ISSN: 0975-766X
CODEN: IJPTFI

Available Online through ***Research Article***
www.ijptonline.com

SECURE AND NOVEL METHODS OF IMAGE ENCRYPTION USING AN IMAGE AS KEY

Shrija Somaraj[1*], Mohammed Ali Hussain[2]

[1*]Research and Development Centre, Bharathiar University, Coimbatore and Assoc.Prof., Dept. of Computer Applicaions, GIET, Rajahmundry, A.P., India, 533296.

[2]Dept.of Computer Science and Engineering ,Andhra Loyola Institute of Engineering and Technology, Vijayawada, A.P., India.

Email: shrija@giet.ac.in

Received on: 11-03-2017 *Accepted on: 05-04-2017*

Abstract

In this paper three methods for image encryption are proposed. The proposed methods of image encryption are Key Bitplane Encryption, Key Scan Encryption and Key RGB Displacement Encryption. All these methods use a common concept of using an image as key for encrypting an image. These algorithms are analyzed for gray as well as color images and for images of different sizes. The three methods proposed in the paper are analyzed for common types of attacks and brute force attacks. The comparative study using statistical techniques is provided for all the methods. Implementation of the methods is done in Matlab and the test images are taken from Computer Vision Group Database.

Keyword: Bitplanes, Image encryption, Image decryption, Pixel displacement, SCAN Approach.

Introduction

Development of networking, internet, cloud and social networking sites have put forth new challenges towards security of data and information. This led to simultaneous development of methods for security and protection of data and information. Conventional methods like Data Encryption Standard (DES) and Advanced Encryption Standard(AES) are good for textual data but not suitable for Multimedia data [1,2].Moreover these methods incur large computational cost and exhibit poor error resilience. The Conventional Methods of encryption are not suitable for image and video data, as the characteristics of text and image differ with respect to size, texture, contour and many more features. Image encryption algorithms are specifically designed for images. Image Encryption based on symmetric as well as asymmetric methods has been developed. The symmetric encryption algorithms also known as secret key algorithms use only one key for encryption and decryption. On the contrary asymmetric algorithms or public key encryption uses two keys- private and public keys for encryption and decryption purpose.

Many novel techniques are proposed based on Chaos, Hash and Pixel Permutations. An image encryption technique based on chaos approach is proposed where for each 16 pixel block a secret key is used and two chaotic logistic maps are used along with a secret key of 80-bit, this secures the image against common attacks [3]. A Chaos based algorithm where two chaotic logistic maps were used has shown better performance[4]. Statistical analysis for chaos based algorithms is also suggested[5]. Some other methods based on chaos and chaotic maps are also proposed[6]. An Image encryption technique for grayscale image using Arnold cat map and Chen's chaotic system was presented[7]. Another image encryption algorithm based on chaos where RGB components of a colour image were made to have an impact over each other have show good results[8].

A method for image encryption was proposed in frequency domain using the concept of discrete Fourier transform along with phase manipulation and differential evolution [9] . A novel algorithm using hash function SHA-512 and hash concept was proposed for image encryption which got commendable results[10]. An Image encryption technique using AES algorithm is suggested with enhancement by addition of a key stream generator[11]. A partial encryption technique was introduced which resulted in a significant reduction in encryption and decryption time as it used to encrypt only part of the compressed data[12].

An image encryption for bit-level permutation and diffusion using Arnold cat map and logistic map was proposed, which is an effective way of permutation for changing position as well as the value of pixels[13]. Some low complexity scanning strategies for bitplanes was proposed consisting of some theoretical and practical mechanisms using rate-distortion theory [14]. A novel encryption technique bitplanecrypt method where another image is used for extracting the key and used for encrypting the original image is proposed[15]. An improvement of the technique is proposed, the decomcrypt algorithm which shows better performance than the bitplanecrypt algorithm[16]. Some methods are proposed using RGB pixel displacement with AES and pixel shuffling, which have shown good results [17,18]. Scrambling is another area which is emerging as one of the effective ways of encryption but may not be providing high level security[19,20]. Some methods of encryption based on Scanning of Images were introduced for multimedia based applications which are suitable for encryption, as well as information hiding and compression also [21,22,23]. Many new methods using and image as key is proposed which has shown commendable results[24,25,26,27]. All the above methods has some security issues and moreover the key space, key processing and key management are some of the issues. In the proposed methods an image is used as key, as it it will improve the key space or key size, which in turn increases the quality and security of encryption . The proposed work is

applicable for gray scale images as well as color images. In the proposed algorithms a key of size M × N is used for a gray image of size M × N and key of size M × N ×3 is used for a color image of six x M x N x 3. Statistical and security analysis have been conducted using images of different sizes and textures. In this paper we are proposing three methods which are symmetric algorithms, these methods use a single key for encryption and decryption. In Section 2 we have discussed about the methods Key Bitplane Encyption, Key RGB Displacement Encryption and Key Scan Encryption. Section 3 deals with Experimental results of the three methods. Section 4 deals with the Statistical Analysis of the proposed methods and existing methods. In the conclusion we have summarized the results.

Methodology

The Methods for encrypting an image are proposed using the basic concept as an image being used as key. All the proposed methods use an image for encrypting a given image. The image used as key may or may not be of same size as the plain image. The three proposed methods are Key Bitplane Encryption, Key Scan Encryption and Key RGB Displacement Encryption.

Key bitplane encryption

In this method the images, the plain and the key are separated into bitplanes. An 8 bit/pixel image will have 8 bitplanes ,if plane image is I then the bitplanes will be $I_0,I_1 \ldots I_8$ and if K is key image then the bitplanes will be $K_0,K_1 \ldots K_8$. The Xor operation can be performed between the bitplanes of the key and the plain image. The sequence may be randomly decided

$$E_8 = I_1 \oplus K_8$$

$$E_7 = I_2 \oplus K_7$$

$$E_1 = I_5 \oplus K_1$$

1) Algorithm Key Bitplane Encyption (KBE)

1: Take the image I to be encrypted (Gray or Color Image).

2: Calculate the size of the above Image.

```
[m n]=size(I)
```

3: Take other image to be used as key image of same size or different size.

4: If Key image is different size then resize it according to the size of the image to be encrypted.

5: Separate the key image into bitplanes. $K_0,K_1 \ldots K_8$

6: Separate the original image into bitplanes. $I_0,I_1 \ldots I_8$

7: Select a sequence for the xor operation

$E_8 = I_1 \oplus K_8$, $E_7 = I_2 \oplus K_7$ .....

8: The selected/all bit planes of original image should be xored with the bit planes of key image. This should be done for all 2 D components if the image is a color image.

9: Resultant image is encrypted image.

Key RGB Displacement Encryption

This method is specifically designed for Color images, where the three components Red, Green and Blue are separated for plain as well as key image. Perform xor operation on each component of original and key image and store in a vector T.

Then calculate average of Key Image. Next find remainder p using average and size of the image. Then calculate remainder for each value of T using p and store as a 3 D array. This 3D Array is the resultant encrypted image.

1) Algorithm Key RGB Displacement Encryption (KRDE)

1: Take the Color image I to be encrypted.

2: Calculate the size of the above Image.

[m n w]= size (I)

3: Take other image to be used as key image K of same size or different size.

4: If Key image is different size then resize it according to the size of the image to be encrypted.

5: Separate three components of I as R_i,G_i,B_i.

6: Separate three components of K as R_k,G_k,B_k

7: Perform

$R_e = R_i \oplus R_k$. Store in in vector T(1 to Size of Re)

$G_e = G_i \oplus G_k$. Store in in vector T(Size of Re+1 to Size of Re + Size of Ge)

$B_e = B_i \oplus B_k$. Store in in vector T (Size of Ge+1 to Size of Re + Size of Ge +Size of Be)

8: Calculate Average of Key Image

9: Find Remainder p using Average and Size of the image.

10: Calculate remainder for each value of T using p and store as a 3 D array

11. The above 3D Array is the resultant encrypted image.

Key Scan Encryption

This method is implemented for color as well as gray image. In this method some scanning patterns are available like Spiral, Continuous Diagonal, Continuous Orthogonal, Continuous Raster which are applied on the original and key image and new transformed images are then xored for getting the encrypted image.

1) Algorithm for Key Scan Encryption

1: Take the image I to be encrypted (Gray or Color Image).

2: Calculate the size of the above Image.

[m n]=size(I)

3: Take other image to be used as key image of same size or different size.

4: If Key image is different size then resize it according to the size of the image to be encrypted.

5: Select a Scanning Pattern from the four basic patterns for the Image I

Scanning Pattern(I,S)for Spiral

Scanning Pattern(I,D)for Continuous Diagonal

Scanning Pattern(I,O)for Continuous Orthogonal

Scanning Pattern(I,C)for Continuous Raster

6: Store the generated image I1.

7: Similarly select a Scanning Pattern from the key image also

Scanning Pattern(K,S)for Spiral ….

8: Store the generated image K1.

9: XOR operation can be performed on the images generated in Step 6 and Step 8 to generate image E1.

10: E1is the resultant encrypted image.

Experimental Results

The proposed methods are applied on different images from Computer Vision Group database(http:/decsai.ugr.es/cvg/dbimages), USC-SIPI database and Matlab. The images taken for study are of different sizes like 128x128, 256x256, 512x512 and 1024x1024 and different types general images, medical images and sar images.

Table 1 shows the results of encyption of gray images using the proposed methods KBE and KSE . Table 2 shows the results of encyption of color images using the proposed methods KBE,KSE and KRDE. The images are taken

from CVG database and they are general images of 256x256 size. The test images are gray images of 256 x 256 size shown in the Table 1 are 'Lena.ppm','peppers.ppm','4.1.05.tif' as original images and 'car3.pgm' and 'tulips.ppm' as key images.

The test images are color images of 256 x 256 size shown in the Table 2 are 'Lena.ppm','peppers.ppm','4.1.05.tif' as original images and 'barche.pbm', 'pallon.pgm' and 'tulips.ppm' as key images.

Table 1. Showing Original test gray images, key images and corresponding encrypted images using KBE and KSE methods.

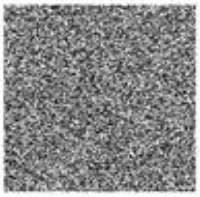
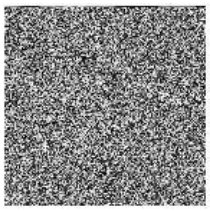
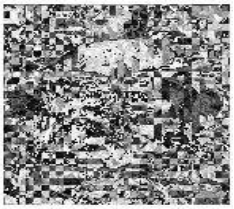
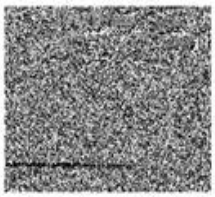
Original Image	Key Image	Encrypted Image (KBE)	Encrypted Image (KSE)
			
			
			

Table 2. Showing Original test gray images,key images and corresponding encrypted images using KBE , KSE and KRDE methods.

Original Image	Key Image	Encrypted Image (KBE)	Encrypted Image (KSE)	Encrypted Image (KRDE)
				

Statistical Analysis

Statistical Analysis of the encrypted images is done using Mean value analysis, correlation analysis, entropy, encryption speed and encryption quality.

1. Mean Value Analysis

Mean Value Analysis is done for observing the distribution of pixel values in an image. In general mean value of pixels vary a lot along the width of a plain image ,while mean values do not vary in an encrypted image .The encrypted image show a moreover uniform distribution of mean values.

Figure 1 shows Mean Value Analysis of Lena image in red color which is encrypted using car3.pgm .The images are taken from Computer Vision Group database. The encrypted images using KBE and SBE are shown in blue colors in Figure respectively. It can be seen in the plots that mean value plot of encrypted image is closer and uniformly distributed.

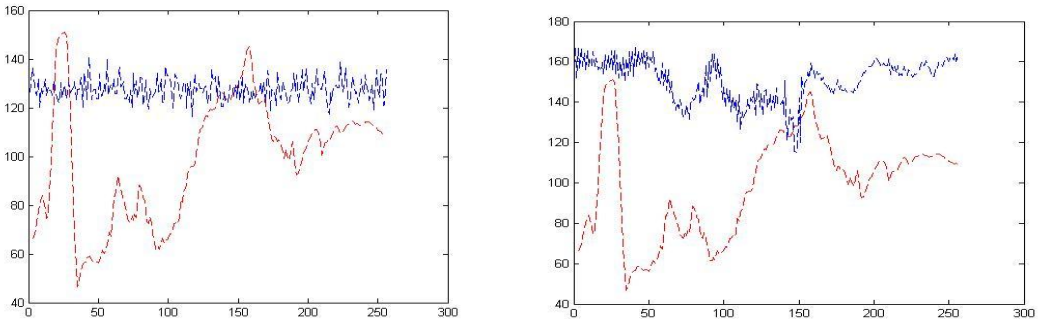


Figure 1. Showing Mean Values using KBE and KSE for Lena gray image.

2. Encryption Quality

Encryption Quality is another measure to evaluate the rate of change of pixel values that occurs during encryption between the original image and the cipher image.

It can be calculated as follows:

$$EQ = \frac{\sum_{i=0}^{255} Oi - Ei}{256} \quad (1)$$

Where i represents the pixel gray level , Oi represents the number of pixels having gray level value as 1 in theoriginal image and Ei represents the number of pixels having pixel gray level value as 1 in the encrypted image. The larger images have higher encryption quality value as with the increase in the size of the image the difference in number of pixels having same gray level value also increases.. The images having same size may have different encryption quality values as the content of different images vary. The encryption quality for the images in consideration using the proposed and existing methods is given in the Table 3.

Table 3. Showing Encryption Quality of test images using KBE, KSE and Zhou's Method.

Image	KBE	KSE	Zhou
Lena	151.1328	216.1406	173.7578
House	204.7578	306.0156	243.4688
Peppers	158.0625	126.4844	208.6328
Average	171.3177	216.2135	208.6198

3. Encryption Speed

The Encryption Speed is another measure for analyzing the performance of an algorithm . Encryption Speed can be calculated by finding number of pixels encrypted per unit of time of the given image. The images taken for study are of different sizes like 128x128, 256x256, 512x512 and 1024x1024 and different types general images, medical images and sar images. using Matlab-7 on Intel Core 2 Duo Processor @ 2.00 GHz and Windows 8.1 Operating System. Table 4 shows the encryption speed for the test images using KBE, KSE and Zhou's Method.

Table 4. Showing Encryption Speed of test images in bytes/sec using KBE, KSE and Zhou's Method.

Image	KBE	KSE	Zhou
Lena	113384	537180	35890
House	104190	468114	62492
Peppers	98402	458293	66846
Average	105325	487862	55076

4. Entropy

Entropy is a measure of uncertainty. In can be calculated using the given formula as follows:

$$E(X) = -\sum_{i=0}^{255} p(i_j)\log_2 p(i_j) \quad (2)$$

Where X is an Image, p (i_j) is the probability density function of the occurrence of the symbol i_j in the image. The entropy E(X) = 8 corresponds to the value for a truly random image and the values for well encrypted images will be around 7.9 approx. It can be seen from the Table 5, the variation of entropy values for different proposed mathods KBE, KSE and Zhou's Method.

Table 5. Showing Entropy of test images using KBE, KSE and Zhou's Method.

Image	**KBE**	**KSE**	**Zhou**
Encrypted Lena	7.9952	7.8810	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

5. Correlation Analysis

Correlation Analysis of images is done to measure the relationship between two pixels in an image. Generally adjacent pixels are closely correlated in a plain image and they are less related in an encrypted image. The correlation value for an image can be calculated using a MATLAB command, corr2(). The correlation values range from 0 to 1, where values close to 1 show high correlation and that close to 0 show less correlation. In plain images the correlation values will be closer to 1 while in encrypted image it will be closer to 0.Table 6 shows the correlation values of gray test images using the proposed methods and also comparison with other methods.

Table 6. Showing Correlation values for KBE, KSE and Zhou's Method.

	Image	Original	KBE	KSE	Zhou
Lena	Horizontal	0.9391	0.1188	-0.226	0.1492
	Vertical	0.9358	0.0074	0.1926	0.2484
	Diagonal	0.8415	-0.0555	-0.0217	0.1342
	Average	0.9054	0.0235	-0.0184	0.1772
House	Horizontal	0.6194	-0.0436	0.1066	0.0407
	Vertical	0.9622	0.0642	-0.0312	0.2653
	Diagonal	0.6378	-0.0441	-0.1297	0.0478
	Average	0.7398	-0.0078	-0.0181	0.1179
Peppers	Horizontal	0.9700	0.0022	-0.0604	0.0335
	Vertical	0.9808	0.0186	0.2511	0.0396
	Diagonal	0.8768	-0.0495	-0.0853	0.0617
	Average	0.9425	-0.0096	0.0351	0.0449
	Overall Average	0.8626	0.0020	-0.0004	0.1133

6. NPCR and UACI tests

The Number of Pixel Change Rate (NPCR) and the Unified Averaged Changing Intensity (UACI) tests are used to assess the effect of changing a single bit of plain image on the cipher image. The NPCR is used to measure rate of change in the number of pixels of the cipher image when only one bit of original image. The UACI is used to measure the average intensity of the one bit changes of cipher images. Let the two cipher images be C1 and C2 whose corresponding original images have a difference of only one pixel. Let D be a bipolar array with the same size as images C1 and C2. Then, D(i,j) is determined by C1(i,j) and C2(i,j), namely, if C1(i,j) = C2(i,j) then D(i,j) = 0, otherwise D(i,j) = 1. Table 7 and 8 show the NPCR and UACI value for test images using KBE,KSE and Zhou's Method.

NPCR is defined as

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times \frac{100\%}{M \times N} \quad (3)$$

Where $$D(i,j) = \begin{cases} 0, if\ C1(i,j) = C2(i,j) \\ 1, if\ C1(i,j) \neq C2(i,j) \end{cases}$$

UACI is defined as

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N} \quad (4)$$

Table 7. Shows the NPCR values of test images using proposed methods and existing methods.

Image	KBE	KSE	Zhou
Lena	99.6201	99.6811	97.0657
House	99.5529	99.6887	96.9330
Peppers	99.6140	99.5880	96.8155
Average	99.5956	99.6526	96.9380

Table 8: Shows the UACI values of test images using proposed methods and existing methods.

Image	KBE	KSE	Zhou
Lena	30.6456	32.5236	18.1534
House	30.6311	34.4802	16.0538
Peppers	29.1252	28.1925	14.7552
Average	30.1339	31.7321	16.3208

Conclusion

This paper proposed three methods of image encryption, namely Key Bitplane Encryption, Key Scan Encryption and Key RGB Displacement Encryption. All the three methods of encryption have used a novel concept of using an image as key for encrypting the actual image. The results of encryption and comparative study of these methods is presented in the paper. Comparative study with other existing methods is also given. These techniques have a large key space and their implementation is also simple. These methods eliminate the key management and key processing requirements and thus make the encryption process faster.

These algorithms give a commendable performance based on the mean value analysis, correlation analysis, encryption quality, encryption speed, NPCR and UACI tests. These algorithms are analyzed for gray as well as color images and for images of different sizes. These techniques can be used for secure transmission of scanned documents on the network and various other applications where security of documents in form of image files is required.

References

1. Data Encryption Standard (DES), Federal Information Processing Standards Publication, 46-3, 1999.
2. Advanced Encryption Standards (AES), Federal Information Processing Standards Publication, 197, 2001.
3. N.K. Pareek ,V. Patidar and K.K.Sud , Image encryption using chaotic logistic map, Image and Vision Computing .2006: pp.926–934.
4. I.A.Ismail, M.Amin, H.Diab. A digital image encryption algorithm based on composition of two chaotic logistic maps. Proceeding 27th IEEE Int'l Conf Signal Processing. 2011:pp. 733–739.
5. D.LMancilla ,J.H.G Lopez, R.J.Reategui, R.Chiu,E.V.Rauda ,C.E.C.Hernandez, G.H.Cuellar. Statistical analysis of imaging encryption using chaos. Latest Trends in Circuits, Systems, Signal Processing and Automatic Control. CISSPA. 2009: p. 86-90
6. X.Zhang, Y.Cao**.** A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme, Hindawi Publishing Corporation, The Scientific World Journal, 2014.
7. Z.H.Guan, F.Huang , W.Guan. Chaos-Based Image Encryption Algorithm. In Physics Letters A ,2005, 346(1–3):pp.153–157
8. X.Wang ,L.Teng,X.Qin. A novel colour image encryption algorithm based on chaos. Signal Process. 2012, 92(4):pp.1101–1108.

9. I.S.I Abuhaiba , M. A. S Hassan, Image Encryption using Differential Evolution Approach in Frequency domain, Signal & Image Processing: An International Journal (SIPIJ) ,2011,2(1): pp. 51-69
10. S.M.Seyedzade, R.E.Atani,S.Mirzakuchaki. A Novel Image Encryption Algorithm Based on Hash Function. In 6th Iranian Conference on Machine Vision and Image Processing,2010.
11. M.Zeghid, Machhout M, Khriji L, Baganne A, Tourki R. A modified AES based algorithm for image Encryption. World Academy of Science, Engineering and Technology. 2007; 1(1):70–5.
12. Cheng H, Li X.(2000). Partial Encryption of Compressed Images and Videos. In IEEE Transactions On Signal Processing. 48(8):2439-2451
13. Zhu Z.-L.,Zhang W.,W.Wong K.,Yu H.(2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf.Sci.181(6): 1171–1186
14. Llinas F A, Marcellin M W. (2012). Scanning order strategies for bitplane image coding.In IEEE Transactions on Image Processing.21(4):1920 – 1933
15. Zhou Y, Panetta K, Agaian S. Image encryption using binary key image. IEEE International Conference on Systems, Man and Cybernetics; San Antonio, TX. 2009 Oct 11-14: p. 4569–74.
16. Yicong Zhou , WeijiaCao,C.L.PhilipChen ,Image encryption using binary bitplane, Signal Processing.2014.100:197–207
17. Q.A.Kester, L.Nana and A.C.Pascu, A novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud using AES and RGB pixel displacement. European Modelling Symposium, IEEE,2013.
18. 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
19. C.Y.Zhang, W.X.Zhang and S.W.Weng, Comparison of Two Kinds of Image Scrambling Methods Based on LSB Steganalysis, Journal of Information Hiding and Multimedia Signal Processing,2015, 6(4):666-673.
20. H.Yuan and L.Jiang, Image Scrambling based on Spiral Filling of Bits.International Journal of Signal Processing, Image Processing and Pattern Recognition.2015.8(3), pp.225-234.
21. Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani , A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR, International Journal of Signal Processing, Image Processing and Pattern Recognition ,2013,6(5) : pp.275-290

22. S.S.Maniccam and N.Bourbakis, "Image and Video encryption using SCAN Patterns",PatternRecognition, 2004,37:pp.725-757.
23. Chao Shen Chen and Rong Jian Chen, Image Encryption and Decryption using SCAN Methodology, Proc.PDCAT, IEEE,2006.
24. S.Somaraj ,M.A.Hussain. Securing medical images by image encryption using key image. International Journal of Computer Applications 2014;104(3):30–4.
25. S.Somaraj ,M.A.Hussain. Performance and Security Analysis for Image Encryption using Key Image. Indian J. of Sci and Tech. 2015:8(35)
26. S.Somaraj, M.A.Hussain. A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images, IEEE 6th International Conference on Advanced Computing (IACC) ,2016.
27. S.Somaraj, M.A.Hussain. An Image Encryption Technique Using Scan Based Approach and Image as Key, Proceedings of the First International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, 2016;507: 645-653.