REVIEW OF IMAGE ENCRYPTION AND DECRIPTION TECHNIQUES FOR 2D IMAGES
Jalpa Shah *1, J S Dhobi 2
*1, 2 Department of Computer Engineering, Government Engineering College, Gandhinagar, Gujarat, India

Abstract:
In the emerging era of Internet, multimedia software and application security of images is of major concern. To offer security to these images encryption is the way for robust security. With Image Encryption it becomes difficult to analyze the image that is communicated over untrusted network. Also it provides security for any unauthorized access. The paper provides an introduction to cryptography and various image encryption techniques are reviewed for 2D images.

Keywords: Internet; Security; Image Encryption; Cryptography; 2D Image; Access.


1. Introduction

Digital image processing is the use of computer algorithms to perform image processing on digital images. The input of that system is a digital image and the system process that image using efficient algorithms, and gives an image as an output.

Image Encryption is the conversion of image to unknown format using some cryptography algorithm and a key. Similarly Image Decryption is the conversion of unknown format of image to original image using the decryption algorithm. The model of Image Encryption & Image Decryption is shown in Fig 1 and Fig 2 respectively.

Figure 1: Model of Image Encryption (Grayscale Image)
Based on the number of keys there are 2 types of Cryptography algorithms: Secret Key Algorithm in which only 1 key parameter is used to encrypt and decrypt the data (text, video, images, etc) and Private Key Algorithm in which 2 keys are used for encryption and decryption purpose. The former is known as Symmetric Key Algorithm and latter is known as Asymmetric algorithm.

The digital images have high correlation between adjacent pixels; hence traditional cryptography algorithms cannot be used.

2. Terminology in Image Encryption and Image Decryption

Various terms that are used in Image Encryption & Image Decryption Algorithms are described as under:

**Plain image**: A source or an original image is known as plain image.

**Cipher image**: encrypted or coded image is called cipher image.

**Encryption or Enciphering**: the process from transforming the plain image to cipher image is called Encryption or Enciphering.

**Decryption or Deciphering**: Restoring the plain image from cipher image is called Decryption or Deciphering.

**Cryptography**: The many schemes used for enciphering constitute the area of encryption that is known as cryptography.

Shannon, in one of the fundamental papers on the theoretical foundations of cryptography [1, 2], gave two properties that a good cryptosystem should have to hinder statistical analysis: diffusion and confusion. Diffusion means that if we change a pixel of the plain image, then several pixels of the cipher image should change, and similarly, if we change a pixel of the cipher image, then several pixels of the plain image should change. This means that frequency statistics of pixels in the plain image are diffused over several pixels in the cipher image, which means that much more cipher image is needed to do a meaningful statistical attack. Confusion means that the key does not relate in a simple way to the cipher image. In particular, each character of the cipher image should depend on several parts of the key.
### 3. Literature Review

The comparison of various image encryption algorithms is given in following table:

<table>
<thead>
<tr>
<th>Paper</th>
<th>Technique Used</th>
<th>Merits</th>
<th>Demerits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital RGB Image Encryption Based on 2D Cat Map and Shadow Numbers[3]</td>
<td>2D Cat Map and Shadow method[RGB]</td>
<td>Shadow number uses 2 keys :1 as image another is derived using the equation</td>
<td>Key Sensitivity analysis not done. O/p of ACM and with shadow numbers does have much difference.</td>
</tr>
<tr>
<td>A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map[5]</td>
<td>ACM and Henon Map</td>
<td>Various formats of images used</td>
<td>Other maps can be used</td>
</tr>
<tr>
<td>Image encryption based on Independent Component Analysis &amp; Arnold's Cat Map[6]</td>
<td>ACM &amp; ICA</td>
<td>Resistance to crypanalysis due to ICA.</td>
<td>2 images are used for Encryption purpose.. For Decryption JADE algorithm is used.</td>
</tr>
<tr>
<td>Image encryption using Camellia and Chaotic maps[8]</td>
<td>ACM and modified Camellia</td>
<td>Large key space and short encryption time</td>
<td></td>
</tr>
<tr>
<td>Image Encryption using Chaos Theory [9]</td>
<td>Chirikov Map</td>
<td>Resistance to cryptanalysis</td>
<td>Only 1 map for both diffusion and confusion</td>
</tr>
<tr>
<td>A Survey paper based on Image Encryption and Decryption using modified advanced encryption[11]</td>
<td>AES</td>
<td>AES better than blowfish, DES, 3DES</td>
<td>Due to close relation in adjacent pixels the AES is not much secure.</td>
</tr>
</tbody>
</table>
4. Conclusions and Recommendations

Thus the image encryption and decryption with the help of chaos system is better than the existing traditional algorithms. The paper gives only theoretical comparison of various methods.

References


*Corresponding author.
E-mail address: jalpa08ce91@gmail.com