An Image Cryptosystem based on Pixel Scrambling and AES Algorithm

Tanvi
Assistant Professor
Baddi University of Emerging Sciences & Technology, Baddi

ABSTRACT

Evolution of information technology has led to creation of tremendous amount of digital data. The major part of the digital data is multimedia data. The multimedia data is often exchanged over internet. So security of this data is very important. Cryptography is one of the ways to ensure security. In recent years much research has taken place to secure digital images. A digital image is a collection of intensity values of the pixels arranged in the form of a two dimensional matrix. It has been observed that the intensity values of the nearby pixels are strongly related. In this paper an image cryptosystem is proposed that encrypts the digital images by first dividing them into blocks, then the pixel values of the blocks are scrambled. Then the scrambled blocks are randomly passed to the AES algorithm. It is hoped that the proposed method decreases the correlation among the nearby pixels and helps to secure the digital images.

Keywords

Advanced Encryption Standard (AES), Cryptography, Image scrambling, Security analysis, entropy, correlation, image encryption.

1. INTRODUCTION

A digital image is defined as a matrix. Each element of the matrix represents the intensity values of the pixels of an image. Over the years many tools have been developed to secure the digital images. Some of the tools used for encrypting images are based upon cryptography. But the cryptographic approaches that work quite well on text data, do not give the same performance on multimedia data. So there is a need to develop algorithms to encrypt multimedia data. Confidential data must be protected against leakage of sensitive information. In the computers the digital data is stored in the form of files. So the task of securing digital images is more of the task of protecting digital files. A large number of methods have been proposed by researches to protect files. But most of the methods that have been proposed are for files that contain textual data. As the multimedia data is very large in size and have lot of redundant information so the methods that wok very good for files that contain textual data, do not work well for multimedia data.

Cryptographic techniques are generally used to provide security during file transfer over open networks such internet. Advanced Encryption Standard (AES) is a well-known algorithm to encrypt the digital data. But it has been observed that this algorithm fails when it comes to encrypt digital images that have a single a single basic color background such as white, red, black or green. So the well accepted algorithm for ensuring security for textual information cannot work well for multimedia data. The cause for this can be attributed to the fact that the multimedia data is very large in size, has lot of redundancy and the adjacent pixels are having close correlation among them.

So in this paper an attempt has been made to augment the strengths of AES algorithm for image data encryption. In order to achieve our goal a preprocessing step has been introduced before passing the data for encryption to AES algorithm. This step has been introduced as it was observed that AES algorithm cannot work upon images that have uniform basic color background. In the preprocessing step the contents of the image are divided into blocks. Then these blocks are scrambled and then the scrambled blocks are randomly passed to the AES algorithm for encryption. The results have been quite encouraging.

In section 2 the previous work has been discussed, section 3 describes the proposed cryptosystem, section 4 presents the security analysis and section 5 concludes the paper.

2. PREVIOUS WORK

Seyed Hossein Kamali, Reza Shakerian, Mayson Hedayati, Morisen Rahmarn [1]. have proposed a new modified version of AES for encrypting the digital images. They have changed the shift rows transformation step of the original AES algorithm. In the shift rows transformation, if the value in the first row and first column is even, the first and fourth rows are unchanged and each byte in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows for greater security and increased performance. But as evident from the results shown by [1] modifying a well-accepted algorithm just helps to improve the entropy of the encrypted image by 0.004% and secondly the method can just encrypt square images.

3. PROPOSED CRYPTOSYSTEM

If an image is encrypted by an AES algorithm then the following results are obtained:

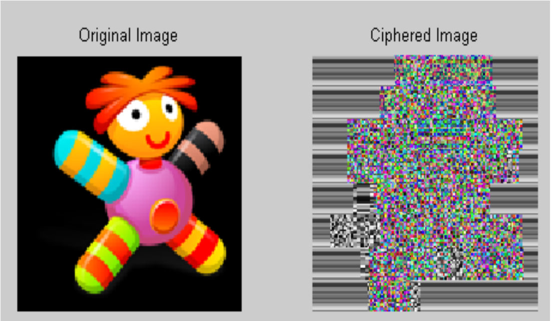


Fig 1: Image Encryption using AES

From the above results the layout of the original image can be easily guessed. So AES algorithm is not a good choice to encrypt the digital images. So [1] proposed a modified the AES algorithm by changing the shift row transformation step of the AES algorithm. By changing the shift rows step there was marginal increase in entropy. But is believed that a well accepted algorithm should not be altered for little improvement in results. In this paper a preprocessing step process has been added to encrypt the images keeping the integrity of the AES algorithm

3.1 Goals

The goal of this work is to develop a system that:

- Decrease the correlation among the neighboring pixels of the ciphered image.
- To increase the entropy of the ciphered image.
- To have more uniform histogram for the ciphered image.
- To compare the correlation, entropy and histogram of ciphered image with the results for AES algorithm.
- The proposed system should work for any size and any type of images.

3.2 Design of Proposed System

The proposed system is free from the size and type of the Image (i.e. jpg, bmp,tiff,gif etc.). The system works as follows:

- All users have a pair of public – private key, through any key generating algorithm (RSA – key generating algorithm).
- A Key Kb for scrambling of blocks.
- A Key Ko giving the random order in which the blocks are to be processed.
- A Key for AES Encryption (Ka).

Following steps are performed at the sender and receiver side:

At the Sender Side

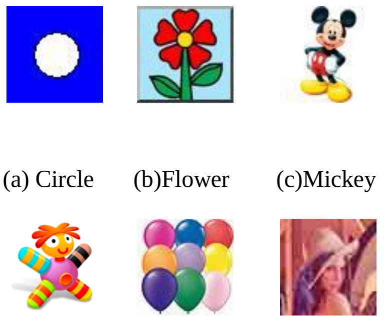
- Divide the input Image in n x n square blocks. Value of n to be provided by user.
- Scramble the blocks based upon key Kb
- Apply AES algorithm on the blocks using the key (Ka) and using the order of encryption based on the key (Ko).
- Transfer the encrypted Image, Ka, Ko, Kb and n to the receiver after encrypting them with the public key of the receiver.

At the Receiver Side

- Decrypt the keys Ka, Ko,Kb and n using receiver's private key.
- Decrypt the Image received from the sender using inverse of AES algorithm with Ko, Ka and n.
- Unscramble the blocks based on Key Kb.
- Image is decrypted.

3.3 Simulation Methodology

In this work, our main aim is to implement the proposed algorithm and analyze the performance. The implementation has been done in MATLAB software package .. For analysis purpose an image set of the following six images has been taken.



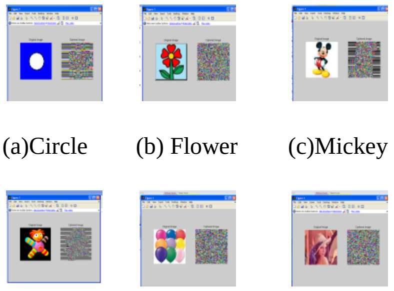
(a) Circle (b)Flower (c)Mickey

(d)Doll (e)Balloons (f)Lena

Fig 2: Image Set

3.4 Results obtained after encryption using AES Algorithm

The image set was subjected to the AES algorithm for the purpose of encryption and following results have been obtained:



(a)Circle (b) Flower (c)Mickey

(d) Doll (e) Balloons (f) Lena

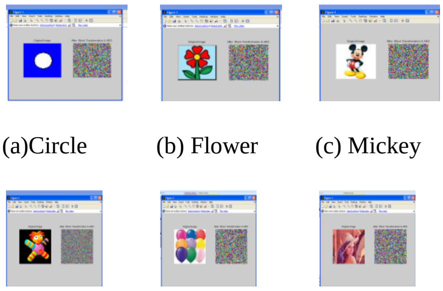
Fig 3: Results of Image Set after application of AES algorithm

After analyzing the above results we can easily figure out that for the images (a), (c), and (d) the results of encryption are still intangible to some extent. One can easily figure out that the contents of the file have been tempered with. The areas that have a single color show unusual results. It has been observed that if AES algorithm is applied to an image that is having major portion of the image as a single color, then it gives these types of results.

To overcome this problem we have proposed an algorithm that scrambles the pixels before applying AES algorithm. By adopting this method the correlation among the neighboring pixels is reduced and entropy is increased.

3.5 Results obtained after encryption using random block transformation followed by AES Algorithm

The AES algorithm cannot be successfully applied to the digital images that are having major portion as a single color. The digital images have high correlation among the neighboring pixels. To lower the correlation a transformation algorithm is proposed in which the image is broken into square blocks of size nxn and then the blocks are transformed based on a key. Then the blocks are randomly fed to the AES algorithm. After this process the following results were obtained:



(a)Circle (b) Flower (c) Mickey

(d) Doll (e) Balloons (f) Lena

Fig 4: Results of Image Set after application of Random Block Transformation and AES algorithm

After viewing the above results we can see that the problem of encrypting an image that has a major portion as a single color has been solved.

4. SECURITY ANALYSIS

A good encryption procedure should be robust against all kinds of cryptanalytic, brute force and statistical attacks[3]. The security of an image cryptosystem is determined by its confusion and diffusion capabilities. The results of the proposed system have been compared with that of AES algorithm. The results have been compared using Histogram analysis, entropy and correlation analysis.

4.1 Histogram Analysis

An image histogram depicts the distribution of pixels in an image by grouping the number of pixels of same intensity values. Since in images the near by pixels have same intensity values so it is desired that while encrypting a ciphered image is created that has very less similarity to the plain image.

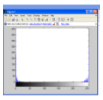
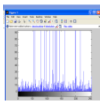
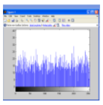
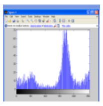
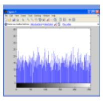
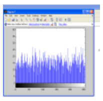
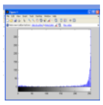
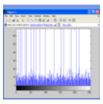
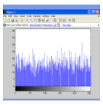
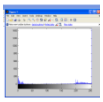
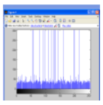
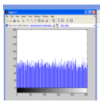
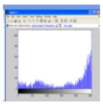
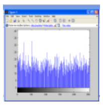
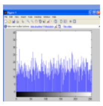
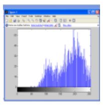
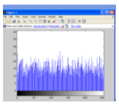
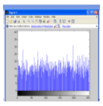
Image	Original Image	Ciphered By AES Image	Ciphered Image by Proposed method
Circle			
Flower			
Mickey			
Doll			
Balloons			
Lena			

Fig 5 : Plot of Histograms

It can been seen from the histograms of the above figure that the proposed method has helped to produce uniform histograms as compared to the original image. Thus signifying that the pixels in the ciphered image are uniformly distributed across the entire image..

4.2 Entropy

Entropy is the measure of randomness. The changing values of the contrast of the image are measured by Image entropy[9]. The images that have very little contrast are having very low entropy where as the images that have varying contrast values have high entropy values. In order to measure the contrast in the original images and the images encrypted with proposed method a measure of entropy was also considered. From the following table it can be observed that the proposed method has significantly increased the entropy value of the encrypted images.

$$H(X) = \sum_{i=1}^{n} p_i \log_2\left(\frac{1}{p_i}\right)$$

Where the entropy H(m) of m can be calculated, where $P(m_i)$ is the probability of m_i and the entropy is expressed in bits.

Table 1: Entropy Values

Image	Original Image	AES	proposed method
Circle	2.0846	6.6230	7.9542
Flower	7.2148	7.9582	7.9627
Mickey	4.0471	7.2781	7.9515
Doll	3.5336	7.1484	7.9896
Balloons	6.8937	7.9563	7.9597
Lena	7.2778	7.9597	7.9740

.

4.3 Correlation Analysis

Correlation is a measure to calculate the similarity among the near by pixels. It can be calculated by finding the correlation coefficient of two adjacent pixels. If the correlation coefficient is 1 it means that the pixel intensities are same and it is it -1 then it means that the pixels are reverse of one another.

Table 2: Correlation Values

Image	AES	proposed method
Circle	0.0053	-0.0099
Flower	0.0042	0.0106
Mickey	0.0932	-0.0290
Doll	0.0417	0.0059
Balloons	0.0126	-0.0292
Lena	7.4424e-004	0.0088

From the above table it can be concluded that the correlation has significantly decreased on application of the proposed method.

5. CONCLUSIONS

In this paper a simple and a robust method has been proposed using a combination of block based random pixel scrambling and encryption technique. Experimental results show that the correlation has decreased when the proposed algorithm was applied to the images before the AES algorithm and entropy has increased. We are able to get more smooth histograms So it is hoped that the proposed cryptosystem based on random scrambling & AES algorithm will provide a valuable tool for securing digital Images.

6. REFERENCES

[1] Seyed Hossein Kamali, Reza Shakerian, Mayson Hedayati, Morisen Rahmarn, “ A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption” International Conference on Electronics & Information Engineering (ICEIE 2010), (VI 141-VI 145) ,IEEE,2010

[2] Jui-Cheng Yen, Jiun-In Guo, “A New Chaotic Image Encryption Algorithm ”, International Conference on Computer Security, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, pp 124-128,2007.

[3] Anil Kumar Yadav , Ravinder Purwar, “ Complexity Analysis of Image Encryption Technique”,International Conference on Image Processing, Department of Computer Applications Institute of Engineering & Technology Kanpur , Vol 3, No 1 ,pp 117-121,2008

[4] Mohammad Ali Bani Younes and Aman Jantan, “An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption”, International Journal of Computer Science & Network Security, Vol 3 No 4, April 2008

[5] Advanced Encryption Standard, NIST FIPS PUB 197, U.S. Department of Commerce, 2001.

[6] J. Daemen, V. Rijmen, The Block Cipher Rijndael, Lecture Notes in Computer Science 1820, pp. 288-296, 2000.

[7] S.S.Maniccam, N.G. Bourbakis, “Lossless Image Compression and Encryption using SCAN”, Journal of Pattern Recognition, Vol 34, pp 1229-1245,2001.

[8] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption Using Block – Based Transformation Algorithm” IAENG, Vol 35, No 1,pp 412-416, February 2008.

[9] Shannon CE., "Communication theory of secrecy system," Bell Syst Tech J 1949,28,656-715.