International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.279-288
http://dx.doi.org/10.14257/ijsia.2015.9.12.26

An Efficient Image Cryptographic Algorithm based on Frequency Domain using Haar Wavelet Transform

Kalyani Mali[1], Shouvik Chakraborty[*2], Arindrajit Seal[3], and Mousomi Roy[4]

[1]*Professor and Head, Department of CSE,*
University of Kalyani, Nadia, WB, India
[2,3,4]*P.G. Student, Department of Computer Science & Engineering,*
University of Kalyani, West Bengal, India
[1]*kalyanimali1992@gmail.com,* [2]*shouvikchakraborty51@gmail.com,*
[3]*arindrajit.seal@gmail.com,* [4]*iammouroy@gmail.com*

Abstract

Presently a number of techniques are used to restrict confidential image data from unauthorized access. In this paper, the authors have proposed an efficient lossless image cryptographic algorithm to transmit pictorial data securely. Initially we take a 64 bit key, we convert our decimal pixel value into binary 8 bits and we XOR the first 8 bits of the key with the pixel value. After that we take the next 8 bits of the key and XOR with the next pixel value. We perform the circular right shit operation when the key gets exhausted. We perform the first level haar wavelet decomposition thereafter. Dividing the LL1 into four equal sections we perform some swapping operations. Decryption follows the reverse of the encryption .Evaluation is done by some parametric tests which includes correlation analysis, NPCR, UACI readings etc. show that the proposed work is resilient and robust in the field of cryptography.

Keywords: *Image cryptography, Haar wavelet transforms, Lossless encryption, Frequency domain*

1. Introduction

For a long time many algorithms have been developed to encrypt images in the frequency domain. In image based transformations the entire image pixels are transformed and in block-based transformations, the pixels of the image are divided into number of blocks of similar sizes and then every block is operated independently. An example of block-based transform methods: Tedmori and Al-Najdawi [1] presented a lossless image cryptography technique where they proposed the encryption algorithm using the discrete cosine transform converting the original image into the frequency domain. The algorithm is designed to reverse the sign and shuffle off each frequency in the transformed domain. Tang [2] proposed the zigzag permutation method applied on the transformed block obtained by the result of the discrete cosine transform. Liu *et al*. [3], proposed a triple image encryption method using Fractional Fourier Transform. Samson and Sastry [4] proposed an image encryption procedure by lossy compressions using multilevel wavelet transform where encryption is carried out using multilevel 2-D Haar by decomposing the compressed image. Wavelet Transform. The frequency domain processing methods that are based on processing and modifying the frequencies of an image, the image pixels can be recovered completely via an inverse process without loss of any information. Therefore, frequency based approaches are clearly suitable.

In this paper, a bit level manipulation of the image is used. In order to tighten the security another layer of encryption is used which is the 'haar' wavelet transform. The

Shouvik Chakraborty is the corresponding author

ISSN: 1738-9976 IJSIA

proposed algorithm is simple, robust, effective, lossless and secure. In comparison to other cryptographic techniques, the proposed work in this paper is completely lossless and it preserves every minute detail of the image.

2. Haar Wavelet Transform

The main goal of image transformation is to reduce the correlation in the transformed image so that it is indecipherable. The discrete wavelet transform is any wavelet transform (such as Daubechies wavelets, Haar wavelet, the Dual-Tree Complex Wavelet Transform), where the wavelets are discretely sampled. The primary advantage it has over block based transforms, is temporal resolution, where it captures both frequency and spatial information. In this paper, the Haar wavelet is used. The Haar transform is one of the oldest transform functions, proposed by a Hungarian mathematician Alfred Haar in 1910. It is found to be effective in applications such as signal and image compression in electrical and computer engineering. The Haar transform is derived from the Haar matrix. An example of a 4x4 Haar transformation matrix is shown in Figure 1.

1	1	1	1
1	1	-1	-1
$\sqrt{2}$	$-\sqrt{2}$	0	0
0	0	$\sqrt{2}$	$-\sqrt{2}$

Figure 1. The 4X4 Haar Transformation Matrix

The Haar transform can be thought of as a sampling process in which rows of the transformation matrix acts as samples of finer resolution.

The basic operation of a discrete wavelet transform when applied to a 2D discrete signal containing N × N samples is as follows: each row of a 2D image is filtered with a low-pass and a high-pass filter (Lx and Hx) and the output of each filter is down-sampled by a factor of two to produce the transient images L and H. L is the original image low-pass filtered and down-sampled in the x-direction and H is the original image high-pass filtered and down-sampled in the x direction. After that, each column of these new images is filtered with low-and high-pass filters (h L and h H) and down-sampled by a factor of two to produce four sub-images (LL, LH, HL and HH) as shown in Figure 2.

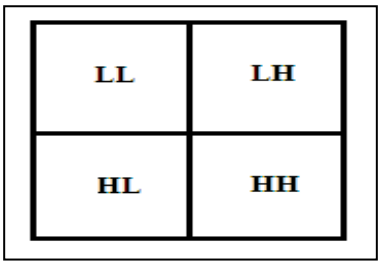

Figure 2. The Haar Wavelet decomposition

These four ‘sub-band’ images can be combined to create an output image with the same number of samples as the original. ‘LL’ is the original image, low-pass filtered in horizontal and vertical directions and sub-sampled by a factor of 2. ‘HL’ is high-pass filtered in the vertical direction and contains residual vertical frequencies, ‘LH’

is high-pass filtered in the horizontal direction and contains residual horizontal frequencies and 'HH' is high-pass filtered in both horizontal and vertical directions. The four sub-band images contain all of the information present in the original image and we achieve the act of compression of the original image. An example of the Haar wavelet transform of first level is given in Figure 3.

Figure 3. Example of First Level Haar Wavelet Transform (Original Image of Lena is in the Left and Image Produced by Haar Wavelet Decomposition is in the Right)

3. Proposed Algorithms

3.1. Encryption Algorithm

The process starts off by choosing a 64 bit key initially. This is essentially a symmetric key encryption algorithm. At first convert a pixel value into the binary. Then take the first 8 bits from the key and perform a bitwise XOR operation with the binary value of the pixel. After getting a result, invert the binary sequence and computes the corresponding decimal value of the binary sequence. This is the new value of the pixel. For the next pixel, the remaining next 8 bits of the key is used. For all pixels perform a similar operation. This process goes on until the key gets exhausted. After that we perform a right circular shift of 8 bits and we continue the process. The circular shift reduces the chance of generating the same sequences for the same pixel value. After all the pixels are manipulated by this approach, perform the 'Haar' wavelet transform dividing the image into four bands namely LL1, LH1, HL1, HH1. Diminishing of LL1 is done by dividing by (mxn) where m is the number of rows of LL1 and n is the number of columns of LL1. This stem reduces the intensity if the pixel value. In the next step, divide the LL1 bands into four equal sections clockwise reading 1,2,3,4 and then swap section 2 with the 2nd section of LH1, section 3 with the 3rd section of HL1 and section 4 with the 4th section of HH1. This step is helpful for reducing the correlation coefficients. In the next step perform a sign reverse operation of LH1, HL1 & HH1 by multiplying by -1. Now swap the contents of LL1 with HL1 and LH1 with HH1. Lastly perform the Inverse Haar wavelet transform. In this step, image frequencies are transformed back into the pixel domain. The encryption algorithm is given below:

Step 1: Choose a 64 bit key and for each pixel perform steps 2 to 4.
Step 2: Inverse the bits of the result obtained after XOR operation and assign the corresponding decimal value to that pixel.
Step 3: For the next pixel take the next 8 bits of the key and so on. When the key gets exhausted perform a circular right shift of 8 bits and then continue.
Step 4: Perform the 1st level Haar wavelet decomposition.
Step 5: Diminish LL1 by the size of the LL1.
Step 6: Divide the LL1 into equal four sections. Swap section 2 with the section 2

of LH1, section 3 with the section 3 of HL1, section 4 with the section of HH1.

Step 7: Reverse the signs of LH1, HL1, and HH1.

Step 8: Swap the contents of LL1 with HL1 and LH1 with HH1.

Step 9: Perform the 1st level Inverse Haar wavelet transform.

3.2. Decryption Algorithm

The decryption process follows exactly the opposite of the encryption process. Initially perform the first level of 'Haar' wavelet decomposition. Then perform a swapping operation as follows: LL1 with HL1 and LH1 with HH1. Next up reverse the sign of LH1, HL1, HH1 by multiplying by -1. We divide the LL1 into four sections clockwise reading 1,2,3,4. We again perform a swapping operation. We swap section 2 with the section 2 of LH1, section 3 with the section 3 of HL1, section 4 with the section 4 of HH1. In the next step, multiply by LL1 by (mxn) to restore the pixel intensity of the LL1 matrix. Now perform the 1st level Inverse 'Haar' Wavelet Transform. In this step, image frequencies are transformed back into the pixel domain. After that, take a pixel and convert its value into eight bit binary sequence and invert it. Now, take the same 64 bit key that is used for encryption. The inverted value of the bit sequence of the pixel is XOR-ed with the 8 bits of the 64 bit key. The resultant value is converted into decimal and assigned as the original value of the pixel. For the next pixel take the next 8 bits of the key and so on. When the key gets exhausted perform a circular right shift of 8 bits and then continue. The process must continue for all the pixels. When all pixels go through by this process then the encrypted image gets completely decoded. Using the proposed encryption/decryption algorithm, the pixels of decrypted image will have the same values like the original image as shown in the following sections. So, it is a completely lossless operation. The decryption algorithm is given below.

Step 1: Perform the 1st level Haar wavelet decomposition.

Step 2: Swap the contents of LL1 with HL1 and LH1 with HH1.

Step 3: Reverse the signs of LH1, HL1, and HH1.

Step 4: Divide the LL1 into equal four sections. Swap section 2 with the section Section 2 of LH1, section 3 with the section 3 of HL1, section 4 with the Section 4 of HH1.

Step 5: Restore LL1 by the size of the LL1.

Step 6: Perform the 1st level Inverse Haar wavelet transform.

Step 7: Take the 64 bit key and for each pixel perform steps 8 to 10.

Step 8: Take a pixel and find the eight bit binary sequence it and make it inverse.

Step 9: Take the inverted bits of the pixel and perform XOR operation with the 8 bits of the key and assign the corresponding decimal value to that pixel.

Step 10: For the next pixel take the next 8 bits of the key and so on. When the key gets exhausted perform a circular right shift of 8 bits and then continue.

4. Experimental Results and Analysis

The main goal of the image cryptographic algorithms is to produce a image that is difficult to understand. The quality of the image may degrade. The algorithm proposed in this paper degrades the image quality during the encryption technique but at the end of the decryption, the original image is restored. Automated quality measurement methods that are based on mathematical and computational algorithms are necessary because of the variability and inconsistency between human observers. The quality of the image is assessed by some parameters. In the following sections, details of the different parameters along with the results are given.

4.1. Correlation Co-efficient

Correlation coefficients have been tested in three different direction *i.e*. horizontal, vertical and diagonal. Correlation coefficients are calculated for the selected pairs using Equation 1 [3].

$$R_{xy} = COV(xy)/\sqrt{D(x)}\sqrt{D(y)} \quad (1)$$

Where,

$$COV(xy) = \frac{1}{T}\sum_{i=1}^{T}((x_i - E(x))(y_i - E(y))) \quad (2)$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i \, , E(y) = \frac{1}{T}\sum_{j=1}^{T} y_j \quad (3)$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x_i)\right)^2 \, , D(y) = \frac{1}{T}\sum_{i=1}^{T}\left(y_i - E(y_i)\right)^2 \quad (4)$$

where x, and y in the above equations are the gray-scale values of the two adjacent pixels in the image, and T is the total pair of pixels randomly selected from the image. Table 1 provides the comparison of proposed approach and some other benchmark approaches. Table 2 shows the results obtained from proposed approach on some standard images.

Table 1.Comparison of Correlation Coefficients in Original and Encrypted images

Encryption Method	Test Image	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
Proposed	Lena	0.946	0.0064	0.973	0.0218	0.921	0.0028
	Lake	0.958	0.0014	0.958	0.0048	0.929	0.0033
Tedmori and Najdawi [5]	Lena	0.919	0.0023	0.927	0.0042	0.962	0.0053
	Lake	0.987	0.0025	0.936	0.0015	0.927	0.0105
Ye [6]	Lena	0.904	0.0020	0.903	0.0042	0.953	0.0088
	Lake	0.976	-0.0730	0.904	-0.0038	0.912	0.0191
Sethi and Sharma [7]	Lena	0.913	0.0031	0.920	0.0049	0.925	0.0062
	Lake	0.942	-0.0016	0.922	0.0036	0.887	0.0144
Huang and Nien [8]	Lena	0.916	0.0058	0.929	0.0092	0.946	0.0058
	Lake	0.982	0.0074	0.898	0.0084	0.924	0.0146

Table 2.Correlation Coefficients in Original and Encrypted Images based on the Proposed Encryption Algorithm Results

Test Image	Horizontal			Vertical			Diagonal		
	Org	Enc	Dec	Org	Enc	Dec	Org	Enc	Dec
Lena	0.946	0.006	0.946	0.973	0.022	0.973	0.921	0.003	0.921
Lake	0.958	0.001	0.958	0.958	0.005	0.958	0.929	0.003	0.929
Living-Room	0.927	0.007	0.927	0.935	0.008	0.935	0.877	0.000	0.877
Pirate	0.943	0.007	0.943	0.956	0.006	0.956	0.913	0.002	0.913
Peeper	0.967	0.001	0.967	0.973	0.013	0.973	0.943	0.006	0.943
Jetplane	0.940	0.005	0.940	0.933	0.004	0.933	0.888	0.001	0.888
House	0.985	0.013	0.985	0.981	0.269	0.981	0.968	0.019	0.968
Cameraman	0.956	0.003	0.956	0.974	0.020	0.974	0.934	0.011	0.934
Mandril	0.874	0.005	0.874	0.836	0.005	0.836	0.795	0.000	0.795
Hestain	0.946	0.007	0.946	0.952	0.006	0.952	0.905	0.009	0.905
Walkbridge	0.940	0.003	0.940	0.919	0.002	0.919	0.885	0.001	0.885
Woman Darkhair	0.991	0.012	0.991	0.993	0.026	0.993	0.986	0.013	0.986

4.2. PSNR

PSNR is an abbreviation for Peak Signal to Noise Ratio. PSNR is a well-known parameter and can be computed from Equation 5 [10]. The PSNR results in an undefined value under one condition only; *i.e*., when the original image is compared to itself. In this case the MSE value in the denominator part of the Equation 5 would result in a zero value, and hence, a division by zero situation occurs).

$$PSNR = 10 \log_{10}\left(\frac{L^2}{MSE}\right) \quad (5)$$

Where

$$MSE = \frac{1}{N}\sum_{i=0,j=0}^{N,N}\left(x_{ij} - y_{ij}\right)^2 \quad (6)$$

N is the number of pixels in the frame, and xij, yij are the ith and jth pixels inthe original and processed frames, respectively. L is the dynamic range of pixel values (L is 0 to 255 for gray-scale images).

Table 3 provides the comparison of proposed approach and some other benchmark approaches. Table 4 shows the results obtained from proposed approach on some standard images.

Table 3. Comparison of PSNR Values

Test Image	Proposed		Tedmori and Najdawi [5]		Samsom and Sastry [4]		Sethi and Sharma [7]		Huang and Nien [8]	
	O-D	O-E	O-D	O-E	O-D	O-E	O-D	O-E	O-D	O-E
Lena	Undefined	0.0069	Undefined	0.0017	40.22	0.113	69.70	0.036	45.78	0.154
Lake	Undefined	0.0063	Undefined	0.0043	33.49	0.098	43.65	0.072	51.83	0.127

Table 4. PSNR Values of Some Standard Images Obtained Using Proposed Approach

Test Image	PSNR	
	O-D	O-E
Lena	Undefined	0.0069
Lake	Undefined	0.0064
Living-Room	Undefined	0.0073
Pirate	Undefined	0.0078
Peeper	Undefined	0.0073
Jetplane	Undefined	0.0039
House	Undefined	0.0058
Cameraman	Undefined	0.0068
Mandril	Undefined	0.0073
Hestain	Undefined	0.0055
Walkbridge	Undefined	0.0074
Woman Darkhair	Undefined	0.0075

4.3. Differential Attacks: NPCR and UACI

To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity(UACI). NPCR and UACI can be defined using Equation 7 and Equation 8 respectively [6].

$$NPCR = \frac{\sum_{i=j=1}^{m,n} D(i,j)}{w \times h} \times 100\% \quad (7)$$

$$UACI = \frac{1}{w \times h}\left[\sum_{i,j}^{m,n} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (8)$$

Where C1 and C2 are two encrypted images corresponding to two original images with subtle change *i.e.*, one pixel difference. w,h are the image width and height , D(i, j) is a bipolar array with the same size as image C1 ,D(i, j) is determined using on Equation 9 [11].

$$D(i,j) = \begin{Bmatrix} 1\ if\ C_1(i,j) = C_2(i,j) \\ 0\ Otherwise \end{Bmatrix} \quad (9)$$

Table 5 provides the comparison of proposed approach and some other benchmark approaches. Table 6 shows the results obtained from proposed approach.

Table 5. Comparison of NPCR and UACI Values

Test Image	Proposed		Tedmori and Najdawi [5]		Ye [6]		Sethi and Sharma [7]		Huang and Nien [8]	
	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%	NPCR%	UACI%
Lena	99.832	39.720	99.941	38.981	99.105	36.241	95.124	20.113	99.214	27.481
Lake	99.785	40.703	99.953	40.874	98.642	37.121	34.124	98.642	98.349	27.628

Table 6. NPCR and UACI Values of Some Standard Images Obtained Using Proposed Approach

Test Image	Proposed Approach	
	NPCR	UACI
Lena	99.832%	39.720%
Lake	99.785%	40.703%
Living-Room	99.805%	38.468%
Pirate	99.796%	35.306%
Peeper	99.825%	37.261%
Jetplane	99.953%	59.872%
House	99.826%	44.722%
Cameraman	99.811%	39.543%
Mandril	99.817%	38.541%
Hestain	99.925%	48.949%
Walkbridge	99.762%	36.354%
Woman Darkhair	99.706%	34.706%

4.4. Histogram

The histogram of the encrypted images is significantly different from the histogram of the original images (left-shifted) and hence it does not provide any useful information to perform any statistical analysis attack on the encrypted image.

Figure 4 shows an example of plotting the histogram of the original, encrypted, and decrypted along with the correlation coefficients.

Figure 5 to Figure 6 shows some of the results of the proposed encoding/decoding algorithms are given. These results are obtained by applying proposed method on some standard test images.

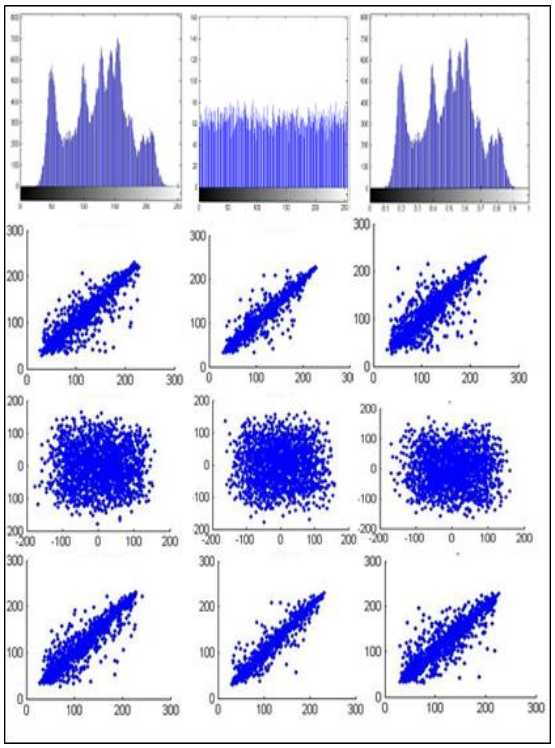

Figure 4. In the First Row Histogram Representation of the Lena Standard Image (from Left to Right: Original, Encrypted and Decrypted), From Second Row-, Top to Bottom: Correlation Coefficients of Original, Encrypted and Decrypted, Left to Right: Correlation Coefficients in Horizontal, Vertical and Diagonal Directions

Figure 1. From Top to Bottom, Standard Images "Lena", "Cameraman" and "Hestain" , from Right to Left, the Figure Present the Original, Encrypted and Decrypted Algorithms Results

Figure 2. From Top to Bottom, Standard Images "Peeper", "Lake" and "Mandril", from Right to Left, the Figure Present the Original, Encrypted and Decrypted Algorithms Results.

5. Conclusion

This proposed work is based on image manipulation at the spatial domain as well as on the frequency domain. Encryption is simple and the decryption follows exactly the opposite of the encryption. The reason why we have assimilated two image encryption techniques is to make our approach stronger in comparison to the contemporary approaches available in present times. We have incorporated the boons of two the best approaches in order to make our approach a standout and also to put in a two level security. This makes our approach resilient, robust and cogent enough in comparison to the other approaches available. We have also used some parameters to test the viability of the approach and it has been found to be satisfactory. Various security and statistical analysis tests are carried out in order to evaluate the robustness of the proposed work. Results are compared against benchmark algorithms and show the effectiveness of the proposed work.

References

[1] S. Tedmori and N. Al-Najdawi, "Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform", Int. Arab J. Inf. Technol., Vol. 9, No. 5, **(2012),** pp. 471-478.
[2] L. Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", in ACMMultimedia, **(1996),** pp. 219–229.
[3] Z. Liu, J. Dai, X. Sun and S. Liu, "Triple image encryption scheme in fractional Fourier transform domains", Elsevier Optics Commun., Vol. 282, No. 4, **(2009),** pp. 518-522.
[4] C. Samson and V. Sastry, "A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform", Int.l J. of Advanced Comput. Sci. App, Vol. 3, No. 9, **(2012),** pp. 178-183.
[5] S. Tedmori and N. Al-Najdawi, "Image Cryptographic Algorithm Based on the Haar Wavelet Transform", Elsevier Information SciencesVol. 269, **(2014)**, pp. 21-34.
[6] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism", Elsevier Optics Commun., Vol. 284, **(2011),** pp. 5290-5298.
[7] N. Sethi and D. Sharma, "Novel Method of Image Encryption Using Logistic Mapping", Int. J. Comput. Sci. Eng.,Vol. 1, No. 2, **(2012),** pp. 115-119.
[8] C.K. Huang and and H. Nien, "Multi chaotic systems based pixel shuffle for image encryption", Elsevier OpticsCommun., Vol. 282, No. 11, **(2009),** pp. 2123-2127.
[9] I. Richardson, "H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia", JohnWiley & Sons, **(2003)**.

[10] S. Tedmori and N. Al-Najdawi, "Hierarchical Stochastic Fast Search Motion Estimation Algorithm", IET Comput.Vis., Vol. 6, No. 1, **(2012),** pp. 21-28.
[11] F. Sun, z. Lu and S. Liu, "A new cryptosystem based on spatial chaotic system", Elsevier Optics Commun., Vol. 283, No. 10, **(2010),** pp. 2066–2073.

Authors

Dr. Kalyani Mali. She is currently working as Professor and Head in the Computer Science & Engineering Department at University of Kalyani, West Bengal, India. She obtained M.Tech. in Computer Science from Calcutta University and received Ph.D in Engineering from Jadavpur University. Her area of interest in research is Pattern Recognition, Image Processing, Data Mining and Soft Computing.

Shouvik Chakraborty. He is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. He received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. His research interests include soft and evolutionary computing, bioinformatics, digital image processing and cloud computing.

Arindrajit Seal. He is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. He received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. His research interests include digital image processing and bioinformatics.

Mousomi Roy. She is pursuing M.Tech in Computer Science and Engineering from University of Kalyani, West Bengal, India. She received his B.Tech in Computer Science and Engineering from Hooghly Engineering & Technology College, West Bengal under West Bengal University of Technology, West Bengal, India. Her research interests include digital image processing and bioinformatics and cloud computing.

