extended Visual Cryptography with Perfect Reconstruction", International Conference on Communication and Signal Processing, 2017.
20. G. Preethi and N.P.Gopalan," Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 13, Number 6 (2018) pp. 3861-3866,2018.
21. Siddhant Bansal and Garima Mehta,"Comparative Analysis of joint encryption and watermarking Algorithms for security of Biomedical Images", 7th InternationalConference on Cloud Computing,Data Science & Engineering – Confluence, 609978-1-5090-3519-9,2017
22. Ming YANG, et al, "Secure Patient Information and Privacy in Medical Imaging", systemics, cybernetics and informatics, volume 8 - number 3 -, year 2010
23. Kalaivani Pachiappan, Dr. Sabari Annaji, Nithya Jayakumar, "Security in Medical Images using enhanced Visual Secret Sharing Scheme", International Journal of Scientific Engineering and Technology Research, Volume.03, IssueNo.09, May-2014, Pages: 1642-1645
24. Hare Ram Sah and G. Gunasekaran, "Preserving Data Privacy with Record Retrieval using Visual Cryptography and Encryption Techniques", Indian Journal of Science and Technology, Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/88703, August 2016
25. Paolo D'Arco, Roberto De Prisco," Visual Cryptography Models, Issues, Applications and New Directions", Published in SECITC 2016, DOI:10.1007/978-3-319-47238-6_2.

AUTHORS PROFILE

Bincy Jolly, is currently pursuing MCA from CHRIST (Deemed to be University), Bengaluru. Karnataka, India. She has completed her BCA degree from University of Kerala, Kerala, India. Research interests includes image processing, biomedical record management and network security.

Dr. Senthilnathan T, is currently working as Associate Professor in the Department of Computer Science at Christ University, Bengaluru, Karnataka, India. He has completed his Ph.D in Computer Science and Engineering in the area of Distributed Systems at Anna University, Chennai. He has more than 19 years of teaching and research experience. He has guided a number of research-oriented as well as application oriented projects which include Cloud Computing, Healthcare record management and IoT. His research interest includes Internet of Things, Security in Distributed System, Applications of Deep Learning in Health care analytics.