Color Image Encryption Using Spiral Encoding Technique and Symmetric key

Jayeeta Majumder and Partha Pratim Bankura

Abstract - Information technology is one of the necessary things today, because a major part of the society depends on it. Several service sectors cannot continue their work without information technology. For this reason matters related to information storing, maintenance, security are essential today. Information may be text, audio, video, images. Image is one of the key information which can tell thousand words. Information security is vital aspect today. Here we discuss Image security. Information security goal can be divided into three part confidentiality, integrity, availability. Confidentiality is achieved through encryption process. We encrypt image through spiral encoding and symmetric key. Both spiral encoding and symmetric key destroy pixel correlation. Our proposed encryption algorithm has two major part one change pixel position other part change pixel value. So good quality encrypted image is achieved through our encryption algorithm. Our proposed decryption algorithm also returns same good quality of image as before encryption. By histogram comparison we prove it and also secure from differential and statistical attack.

Index Terms - spiral encoding, spiral decoding, plain image, cipher image, NPCR, UACI, PSNR

1. Introduction

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several areas. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Here we encrypt image with different technique. This is known as spiral encoding technique. Encryption process has two major different step one manipulate pixel position which is very simple. But adding some feature it become very efficient for encryption. Other step we manipulate pixel value. This type of manipulation is done by symmetric key. Spiral encoding or spiral scanning [1] is one of popular technique which is used in the various fields including medical science also. This technique is also useful for image encryption. It transforms a plain image into an image which is completely noisy from where image recovery is not possible without proper decryption process. Spiral decryption or spiral decoding [1] process is very efficient because it returns exact pixel value of plain image and it does not use complex mathematical computation which take lot of time.

But this technique is very efficient because adding some feature with it gives good quality of image encryption.

2. Proposed Encryption Algorithm

Input: secret image, shared key key1 and r, dummy image
Output: encrypted image

Step1: compute s=secret image XOR dummy image. (Here dimension of both image are same)
Step2: for each pixel location (x,y) of s
        If(y mod 2=0)
            s1= s XOR key1
        else
            s1=s XNOR key1
Step3: choose a shared secret number r, where r ∈ Zn*
Step4: SPI= spiral encoding of s1, r times
Step5: compute  T = \sum_{x,y=1}^{w,h} SPI(x,y)
Here x,y is the pixel coordinate and w,h are width and height of image
Step6: EP=SPI(x,y)+T
Step7: Key2=Key1+T;
Step8: ENC= Encrypt [key2 and information of dummy image]
Step9: Send ENC, EP

3. Proposed Decryption Algorithm

Input: ENC, EP
Output: secret image

Step1: D=decrypt ENC
Step2: k=key2-key1
Step3: D1=EP-k
Step4: DI1=perform spiral decoding of image D1, r times
Step5: for each pixel location(x,y) of DI1 do
If(y mod 2=0)
DI2=DI1 XOR key1
Else
DI2= DI1 XNOR key1
Step6: compute DI=DI2 XOR dummy image (DI is original secret image)

4. Security analysis
4.1 Differential analysis

Differential attack is one kind of chosen cipher text attack. It occurs when attacker any how access computer and chooses plaintext and cipher text pair. His main objective is to find key. In case of image encryption NPCR [2] and UACI [2] test are used to reduce the probability of differential attack. High NPCR and UACI are expected to reach the goal. NPCR defined as number of pixels change rate of chipper image while one pixel is changed. Mathematical expression of NPCR as follows:

\[
NPCR = \frac{\sum D(i,j)}{W \times H} \times 100\%
\]

Where D(i,j) is defined as

\[
D(i,j) = \begin{cases} 
0, & \text{if } c_1(i,j) = c_2(i,j) \\ 
1, & \text{if } c_2(i,j) \neq c_2(i,j) 
\end{cases}
\]

Here W means width of image and H height of image.

UACI is used to find average intensity change between two cipher images whose one pixel is changed. Mathematical expression is as follows:

\[
UACI = \frac{\sum [c_1(i,j) - c_2(i,j)]}{F \times T} \times 100\%
\]

Here c1 and c2 are cipher images of plain image P1 and P2. P1 and P2 are same except one pixel. F is largest pixel value supported by cipher image. T is total number of pixel.

4.2 Statistical analysis
4.2.1 Correlation analysis

Correlation is used to find the similarity between two variables. Correlation 1 means two variables are same. Correlation 0 means two variables are totally different. Correlation among pixels of cipher image should be very low otherwise correlation attack will occur.

4.2.2 Information entropy analysis

Cipher image entropy [3] should be higher than plain image entropy otherwise entropy attack will occur. Entropy H(s) defined as follows

\[
H(S) = \sum_{i=0}^{2^N-1} P(S_i) \log_2 \left( \frac{1}{P(S_i)} \right)
\]

where P(s) represents the probability of symbol s and the entropy is expressed in bits.

4.2.3 PSNR analysis

Peak Signal-to-Noise Ratio (PSNR) is playing significant role in analysis of encryption process. If PSNR [4] value is greater than 30 db then signal is recoverable. So PSNR value of encrypted image should be very low, otherwise encrypted image may decrypted without using proper decryption process.

5. Result of various experiments
5.1 Result of NPCR and UACI test

<table>
<thead>
<tr>
<th>Image Size</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>128 x 128</td>
<td>99.41</td>
<td>0.38</td>
</tr>
<tr>
<td>255 x 255</td>
<td>99.50</td>
<td>6.67</td>
</tr>
<tr>
<td>1440 x 900</td>
<td>99.42</td>
<td>0.13</td>
</tr>
</tbody>
</table>

Table1: Result of NPCR and UACI test

<table>
<thead>
<tr>
<th>Adjacent pixels</th>
<th>Correlation coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Plain image</td>
</tr>
<tr>
<td>Horizontal</td>
<td>0.867</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.874</td>
</tr>
</tbody>
</table>

Table2: Result of Correlation test
5.3 Result of information entropy test

<table>
<thead>
<tr>
<th>Plain image Entropy</th>
<th>Cipher image entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7337</td>
<td>7.9953</td>
</tr>
<tr>
<td>5.9766</td>
<td>7.9430</td>
</tr>
<tr>
<td>6.4017</td>
<td>7.9997</td>
</tr>
</tbody>
</table>

Table3: result of entropy test

5.4 Result of PSNR test

<table>
<thead>
<tr>
<th>PSNR of cipher images</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0939</td>
</tr>
<tr>
<td>6.9192</td>
</tr>
<tr>
<td>8.7321</td>
</tr>
</tbody>
</table>

Table 4: result of PSNR test

<table>
<thead>
<tr>
<th>Images taken for experiment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain image</td>
</tr>
<tr>
<td><img src="image1" alt="Plain image" /></td>
</tr>
<tr>
<td><img src="image3" alt="Plain image" /></td>
</tr>
<tr>
<td><img src="image5" alt="Plain image" /></td>
</tr>
</tbody>
</table>

Table5: Image Taken for experiment

6. Histogram analysis

Figure1: Histogram of plain image

Figure2: Histogram of encrypted image

Figure3: Histogram of decrypted image

7. Conclusion

In this paper, we proposed two algorithms, one for image encryption process and other for decryption. Here we use spiral encoding and spiral decoding technique for creating confusion of neighboring pixel correlation. Here we use a symmetric key and shared secret number which enhanced the overall encryption technique. Several experiments show that proposed algorithms are good enough to prevent differential attack and statistical attack.
8. References


