Indian Journal of Science and Technology, Vol 10(4), DOI: 10.17485/ijst/2017/v10i4/110673, January 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# Image Encryption using Edge Map and Key Image

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

[1]Research and Development Centre, Bharathiar University, Coimbatore - 641046, Tamil Nadu, India; shrijamadhu@yahoo.co.in
[2]Department of Electronics and Computer Engineering, KL University, Guntur - 522502, Andhra Pradesh, India; alihussain.phd@gmail.com

## Abstract

**Objective:** An Image Encryption algorithm is proposed which uses an image as key and concept of Edge Map for Encryption. **Method/Analysis:** The proposed algorithm uses gradient operators like Sobel, Roberts, Prewitt and Canny edge detectors for generating the edge map of key image and which is used for encrypting the original image with xor operation. **Findings:** The encrypted image shows remarkable difference from the actual image which is shown in the histogram analysis and other statistical tests. **Conclusion/Applications:** The proposed algorithm achieves considerable level of encryption, which makes it suitable to be used in different applications. It is used for protection of images against various kinds of common attacks like brute force attacks.

**Keywords:** Cryptanalysis, Edge Map, Gradient Operators, Histogram Analysis, Image Encryption, Key Image

## 1. Introduction

Networking, Internet and Cloud have made everything accessible but at the same time have added complexity to the problem of security. The changes that have been brought about by technology and the Internet are indispensable. Gone are the days when only data was available as text, moreover data as image, audio, video and all sorts of multimedia have taken over the textual data. High speed networks and satellites have taken communication to a different level. Large files can be transmitted in fraction of seconds geographically anywhere in this world. The advantages obtained obviously come at a cost which is in the form of compromising privacy of the data that is being sent. Conventional solution to the problem of security is by encrypting the data[1].

Using encryption, data can be converted or transformed into a format which is unrecognizable, which makes it secure against different kinds of intentional attacks and unintentional changes. Many data encryption techniques are widely available, but the irony is that most of the techniques are suitable only for textual data. Based on the data, the technique used for protection of data varies. Image data differs from textual data, so encryption technique followed for image encryption is different from textual encryption. In recent times many new techniques have been proposed based on Fibonacci P-Codes[2], Chaotic sequences[3], Spiral Filling of bits[3] and Image Scrambling[4]. Many techniques for image encryption have been suggested using Fibonacci p-codes[2], concept based on Chaotic sequence-decomposition and reconstruction[3], another based on spiral filling of bits[4], Scrambling[5]. A method for hiding information in encrypted images is also proposed[6]. Some methods based on Chaos and Block based techniques are also suggested[7–10]. Methods using the concept of bitplane such as selectively encrypting the bitplanes and encrypting using key image by use of bitplane and edgemap are also done. These methods have shown better performance as compared to previous ones as the key space problem is not there[11–13]. This paper is also based on this concept of bitplane and edgemap which is done without the use of scrambling. In this paper we have proposed a technique which uses the gradient operators of edge detection like Sobel, Prewitt, Roberts and

*Author for correspondence

Canny, which are applied on the Image chosen as key and the generated edgemap is used for encrypting the original image. Section 2 provides an overview about gradient operators and edgemap. Section 3 gives a brief description of the proposed method. Section 4 contains the experimental results. Section 5 provides an overview of the cryptanalysis done for the proposed algorithm. Finally Section 6 contains the conclusion followed by the References.

## 2. Edge Map and Gradient Operators

The edge map of an image is generally used in image enhancement, edge detection, compression, recognition and segmentation. In the proposed algorithm we are extending its use in image encryption. An edge map of the key image is generated using the available gradient operators and threshold value for edge detection. Some of the gradient operators which are available are Sobel, Roberts, Canny and Prewit which are shown in Figure 1.

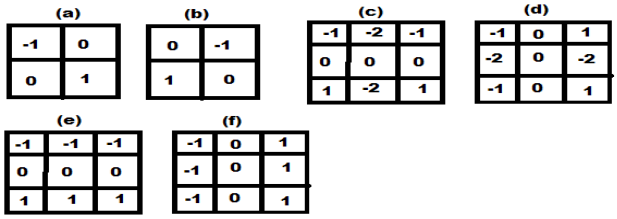


**Figure 1.** Gradient operators (a) and (b) Roberts, (c) and (d) Sobel, (e) and (f) Prewitt.

## 3. Proposed Alogorithm

The basic requirement inthe Proposed Algorithm is that the original image and the encrypted image should be of the same size. An edgemap of the key image is generated using any of the above gradient operators and by using edge() function from MATLAB. Next xor operation of all the bitplanes of the original image and edgemap of key image is done. The method followed is same for gray as well as color image with only difference that in color image for all three components red, green and blue should be done seperately. Lastly the cipher image is obtained by shuffling bitplanes of the image. The reverse procedure is followed for decryption.

Algorithm for Edge Map based Encryption (EMBE)

- Take a Plain image (Color Image or Gray Image).
- Take a Key image, find size of the key image,it should be same as the size of plain image.
- Select an edge detection gradient operator and use it to for getting the edge map of the key image.
- XOR operation should be performed of the bit planes of original image with the edge map of the key image.
- The resultant image is generated by shuffling of bitplanes in a particular sequence.
- The final image obtained is the encrypted image.

Algorithm for Edge Map Based Decryption (EMBD)

- Input is the Encrypted Image.
- The key image selected for encryption should be used for decryption also and should be of same size as the cipher image.
- Take the same edge detection gradient operator used in encryption process and use it to for getting the edge map of the key image.
- XOR operation of all bit planes of the cipher image should be done with the edge map generated from the image used as key.
- The decrypted image can be obtained by reshuffling.
- Resultant image is the plain original image.


**Figure 2.** (a) Key image tulips.ppm (b) key image tulips.pgm.

## 4. Experimental Results

The proposed algorithms EMBE and EMBD are implemented in MATLAB 7.0 and the images used are from the database[14]. Figure 2 shows the key images used for encrypting gray and color images, the images are tulips.pgm (gray, 256x256) and tulips.ppm (color, 256x256). Figure 3 shows the encryption reults of gray images while Figure 4 shows for color images, both the figures shows the original images as (a),the corresponding encrypted images as (c), histograms of original images is (b) and histograms of encrypted images is (d).

## 5. Cryptanalysis

The major aspect of encryption is security, where the encrypted objects as well as the encryption algorithms should be secured from different kinds of attacks. In the proposed method as an image is used as key it is not easy for the unauthorized persons to retrieve the key or the encrypted information.

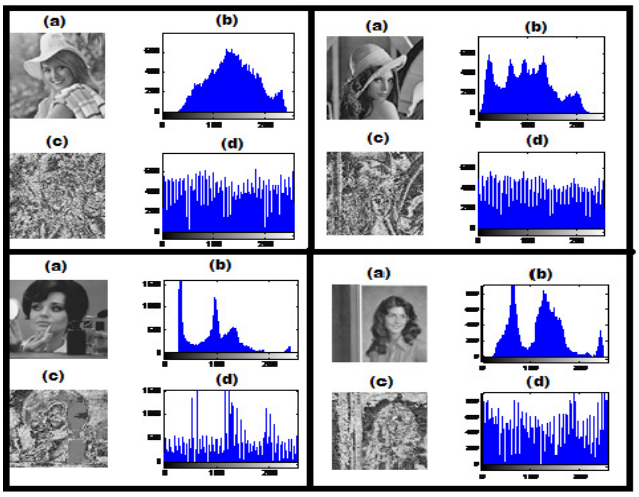


**Figure 3.** 4 blocks with gray image encryption – each block (a, b) original image and its histogram, (c, d) encrypted image and its histogram.

### 5.1 Brute Force Attack

In this type of attack, the attacker usually tries to guess the keys and all combination of keys which are possible and performs a kind of exhaustive search using them. For getting any fruitful result in this type of attack the key space used in the algorithm should be limited and moreover the attacker should also know the algorithm used for encryption, both of which is not possible in this method as key size is same as the size of original image and knowing the algorithm alone will not work. Moreover the users can select each time a different image as key for different transactions.

### 5.2 Ciphertext Related Attacks

In this type of attack, the attacker usually tries to retrieve the key from the ciphertext. An exhaustive study of the ciphertext needs to be done, but it may also prove difficult as the encrypted image will be unrecognizable and will not contain any useful information about the plain original image, so the attacker cannot use them for finding the key or the original image.

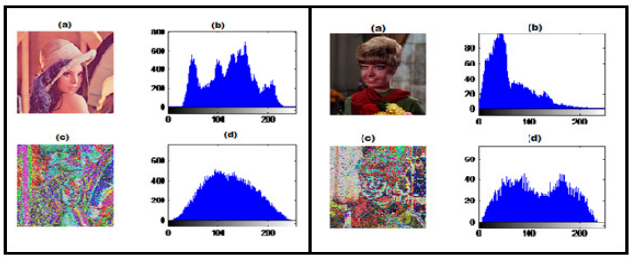


**Figure 4.** 2 blocks with color image encryption – each block (a, b) original image and its histogram, (c, d) encrypted image and its histogram.

## 6. Conclusion

In this paper, a new method for encrypting an image is introduced based on the concept of edge map which has given good results when implemented in MATLAB. Images for encryption were taken from a standard database[14]. The method was implemented for both gray and color images and for different sizes like 128x128, 256x256 and 512x512. From the histogram analysis it is shown that there is remarkable difference between the plain original image and the encrypted (cipher) image, which also adds to the security of the actual image. Cryptanalysis also shows that the proposed method protects the image against commonly known attacks. The proposed method can be used for securing images and similar kind of data in a variety of environments and applications.

## 7. References

1. Somaraj S, Hussain MA. Performance and security analysis for image encryption using key image. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–4.
2. Zhou Y, Again S, Joyner VM, Panetta K. Two fibonacci p-code based image scrambling algorithms. Proceedings. SPIE 6812, Image Processing: Algorithms and Systems VI; 2008 Mar. p. 1–12.
3. Wang D, Chang CC, Liu Y, Song G, Liu Y. Digital image scrambling algorithm based on chaotic sequence and decomposition and recombination of pixel values. International Journal of Network Security. 2015 May; 17(3):322–7.
4. Yuan MH, Jiang L. Image scrambling based on spiral filling of bits. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2015 Apr; 8(3):225–34.
5. Hu J, Han F. A pixel-based scrambling scheme for digital medical images protection. Journal of Network and Computer Applications. 2009 Jul; 32(4):788–94.

6. Ma K, Zhang W, Zhao X, Yu N, Li F. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Transactions on Information Forensics and Security. 2013 Mar; 8(3):553–62.
7. Jolfaei A, Mirghadri A. Image encryption using chaos and block cipher. Computer and Information Science. 2011 Jan; 4(1):1–14.
8. Sam IS, Devaraj P, Bhuvaneswaran RS. An intertwining chaotic maps based image encryption scheme. Journal of Nonlinear Dynamics. 2012 Sep; 69(4):1995–2007.
9. Younes MAB, Jantan A. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science. 2008 Feb; 35(1):1–9.
10. Zhang X, Cao Y. **A** novel chaotic map and an improved chaos-based image encryption scheme. Hindawi Publishing Corporation. The Scientific World Journal. 2014 Jul; 2014:1–8.
11. Prasad SRJ, Sathyanarayana RVS. Image encryption using color key images. International Journal of Electrical and Electronic Engineering and Telecommunications. 2013Oct; 2(4):1–12.
12. Podesser M, Schmidt HP, Uhl A. Selective bitplane encryption for secure transmission of image data in mobile environments. 5th Nordic Signal Processing Symposium; 2002. p. 1–6.
13. Image encryption using binary key-images. 2009. Available from: http://ieeexplore.ieee.org/document/5346780/
14. Computer Vision Group. 2016. Available from: https://vision.in.tum.de/