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 its work without information technology. For this reason matter 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. Here we discuss image encryption. 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 $key_1$ 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)
$s_1$= s XOR $key_1$
else
$s_1$=s XNOR $key_1$
Step3: choose a shared secret number r, where r $\epsilon$ $Z_N^+$
Step4: SPI= spiral encoding of $s_1$, r times
Step5: compute $T = \sum_{x,y=1}^{w,h} \mathrm{SPI}(x,y)$
Here x,y is the pixel coordinate and w,h are width and height of image
Step6: EP=SPI(x,y)+T
Step7: $Key_2$=$Key_1$+T;
Step8:  ENC= Encrypt [$key_2$ 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=$key_2$-$key_1$
Step3: $D_1$=EP-k
```

•Author name isJayeeta Majumder . Currently she is an Assistant Professor at Haldia Institute of Technology, Haldia,West Bengal, India. Her E-mail ID is jem2003_kolkata@yahoo.co.in.
•Co-Author name is Partha Pratim Bankura. Currently he is pursuing master degree in computer science & engineering at Haldia Institute of Technology, Haldia, West Bengal, India. His E-mail ID is parthabankura@gmail.com.

```
Step4: DI1=perform spiral decoding of image $D_1$, r times
Step5: for each pixel location(x,y) of DI1 do
If(y mod 2=0)
 DI2=DI1 XOR $key_1$
Else
DI2= DI1 XNOR $key_1$
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:

Suppose P1 is a plain image and c_1 is corresponding cipher image. Now P2 is another plain image which is exactly same as P1 except one pixel. Now c_2 is cipher image of plain image P2.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

Where D(i,j) is defined as

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

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:

$$UACI = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{F.T} X\ 100\%$$

Here $c_1$and c_2 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

4.2.1Correlation 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. Correlations among pixels of plain image are very high. Correlation among pixels of cipher image should be very low otherwise correlation attack will occur.

4.2.2Information entropy analysis

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

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

where $P(s_i)$represents the probability of symbol s_i 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

Image Size	NPCR	UACI
128 x 128	99.41	0.38
255 x 255	99.50	6.67
1440 x 900	99.42	0.13

Table1: Result of NPCR and UACI test

5.2 Result of correlation test

Adjacent pixels	Correlation coefficients		
	Plain image	Encrypted image	Number of pixel pairs
Horizontal	1	-0.094	26
Vertical	0.996	-0.126	250
Horizontal	0.867	0.012	50
Vertical	0.874	0.124	100

Table2: Result of Correlation test

5.3 Result of information entropy test

Plain image Entropy	Cipher image entropy
7.7337	7.9953
5.9766	7.9430
6.4017	7.9997

Table3: result of entropy test

5.4 Result of PSNR test

PSNR of cipher images
6.0939
6.9192
8.7321

Table 4: result of PSNR test

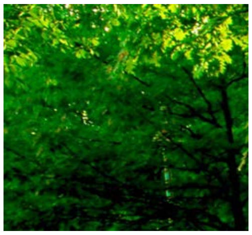
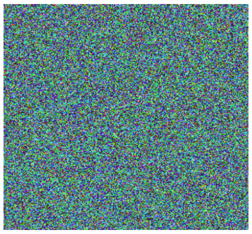
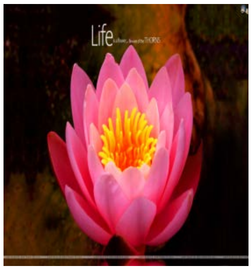
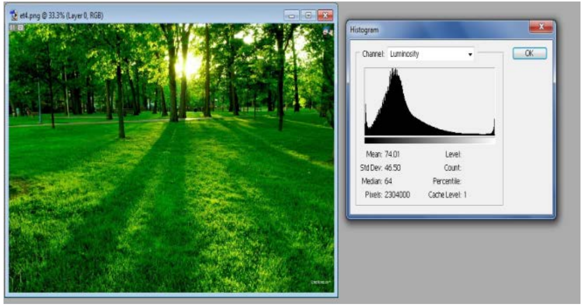
Images taken for experiment	
Plain image	Encrypted image
	
	

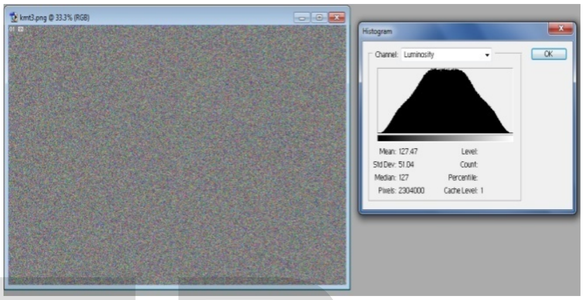
Table5: Image Taken for experiment

6. Histogram analysis



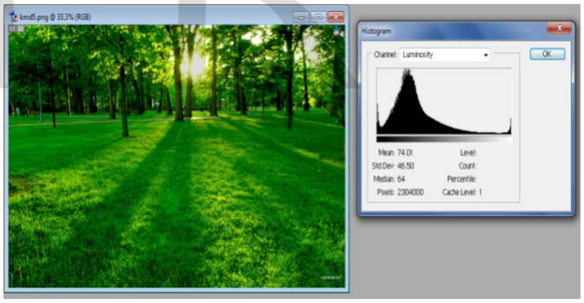
Mean: 74.01 Level:
Std Dev: 46.50 Count:
Median: 64 Percentile:
Pixels: 2304000 Cache Level: 1

Figure1: Histogram of plain image



Mean: 127.47 Level:
Std Dev: 51.04 Count:
Median: 127 Percentile:
Pixels: 2304000 Cache Level: 1

Figur2: Histogram of encrypted image



Mean: 74.01 Level:
Std Dev: 46.50 Count:
Median: 64 Percentile:
Pixels: 2304000 Cache Level: 1

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

[1] NilanjanDey, SouravSamanta, AnamitraBardhan Roy, *"A Novel Approach of Image Encoding and Hiding using Spiral Scanning and Wavelet Based Alpha-Blending Technique"*, IJCTA, Vol 2 (6), 1970-1974, ISSN:2229-6093, NOV-DEC 2011

[2] Jawad Ahmad and Fawad Ahmed *"Efficiency Analysis and Security Evaluation of Image Encryption Schemes"* International Journal of Video & Image Processing and Network Security, IJVIPNS-IJENS Vol:12 No:04,August 2012.

[3] Ahmed Bashir Abugharsa, AbdSamad Bin HasanBasari, Hamida Almangush*"A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm"* , International Journal of Computer Applications, Volume 42– No.9, March 2012

[4] Narendra K Pareek*"Design And Analysis Of A Novel Digital Image Encryption Scheme"*, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012