Secure Sharing of Documents using Image Encryption and Key Image

N.Archana, S.Manogna, Mohammed Ali Hussain, Sk. Razia

Abstract: *This Paper Presents Two Strategies For Encryption And Decryption Of Pictures Utilizing Xor Activity. The First Picture Is Encoded By The Key Picture Utilizing The Xor Activity And The Decoding Procedure Likewise Utilizes A Similar Key Picture With Xor Activity Is Done In The Primary Technique. In The Second Strategy One Of The Bit Planes, Rgb Technique, Filter Strategy For The Key Picture Is Utilized For Encoding The First Picture And Rearranging Is Accomplished For Getting The Scrambled Picture. This Technique Additionally Utilizes Xor Activity The Two Strategies Utilize A Picture Of A Similar Size As The Key For Scrambling The First Picture. Trials Have Demonstrated That The Two Calculations Are Appropriate For 2d Just As 3d Pictures. In The Matlab Condition, These Calculations Are Actualized And Tried On Different Pictures That Have Indicated Great Outcomes. For Scrambling Different Pictures These Strategies Are Likewise Utilized.*

Keywords: ***Image Encryption, Image Decryption, Bit Plane, Rgb, Scan Xor Activity, Key Picture.***

I. INTRODUCTION

In this era of computing, everything is online, this poses a major threat to data. Another important aspect is that all scanned documents will be in the image format. This makes the security of images a prime task. Though a conventional approach, today also encryption is considered to be the best way to secure the data, whether text or image.

Taking this into account we have proposed an Image Key Based Encryption(IKBE), which ensures an end to end security, free from attacks and devoid of all key-related issues. In the proposed method we have a picture as key for scrambling another picture. Numerous methods for encryption are as of now accessible utilizing bedlam based, hash capacity, and recurrence based techniques. In the existing symmetric encryption techniques key generation, key processing, and key management are some major activities. These key related activities place extra load on the overall time taken for encryption and decryption.

The other disadvantage is the management of the keys and their storage. If some third party is involved in managing the keys, there is a threat to security and confidentiality.

A novel way of encrypting an image using another image as a key image is proposed in this paper. Earlier an image was used for generating a key from it but in the present work whole image is used as a key. The major advantage of this is the key size that will be achieved. If the image selected as the key is of size 128 x 128 then the key size will be 214, similarly, if the image size is 256 x 256 then the key size will be 216, likewise with the expansion in the size of the key picture, the key size will increment proportionately.

II. RELATED WORK

The security of computerized pictures has become a significant worry because of the advancement of the Internet. The pictures which are having security has pulled in more consideration as of late, and a wide range of picture encryption techniques have been proposed for Image encryption techniques using a key image generated from other images as a bitplane or edge map, which is suitable for encrypting multimedia and images, was proposed [Zhou et al 2009]

This method is suitable for wireless and mobile applications also. Two lossless image encryption algorithms are proposed using bitplane and edge map. The performance and cryptanalysis of these algorithms prove the robustness of these methods.

Asymmetric key encryption based on pixel property separation was proposed [Iyer et al 2009], which works on the pixels disturbing the semantics of the image. This method is suitable for wireless and mobile applications also. Two lossless image encryption algorithms are proposed using bitplane and edge map. The performance and cryptanalysis of these algorithms prove the robustness of these methods.

To secure data stored on the cloud and other data centers, it should be encrypted. A hybrid method of digital image encryption based on asymmetric encryption and visual cryptographic encryption is proposed [Kester et al 2013].]. The key used in this encryption technique is a public key and the algorithm used is a public key exchange algorithm, which is suitable for secure and insecure communication networks.

III. INVENTION AND ITS IMPLEMENTATION USING TEXT AND DIAGRAMS

Nowadays, transactions are done online and scanned documents (images) need to be submitted by the clients to merchants or in another scenario two friends need to share some photographs (images), in any case, the security of the documents is a major concern. In the proposed method Image Key Based Encryption(IKBE) an image has used as a key, which can be any personal images or images publically available.

Manuscript published on November 30, 2019.
* Correspondence Author

N.Archana*, B.Tech, Dept. Of Ecm, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., A.P., India.

S.Manogna, B.Tech, Dept. Of Ecm, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., A.P., India.

Dr.Md Ali Hussain, Professor, Dept. Of Ecm, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., A.P., India.

Dr. Sk. Razia, Assoc.Professor, Dept. Of Cse, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., A.P., India.

Retrieval Number: D9724118419/2019©BEIESP
DOI:10.35940/ijrte.D9724.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

From a security point of view, every key will be used only once. A Sender(S) who wants to send a document (image)(I) to the Receiver(R) in an encrypted form uses another image as a key (K) for encryption. The same key(K) is used by the receiver for Decryption. Earlier image was used as a source for generating the key but here we are using an image itself as key.

Sender : $C = E(O,K)$
Receiver : $O = D(C,K)$

Where E is Encryption Method, O is the Original Image, K is key Image, C is the Encrypted Image and D is the Decryption Method.

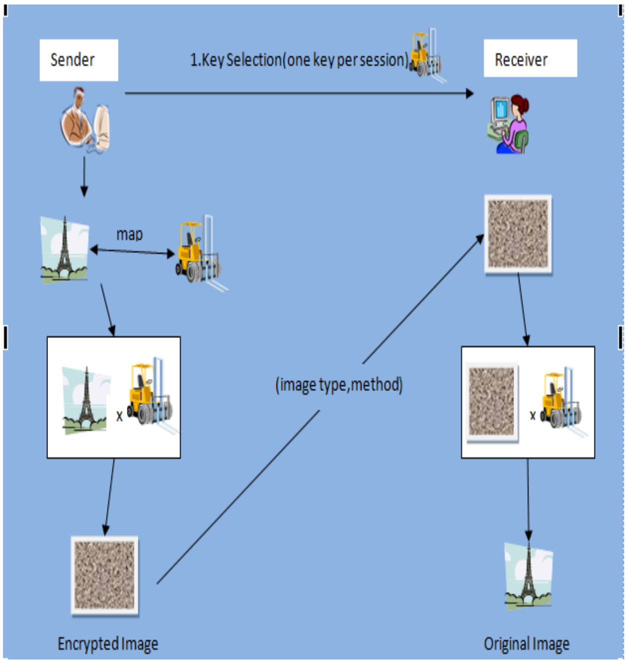


Figure 1: Procedure for Secure Sharing of the Image Documents using image Key Based Encryption(IKBE)

A.Key Selection

A one time key, which will be an image, should be decided by the sender and receiver for a particular session. Any image only available with the sender and receiver or any commonly available image on the internet can also be used. This may not pose any threat as it is going to be used only once.

B. Size Mapping

The size of the picture to be scrambled and the size of the key ought to be mapped. The image to be encrypted and the key is chosen should be of the same size. If the images differ in their sizes then extension or resizing of the images should be done.

3.1 ENCRYPTION METHOD SELECTION

After selecting the key and size mapping, the original image should be encrypted using the key image. This can be done in three different ways:

- BITPLANE METHOD
- RGB Method
- SCAN Method

3.1.1 Bitplane Method

This method is applied by splitting the images into their bitplanes.

Algorithm 1:

Step 1: Read the image of 8 bits/pixel it will have 8 bitplanes.

Step 2: The bitplanes of the original image will be combined with the bitplanes of the key image randomly using xor operation.

Step 3: The bitplanes of the original image can be combined with the bitplanes of the key image.

Step 4: 1-5 Combination: 1stbitplane of the original image with 2ndbitplane of the key image and so on.

Step5: 1-8 Combination: 1stbitplane of the original image with 8th bitplane of the key image and 2nd with 7th and so on. This method is suitable for both gray and color images

Algorithm 2: For Decryption using, Key image is combined with the original image with XOR operation

Step 1: The receiver reads the Encrypted Image.

Step 2: Take the key image which was used for encryption by the sender at the sending.

Step 3: Convert key image and encrypted image to gray image in bitplane technique.

Step 4: A key image pixel by pixel is encrypted by XOR operation is to be performed

Step 5: The original image is the resultant image

XOR Operation

On the basis of the sequence selected XOR operation will be performed between the bitplanes of the original image and the key image.

$$E8 = I1 \oplus K8,\ E7 = I2 \oplus K7 \ \ldots\ldots$$

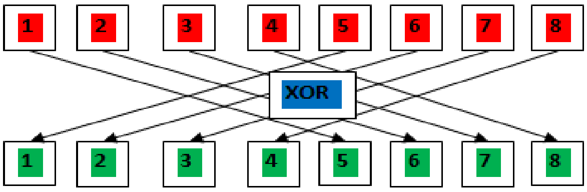


Figure 2: BitplaneProcedure

3.1.2 RGB Method

This is method is suitable for color images.

Algorithm 1:

Step1: In this method, the RGB components of the original image are combined with the RGB components of the Key image.
Step2: Using xor operation and further to increase the confusion –diffusion modulus operation is performed on the resultant pixels.
Algorithm 2: For Decryption using, Key image is combined with the original image with XOR operation

Step 1: The receiver reads the Encrypted Image.

Step 2: Take the key image which was used for encryption by the sender

Step 3: A key image is encrypted by the XOR operation.

Step 4: The original image is the resultant image.

Remainder Calculation

Next the average of all the values of the Key Image should be calculated. Using the size of the image and average of key, the remainder p is calculated. Each value of T should be divided using p and should be replaced by the remainder.

Avg (K)

$$p = \text{Size}(I) \bmod \text{Avg}(K)$$

$$T(j)=T(j) \bmod p$$

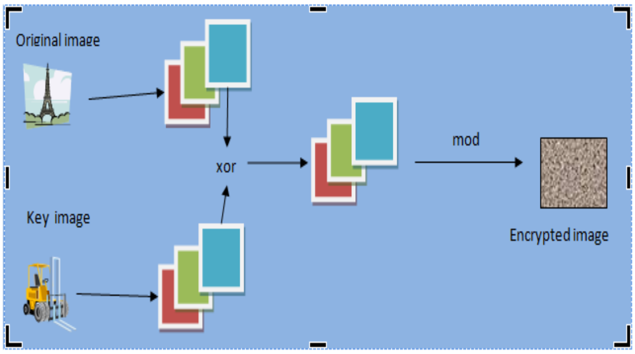


Figure 3: RGB Procedure

3.1.3 SCAN METHOD

This method is also suitable for both gray and color images.

Algorithm 1:

Step1: In this method, the original and the key images can be scanned in different ways like a spiral, orthogonal and diagonal.

Step2: And then xor operation is performed on the key image and the original image to generate the encrypted image.

Algorithm 2: For Decryption using, Key image is combined with the original image with XOR operation

Step 1: The receiver reads the Encrypted Image.

Step 2: Take the key image which was used for encryption by the sender

Step 3: A key image is encrypted by the XOR operation.

Step 4: The original image is the resultant image.

Encryption Scheme

Let the initial image be I, key image be K, S and S1 and S2 completely different scanning patterns and E is that the Encrypted Image then the method of Encoding and decoding will be diagrammatical as follows:

Encryption

$$I + S -> I1 \qquad (1)$$
$$K + S1 -> K1 \qquad (2)$$
$$E <- I1 \oplus K1 \qquad (3)$$

Decryption

$$K + S1 -> K1 \qquad (4)$$
$$D <- E \oplus K1 \qquad (5)$$
$$D + S -> I \qquad (6)$$

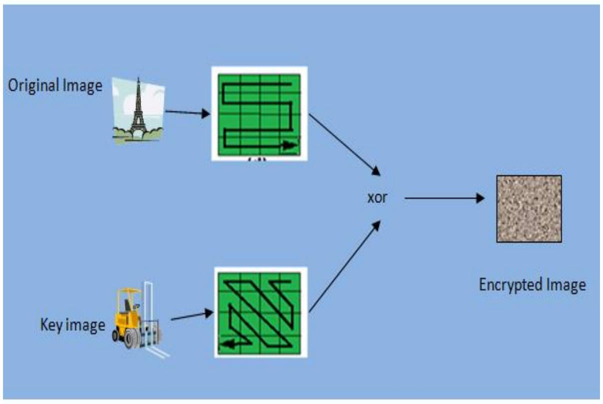


Figure 4: Scan Procedure

IV. EXPERIMENTAL RESULTS

1)The experimental results using the Bitplane and Scan Method for Gray images Lena, House, and Pepper and car3 is taken as a key image, all images taken from CVG(Computer Vision Group) Database is shown in table1.

2) The experimental results using the Bitplane, RGB and Scan Method for Color images Lena, House, and Pepper, ship, tulips, and balloon are taken as key images, all images taken from CVG(Computer Vision Group) Database.

Retrieval Number: D9724118419/2019©BEIESP
DOI:10.35940/ijrte.D9724.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

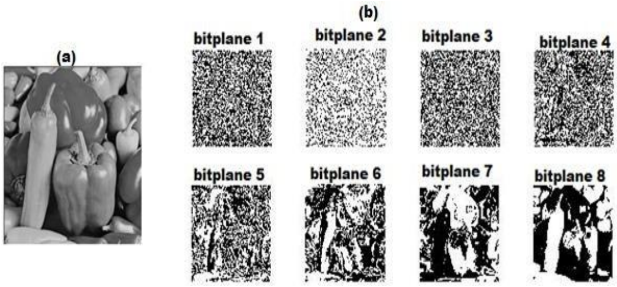


Figure 5: (a) Image 'peppers.pgm',(b) 8 bitplanes of the image 'peppers.pgm'

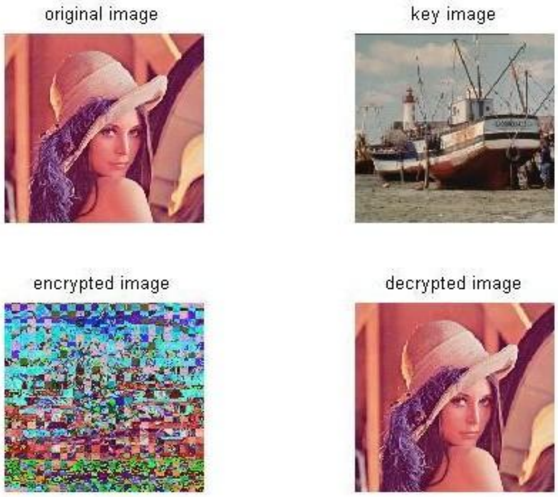


Figure 6: Showing the Encryption of Lena Image (256×256x2)

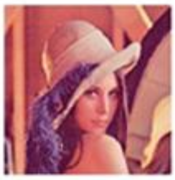
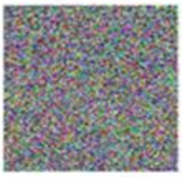
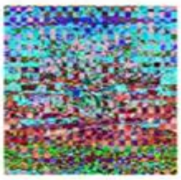
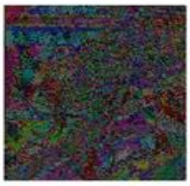
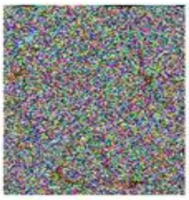
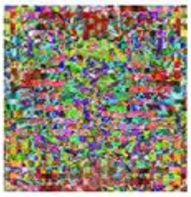
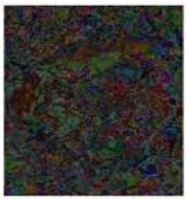
Original Image	Key Image	Encrypted Image Bitplane Method	Encrypted Image Scan Method	Encrypted Image RGB Method
				
				

Table 1:Original image, key image and encrypted images using Bitplane Method, RGB Methods and Scan method

Table 2:Entropy ofencrypted images using Bitplane Method, Scan method and Zhou's Method

Image	**Bitplane Method**	**Scan Method**	**RGB Method**
Encrypted Lena	7.9952	7.881	7.8024
Encrypted House	7.9913	7.7593	7.5614
Encrypted Peppers	7.9969	7.9611	7.6423
Average	7.9944	7.8671	7.6687

V. CONCLUSION

Image Key Based Encryption(IKBE) is where an image is used as a key for encrypting another image. Earlier an image was used as a source from which key was generated. One of the methods that use this is Zhou's method. Entropy analysis of the proposed method and Zhou's The method shows that the proposed method can achieve better encryption as compared to the existing method. This approach saves time and effort as it eliminates the key generation phase in the encryption process.

It provides faster encryption. It also eliminates the need for the third party for key management, as every key is used only once. The proposed methods have a good key space as the whole image is used as key. These methods are less complex as compared to existing methods. Overall the proposed methods show a better performance than existing methods as can be seen from the NPCR and UACI values.

VI. FUTURE ENHANCEMENTS

He work presented in this thesis can further be extended in the following directions:

A. Efficient ciphers

The ciphers proposed are good but there are some proven techniques available in encryption which is not considered in the present work, techniques like hashing and chaos can be used for developing some efficient ciphers.

B. Suitable keys

Different images can be tested for their suitability as keys. There are possibilities that some particular type of images with difference in texture and contour may give better results.

C. Compression

In the proposed ciphers the original image and encrypted image will be of same size but as far as transmission is concerned if compression is applied it will result in faster transmission.

REFERENCES

1. Data Encryption Standard (DES), Federal Informat -ion Processing Standards Publication, 46-3, 1999.
2. Advanced Encryption Standards (AES), Federal Information Processing Standards Publication, 197, 2001.
3. YicongZhou,WeijiaCao,C.L.Philip Chen,Image encryption using binary bitplane, Signal Processing 100(2014)197–207.
4. Zhi-Liang Zhu, Wei Zhang, Kwok-Wo Wong, Hai Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation”, Information Sciences 181 1171–1186, Elsevier, 2010.
5. X.Zhang, Y.Cao.A Novel Chaotic Map and an I Improved Chaos-Based Image Encryption Scheme,Hindawi Publishing Corporation, The Scientific World Journal, 2014.
6. Zhou Y, Panetta K, Agaian S. Image encryption using the binary key image. IEEE International Conference on Systems, Man and Cybernetics; San Antonio, TX. 2009 Oct 11-14: p. 4569–74.
7. H.Yuan and L.Jiang, Image Scrambling based on Spiral Filling of Bits.International Journal of Signal Processing, Image Processing and PatternRecognition. 2015.8(3), pp.225-234.
8. Q.A.Kester, A cryptographic Image Encryption technique based on the RGB PIXEL shuffling. International Journal of Advanced Research in Computer Engineering & Technology .2013,2(2):pp. 848-854.
9. Image encryption and image decryption apparatus and method, Hideaki Ishii, Taizo Anan, Kensuke Kuraki, ShoheiNakagata, US 8588414 B2, Fujitsu Limited, Nov 19, 2013.
10. Image encryption/decryption system, Kensuke Kuraki, Hiroji Fukui, Taizo Anan, ShoheiNakagata,US 20080298596 A1, Fujitsu Limited, Dec 4, 2008.
11. Shrija Somaraj, Mohammed Ali Hussain, Securing Medical Images by Image Encryption using Key Image, International Journal of ComputeApplications (0975 – 8887) Volume 104 – No.3, October 2014.
12. RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication,Musbah J. Aqel1 *, Ziad ALQadi2, Ammar Ahmed Abdullah3, July 2018.