Image Encryption in Transform Domain using Circular Shift

Tanuja Sarode, PhD
Thadomal Shahani Engineering College Affiliated to Mumbai University, India

Devishree Pillai
Thadomal Shahani Engineering College Affiliated to Mumbai University, India

Shalmalee Pokale
Thadomal Shahani Engineering College Affiliated to Mumbai University, India

Tejashri Prabhu
Thadomal Shahani Engineering College Affiliated to Mumbai University, India

ABSTRACT
With the advent of cloud storage and increase in transmission images through internet, images are more vulnerable to attacks of various hackers. A lot of private images are leaked from the cloud. Information security has become a major concern. Also, as the use of digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. Encrypting the images is one way of dealing with this threat. Image encryption techniques try to convert original image to another image which is hard to decipher so that the image is kept confidential between users, in other words, it is essential that nobody will get to know the content without a key for decryption. This paper proposes a new approach to image encryption using circular shift in transform domain.

General Terms
Image encryption, Security

Keywords
Circular shift, Discrete Cosine Transform

1. INTRODUCTION
Encryption is a process of converting the message into a coded format (cipher) which ensures that the message is unintelligible to anyone without means to decipher it [1]. Decryption is converting the cipher back to the original message so that it is readable [1]. Encrypting data provides confidentiality, integrity and authentication [2]. Traditional text encryptions cannot be used for encrypting images as they are much larger in size which causes overhead and is a costly process [3]. The vicinal pixels are highly correlated in images and hence text encryptions fail to conceal the entire Image; also the images have patterns and repetitive backgrounds which are not taken into account by the text encryptions and this increases redundancy [3]. Also complete accuracy is not needed in image encryption unlike text encryption. Hence conventional encryption algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, and International Data Encryption Standard (IDEA) are not suitable for image encryption, hence encryption algorithms made exclusively for images are needed [3]. This paper presents image encryption in transform domain; in which a series of row or columnar circular shifts are applied to a DCT transformed image and the image is decrypted back by undoing those circular shifts.

2. SYSTEM DESCRIPTION

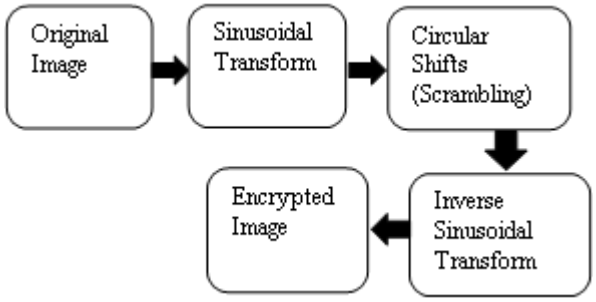

Figure 1: Steps of Encryption

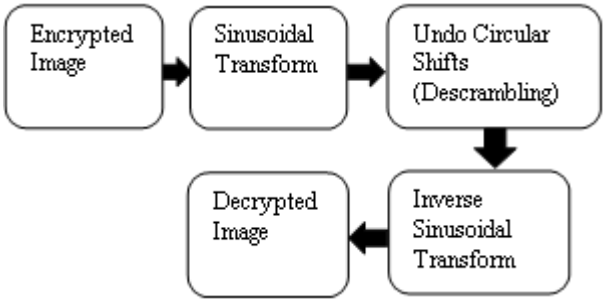

Figure 2: Steps of Decryption

3. PROPOSED ALGORITHM

3.1 Encryption Phase
1. The image is DCT transformed.
2. Now either perform row-wise or column-wise circular shift, to do that first the image is divided into two parts and circular shifted by a number which can be user input key.
3. Keep dividing the image into halves and repeat step 2.
4. After all circular shifts are done perform inverse DCT transform on the image
5. This completes the encryption stage.

3.2 Decryption Phase
1. The image which is received from the encryption phase is again DCT transformed.
2. Divide the image into half and undo the circular shift
3. Divide the two halves into halves and undo the circular shifts
4. Keep repeating step 3 till you get back the image.
5. After the circular shifts are undone apply inverse DCT transform and get back the original image.

3.3 DCT Transform

Discrete Cosine Transform expresses an image into a summation of Cosine functions that converts it into the frequency domain [4]. DCT transform contains the real coefficients and is more efficient than Discrete Sine Transform [4]. The general equation for 2D discrete cosine transform is as follows.

$$F(m,n)= \frac{2}{\sqrt{MN}}\mu(m)\mu(n)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \cos\frac{(2x+1)m\pi}{2M} \cos\frac{(2y+1)n\pi}{2N} \quad (1)$$

Where $\mu(m)$, $\mu(n)=\frac{1}{\sqrt{2}}$ for m, n = 0 and C(m), C(n)=1 otherwise.

3.4 Example

Step 1: Representing image as a matrix

12	34	15	76	55	99	14	26
47	89	111	94	48	58	41	78
18	87	45	44	89	41	79	22
85	98	77	49	41	97	99	45
11	54	165	47	19	22	44	94
46	41	66	17	25	24	11	41
18	94	92	44	56	129	41	77
07	01	98	11	24	26	27	01

Step 2: Divide the matrix into half.

12	34	15	76	55	99	14	26
47	89	111	94	48	58	41	78
18	87	45	44	89	41	79	22
85	98	77	49	41	97	99	45
11	54	165	47	19	22	44	94
46	41	66	17	25	24	11	41
18	94	92	44	56	129	41	77
07	01	98	11	24	26	27	01

Step 3: Circular- Shift the two halves of the matrix

76	12	34	15	26	55	99	14
94	47	89	111	78	48	58	41
44	18	87	45	22	89	41	79
49	85	98	77	45	41	97	99
47	11	54	165	94	19	22	44
17	46	41	66	41	25	24	11
44	18	94	92	77	56	129	41
11	07	01	98	01	24	26	27

Step 4: Divide the two parts of the matrix into halves.

76	12	34	15	26	55	99	14
94	47	89	111	78	48	58	41
44	18	87	45	22	89	41	79
49	85	98	77	45	41	97	99
47	11	54	165	94	19	22	44
17	46	41	66	41	25	24	11
44	18	94	92	77	56	129	41
11	07	01	98	01	24	26	27

Step 5: Encrypted matrix.

12	76	15	34	55	26	14	99
47	94	111	89	48	78	41	58
18	44	45	87	89	22	79	41
85	49	77	98	41	45	99	97
11	46	165	54	19	94	44	22
46	17	66	41	25	41	11	24
18	44	92	94	56	77	41	129
07	11	98	01	24	01	27	26

4. PERFORMANCE MEASURES

- **Correlation**

An important aspect of similarity measure is image matching. Image matching has many applications some of them being facial recognition, tracking, classification and change detection [5]. Correlation is one of the image matching technique that is widely used. Correlation helps find similarity between two images by comparing the pixel's neighborhood [5]. In this paper correlation helps find the degree of similarity between the original image and restructured image i.e. the one obtained after encryption and decryption.

The Pearson coefficient is one of the ways to measure correlation. It is given by

$$r = \frac{n(\sum xy)-(\sum x)(\sum y)}{\sqrt{[n\sum x^2-(\sum x)^2]}\sqrt{[n\sum y^2-(\sum y)^2}} \quad (2)$$

Correlation coefficient r lies between -1 & 1. Where r = –1 indicates a strong negative relationship between x & y and r = 1 indicates a strong positive association between x & y. r = 0 indicates that x & y are not related at all [6].

- **Root Mean Square Error**

The equation of root mean square error is as follows [7]

$$e_{rms} = \sqrt{\frac{\sum_{j=1}^{n}(\bar{x}_j - x_j)^2}{n}} \quad (3)$$

Where $\bar{x}_j$ is the j[th] pixel of the restructured image

x_j is the j[th] pixel of the original image

n is the total number of pixels

- **Peak Signal-To-Noise Ratio**

PSNR is used for quality detection of the reconstructed image; higher value of PSNR is an indicator of better quality of the reconstructed image [7].

PSNR is given by $10\log_{10}\frac{R^2}{MSE}$ (4)

- **Entropy**

Entropy of an image is based on different grey levels that image contains.[8] Entropy is higher for an image with more number of grey levels and is lower if the image has less grey levels. If all the pixels are saturated at a particular grey level then the entropy is zero.[9]

Entropy also is a measure of information content so an image with higher entropy value holds more information. Another important characteristic is that scrambling an image doesn't change its entropy. Shannon's entropy [10] is given as

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (5)$$

5. EXPERIMENTAL RESULTS

The correlation results for row-wise & column-wise algorithm are given in Table 1 & 2 respectively. The correlation between the original image and the decrypted image is 0.99 and suggests that the images are strongly correlated. In the tables each iteration further divides the image into halves and circular shifts those halves. The Entropy of the original image was calculated to be 7.4455. The Entropy of the original and restructured image is nearly same according to the table data and hence there is negligible information loss.

The image 3(a) is the original 512×512 image. 3(b) to 3(g) are row-wise encrypted images and Figure 4(a) to 4(d) are column wise circular shifted in both the cases the number of iterations depict the number of halves the image is divided into. In the 1st iteration an outline of the original image is visible but as the number of iterations increase the obscureness of the image increases

Table 1: The following table shows the Correlation, Root Mean Square Error (RMSE), and Peak Signal to Noise Ratio (PSNR) results corresponding to row circular-shifted image.

After iteration	Correlation	RMSE	PSNR
1	0.9976	3.5497	37.1269
2	0.9973	3.7360	36.6827
3	0.9979	3.2871	37.7944
4	0.9987	2.6819	39.5619
5	0.9987	2.6977	39.5109
6	0.9988	2.5491	40.0031
7	0.9988	2.5633	39.9548
8	0.9989	2.5367	40.0453
9	0.9990	2.4223	40.4461
10	0.9990	2.4223	40.4461

Table 2: Entropy of the original, encrypted and restructured image for 10 iterations. The results correspond to row circular-shifted image.

After iteration	Entropy of Original image	Entropy of Scrambled image	Entropy of Decrypted image
1	7.4482	7.5393	7.4370
2	7. 4482	7.5445	7.4405
3	7. 4482	7.5563	7.4430
4	7. 4482	7.5692	7.4434
5	7.4482	7.5685	7.4435
6	7.4482	7.5715	7.4438
7	7.4482	7.5715	7.4436
8	7.4482	7.5719	7.4436
9	7.4482	7.5735	7.4437
10	7.4482	7.5735	7.4437

Table 3: The following table shows the Correlation, Root Mean Square Error (RMSE), and Peak Signal to Noise Ratio (PSNR) results corresponding to column circular-shifted image.

After iteration	Correlation	RMSE	PSNR
1	0.9976	3.5264	37.1842
2	0.9976	3.4819	37.2944
3	0.9980	3.2080	38.0060
4	0.9983	3.0249	38.5166
5	0.9987	2.6781	39.5744
6	0.9988	2.5839	39.8853
7	0.9987	2.6366	39.7099
8	0.9988	2.6105	39.7964
9	0.9988	2.5841	39.8848
10	0.9988	2.5841	39.8848

Table 4: Entropy of the original, encrypted and restructured image for 10 iterations. The results correspond to column circular-shifted image.

After iteration	Entropy of Original image	Entropy of Scrambled image	Entropy of Decrypted image
1	7.4482	7.5403	7.4363
2	7.4482	7.5447	7.4392
3	7.4482	7.5490	7.4402
4	7.4482	7.5566	7.4415
5	7.4482	7.5662	7.4419
6	7.4482	7.5661	7.4410
7	7.4482	7.5660	7.4414
8	7.4482	7.5661	7.4407
9	7.4482	7.5653	7.4410
10	7.4482	7.5653	7.4410

Figure 3(a): Original image

Figure 3(b):Row-wise encryptedimage after 1 iteration.

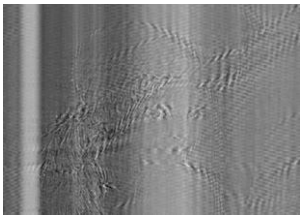

Figure 3(c): Row-wise encryptedimage after 2 iterations.

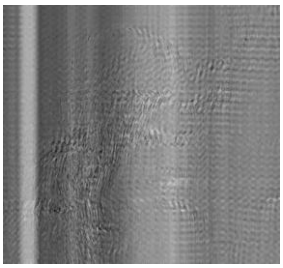

Figure 3(d): Row-wise encryptedimage after 3 iterations.

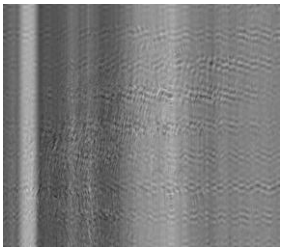

Figure 3(e): Row-wise encrypted image after 4 iterations.

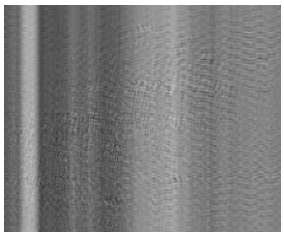

Figure 3(f): Row-wise encrypted Image after 5 iterations

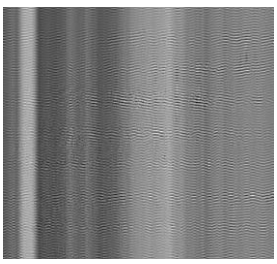

Figure 3(g):Row-wise encrypted image after 10 iteration.

Figure 3(h): Image obtained afterdecryption.

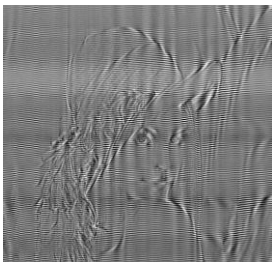

Figure 4(a): Column-wise encrypted image after 1 iterations.

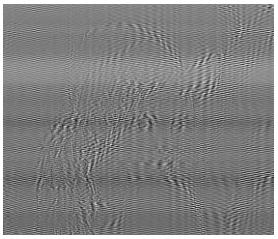

Figure 4(b): Column-wise encryptedimage after 2 iterations.

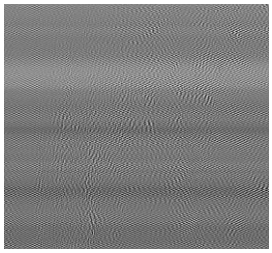

Figure 4(b): Column-wise encrypted Image after 3 iterations.

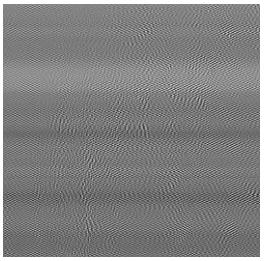

Figure 4(c): Column-wise encrypted image after 5 iterations.

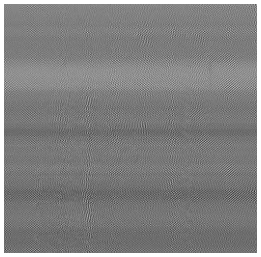

Figure 4(c): Column-wise encrypted image after 10 iterations.

Figure 4(e): Image obtained after Decryption.

6. CONCLUSION

Thus the novel approach to image encryption presented by this paper using circular shift is a secure and efficient method for encryption of images. The correlation and entropy values obtained verify that the image obtained after decryption suffers negligible loss and matches the original image to a greater extent. Also applying sinusoidal transform provides security to the algorithm and reduces chances of it being hacked. The algorithm is also simple to use and gives a higher degree of accuracy.

7. REFERENCES

[1] John Justin M, Manimurugan S., "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[2] Rinki Pakshwar, Vijay K. Trivedi, Vineet Richhariya, " A Survey on Different Image Encryption and Decryption Techniques", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 4 (1), 2013, 113 – 116

[3] Nicholas J. Daras, Michael Th. Rassias Computation, Cryptography, and Network Security Springer, 16-Sep-2015

[4] H. B. Kekre, Tanuja Sarode, Pallavi N. Halarnkar & Debkanya Mazumder, "Comparative Performance of Image Scrambling in Transform Domain using Sinusoidal Transforms", International Journal of Image Processing (IJIP), Vol. 9, issue 2, 2014.

[5] Tai-hoon Kim, Hojjat Adeli, Carlos Ramos, Byeong-Ho Kang Springer, "Signal Processing, Image Processing and Pattern Recognition: International Conferences, SIP 2011, Held as Part of the Future Generation Information Technology Conference, FGIT 2011, in Conjunction with GDC 2011, Jeju Island, Korea, December 8-10, 2011. Proceedings", 02-Dec-2011

[6] Mintu Philip, "An Enhanced Chaotic Image Encryption", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, Dec 2011

[7] Hala Bahjat, May A.Salih, "Dynamic Shuffling for Speed Image Encryption", International Journal of Computer Applications (0975-8887), Vol. 89, No. 7, March 2014

[8] Sowmyashree, R.R. Sedamkar, "A Hybrid Approach for Secure Data Communication using Reversible Data Hiding and Image Encryption", International Journal of Current Engineering and Technology, Vol. 4, No. 6, Dec 2014

[9] Dr. H.B. Kekre, Sudeep D. Thepade, Tanuja K. Sarode, Vashali Suryawanshi, "Image Retrieval using Texture Features extracted from GLCM, LBG, KPE", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October 2010, 1793-8201.

[10] Yue Wu, Yicong Zhou, George Saveriades, Sos Agaian, Joseph P. Noonan, Premkumar Natrajan, "Local Shannon entropy measure with statistical tests for image randomness", Information Sciences, Vol. 222, February 10, 2013, Pages 323-342.