Performance and Security Analysis for Image Encryption using Key Image

Shrija Somaraj* and Mohammed Ali Hussain2

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

Abstract

Objective: This work is a review of image encryption algorithm using a key image, namely a secure image encryption algorithm based on bitplane principle. Method/Analysis: The analysis of the algorithm is done in terms of the parameters like histogram analysis, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Mean value analysis and Correlation coefficient. Findings: The results show that the algorithm reviewed offers commendable security against common types of attacks. Conclusion/Application: Most of the image encryption techniques have some security and performance issues. So there is a need to evaluate and analyze the efficiency of the algorithms used for encryption. These parameters are useful in judging the quality of encryption algorithms and can also be used for checking the level of security, the method actually provides to the actual image.

Keywords: Image Encryption, Key Image, Performance Analysis, Security Analysis, Statistical Analysis

1. Introduction

In the recent years with the coming of cloud and social networking sites, security of information has become a major challenge. Among multimedia, images are the ones which are most searched, uploaded and shared. This makes images more vulnerable for all sorts of attacks. Unlike text messages, the image data has some special features like high capacity, redundancy and high correlation among its constituent pixels. One of the main goals that must be achieved during the transmission of information over the network is security. Cryptography is the conventional way of dealing with this problem. It is a technique that can be used for secure transmission of data. The basic method involved in cryptography is to make the information to be transmitted unreadable by encryption so that only authorized persons can correctly recover the information. This kind of security through encryption can be provided for an image by using different encryption methods.

Different chaos based algorithms have been proposed with their performance analysis1–4. A novel image encryption technique based on Pixel Property separation is proposed5. The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics and unpredictable behavior. A novel image encryption method based on total shuffling scheme is also suggested6. Image encryption as an enhancement to AES algorithm by adding a key stream generator is also suggested7.

But all these methods have some security issues, as the key space or key size increases the quality and security of encryption also improves. Our work is based on encryption algorithm using an image as key, that can be applied to gray scale images as well as color images8. The algorithm uses a key of size M × N, where M × N is the size of the gray scale image or M × N × 3 for a color image8.

Tests have been conducted using images of different sizes and textures for statistical and security analysis. These include 1. Histogram analysis, 2. Adjacent pixel correlation analysis, 3. Mean value analysis, 4. Encryption quality, 5. Key space analysis, 6. Encryption speed comparison and 7. NPCR and UACI tests.

*Author for correspondence
Performance and Security Analysis for Image Encryption using Key Image

Statistical analysis of encrypted images provides information about the security of a cipher with respect to statistical attacks that could be done against the cipher. There are two important methods of statistical analysis of encrypted images. The first is histogram analysis and the second is the adjacent pixel correlation analysis.

2. Methodology

2.1 Bitplane Algorithm

Two new lossless image encryption algorithms using a new concept "key-image" which is a binary image with the same size as the original image to be encrypted was introduced\(^6\). Based on this bitplane algorithm is proposed\(^8\). It divides the image into 8 bit planes, and one of the bit plane of the source image is used as Key for encrypting the original image. The statistical and performance analysis of the algorithm is proposed in this paper. Image used for analysis is “Cameraman.tif (256x256 pixels)” from Matlab.

2.2 Histogram Analysis

The histogram of an image refers to a graph of the pixel intensity values. The histogram is a graph showing the number of pixels in an image at different intensity values found in the image. In an 8-bit grayscale image, there are 256 different possible intensities, and so the histogram will display 256 numbers showing the distribution of pixels amongst those grayscale values. For a good encryption, the distribution of gray scales in the encrypted image should be fairly uniform.

The gray scale images and color images of different sizes and textures are used for developing histograms of encrypted images obtained from algorithm in has been analyzed\(^8\). In Figure 1 it is observed that the histogram of

![Figure 1. (a) Original image and its histogram. (b) Encrypted image and its histogram.](image)

2.3 Adjacent Pixel Correlation Analysis

Correlation is a measure of the relationship between two variables or pixels in an image. If the two pixels are the two neighbouring pixels in an image, then there is a very close correlation between them else it is said they are less correlated. This is called adjacent pixel correlation in an image. The correlation coefficient CC, is computed using the equations 1-4 where x and y are gray values of two adjacent pixels in the original and encrypted image and N is the total number of adjacent pixels selected from the image and E refers to mean. The correlation coefficient, CC, has been computed using MATLAB command -corr2(). In the case of an encrypted image, the adjacent pixel correlation will be less if the encryption process is capable of hiding the details of the original image. Comparison of correlation coefficients in selected images and their cipher images obtained from encryption is given in table\(^8\).

Correlation Coefficient is calculated as:

\[
cc = \frac{\text{cov}(x, y)}{\sigma_x \times \sigma_y}
\]  
(1)

where \(\sigma_x = \sqrt{\text{var}(x)}\) 
(2)

\(\sigma_y = \sqrt{\text{var}(y)}\) 
(3)

\[
\text{var}(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2
\]  
(4)

\[
\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))
\]  
(5)

Table 1. Correlation coefficient values

| Cameraman Image     | Horizontal | Vertical | Diagonal |
|---------------------|------------|----------|----------|
| Original Image      | 0.9637     | 0.8877   | 0.8960   |
| Encrypted Image     | 0.0456     | −0.0568  | −0.0202  |
2.4 Mean Value Analysis
Mean Value Analysis is used for finding the vertical distribution of mean pixel gray values of an image. It gives the average horizontal distribution of intensity of pixel values in the image. In a plain image, the mean value vary along the width of the image, on the contrary in the encrypted image the mean value remains consistent along the width of the image, which is an indication of uniform distribution of values along the vertical lines of the encrypted image. Mean value data is collected from the encrypted images obtained from for different images.

Figure 2 shows the mean values obtained from the gray scale image 'Cameraman', and the mean values of the encrypted images obtained from encryption scheme. In the mean value plots of encrypted image, the mean value across the image remains nearly consistent and it can also be seen that the mean values of the encrypted images generated by are close to each other.

2.5 Measurement of Encryption Quality
The encryption quality refers to total changes in pixel gray values between the original image and the encrypted image.

Encryption Quality $Q$ is calculated as:

$$Q = \frac{\sum_{L=0}^{255} |HL(F) - HL(F')|}{256}$$

(6)

Where $L$ is the pixel gray level, $HL(F)$ the number of pixels having gray level $L$ in the original image and $HL(F')$ the number of pixels having gray level $L$ in the encrypted image. The encryption quality values of have been evaluated, using images of different sizes and textures.

A large size image contains more number of pixels and as the number of pixels increases, difference in number of pixels having same gray level increases giving a higher encryption quality value. The encryption quality varies for different images of same size as the image contents are different.

2.6 Key Sensitivity Analysis
Key sensitivity analysis is used for checking how much change is produced in the encrypted image, due to a small change i.e. 1 bit in the secret key. For determining this first the encryption program is run with the input image I and secret key K1 and the cipher image, C1 is obtained. Then the program is run with the same input image and another secret key K2, which is different by one bit with respect to K1 and the cipher image, C2 is obtained. Using these two encrypted images the difference image, $(|C1-C2|)$ is obtained. Figure 3 shows the encryption of original image using these keys by encryption algorithm and the difference images.

2.7 Measurement of Encryption Speed
The encryption speed is calculated by taking the ratio of the number of pixels (Bytes) in the image to the time taken for encryption. The tests have been conducted using Matlab-7 in an Intel Core 2 Duo CPU @ 2.00 GHz with Windows-8 operating system. Image of size 256 x 256
Performance and Security Analysis for Image Encryption using Key Image

pixels is used. The time taken for encryption is measured using Matlab commands tic and toc.

2.8 NPCR and UACI Tests

In order to test the influence of one-pixel change on the plainimage and the encrypted image, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Consider two images, whose corresponding plain images and encrypted images, be denoted by Io and Ienc. A bipolar array, D with the same size as images Io and Ienc is defined. Then, D(i,j) is determined by Io(i,j) and Ienc(i,j), namely, if Io(i,j) = Ienc(i,j) then D(i,j) = 0; otherwise, D(i,j) = 1.

NPCR is defined as

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

where

$$D(i,j) = \begin{cases} 0, & \text{if } Io(i,j) = Ienc(i,j) \\ 1, & \text{if } Io(i,j) \neq Ienc(i,j) \end{cases}$$

The NPCR measures the percentage of different pixel numbers between the plainimage and the cipherimage.

UACI is defined as

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

which measures the average intensity of differences between the two images. Some tests have been performed on ‘Cameraman image’ about the influence of only one-pixel change on the 256 grey scale image and color image. Generally, these obtained results for NPCR and UACI show that the proposed algorithm is very sensitive with respect to plain image.

3. Conclusion

In this paper analysis of the bitplane algorithm is done. The technique using bitplane principle has a large key space and its implementation is quite simple. It is observed that the algorithm gives a commendable performance based on the histogram analysis, adjacent correlation coefficient analysis, mean value analysis, encryption quality, encryption speed, NPCR and UACI tests. The algorithm is analysed for gray as well as color images and for different sizes.

4. References

1. Ismail IA, Amin M, Diab H. A digital image encryption algorithm based on composition of two chaotic logistic maps. Proceeding 27th IEEE Int'l Conf Signal Processing. 2011; 733–9.
2. Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences. Elsevier. 2010; 181:1171–86.
3. Mancilla DL, Lopez JHG, Reategui RJ, Chiu R, Rauda EV, Hernandez CEC, Cuellar GH. Statistical analysis of imaging encryption using chaos. Latest Trends in Circuits, Systems, Signal Processing and Automatic Control. CISSPA. 2009. p. 86-90
4. Ashtiyani M, Birgani PM, Hosseini HM. Chaos-based medical image encryption using symmetric cryptography. 3rd International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA; Damascus. 2008 Apr 7-11. p. 1–5.
5. Iyer KC, Subramanya A. Image encryption by pixel property separation. Cryptology ePrint Archive. 2009. Available from: http://eprint.iacr.org/2009/043.pdf
6. Zhang G, Liu Q. A novel image encryption method based on total shuffling scheme. Optics Communications. 2011 Jun 1; 284(12):2775–80.
7. Zeghid M, Machhout M, Khirji 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.
8. Somaraj S, Hussain MA. Securing medical images by image encryption using key image. International Journal of Computer Applications. 2014 Oct; 104(3):30–4.
9. Tamilselvi R, Ravindran G. Image encryption using pseudo random bit generator based on logistic maps with radon transform. Indian Journal of Science and Technology. 2015 Jun; 8(11).
10. 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.