Image Encryption using Curved Scrambling and Diffusion

Neha Dwivedi[*1], Rishi Kumar Gupta[*2], Shafali Agarwal[*3]
[*]Department of Computer Applications, JSSATE, Noida, India
nehadwivedi496@gmail.com[1]
agraharirishikumar@gmail.com[2]
shafali.agarwal@gmail.com[3]

***Abstract*- In the recent world, designing of a secure cryptosystem is prime focused area for the researchers. This paper emphasizes on the image encryption/decryption technique using a key derived from a plain image. In the proposed algorithm, encryption key is derived by applying new curved scrambling method to the RGB layers of a plain image. In next step, a temporary cipher image is obtained by modulo arithmetic using encryption key. To enhance security level, execute additional diffusion method to reset the pixel values within the given block and finally generate a cipher image. The described algorithm achieves a larger key space, good statistical property and effective resistance to the brute force attack thus provides highly secure cryptosystem for the real world applications.**

Keyword - Image encryption and decryption, curved scrambling, diffusion, security

I. INTRODUCTION

Now a day, a huge amount of data in terms of text, image, audio and video has to transmit over the network. An image carries lot of information compared to text hence importance of secure transmission of an image increases. Because of sensitivity of image data, enormous size, high correlation among pixels of images and strong redundancy of uncompressed data, traditional encryption methods are not suitable to achieve strong level of security of transmitted data. The requirement of such a system arises so that illegal acquisition, modification, alteration, copying and unauthorized accessing can be prevented and data must be transferred with original contents. In some systems, image transmission is an important tool to pass detailed information like medical imaging, military communication, scientific observation, health care, multimedia, picture messaging application on cell phone, biological data etc. An efficient, strong and reliable encryption method is required to achieve a secure transmission of confidential data over the network.

Image encryption is a technique used to convert original image into another image which is not identifiable by unauthorized user [1], [2]. This is a method of transferring the information embedded in a digital image to a non-recognizable form so that no one can access the data except those having details of decryption method with key required to decrypt the data.

An important tool in image encryption is scrambling deals with change in position of the pixels and helps to minimize the correlation coefficient value [3]. If correlation coefficient between original image and encrypted image is zero or near to zero, hacker will be unable to guess the encryption method or key. Recently authors [4] used DNA sequences as a secret key and implemented permutation process using Hao’s fractal representation. They also used diffusion and scrambling to make the encryption process more secure and complicated. There are remarkable methods available to achieve this such as steganography, water marking and cryptography. This paper focuses on implementing a cryptography method using new curved scrambling and diffusionprocess to encrypt/decrypt the digital images.

II. RELATED WORK

Authors designed a secure cryptosystem using diffusion and permutation in addition to multiple chaotic based circular mapping, provides a large number of secret keys and key dependent pixel value replacement [5]. Sometimes researchers analyzed the existing cryptographic algorithms [6] and suggested a better solution based on the outcome. Here in [7], cryptanalysis was carried out by the authors and concluded that the system is completely breakable under chosen plaintext attack. They suggested a more secure cryptosystem by introducing two additional phases i.e. pixel shuffling phase and pixel encoding phase. Further diffusion process with a combination of chaotic maps were used to encrypt RGB images in [8]. Authors used a 128-bit key to encrypt an image which is layered into red, green and blue channel. A repeated execution of diffusion, mixing and substitution process on each RGB layer resultant into a secure cryptosystem [9].

The author utilized the randomness of chaos in order to encrypt the images. They applied Henon map and Lorentz map for pixel shuffling and calculated the correlation coefficient between the original image and cipher image. Result shows that the proposed algorithm is best suited for a wireless communication using any single map [10]. In the paper [11] an external secret key is used to encrypt an image. Author applied both pixel substitution and pixel permutation process to get a secure cryptosystem. A feedback mechanism is applied to make it secure from the differential attack. Author generate encryption key sequence by utilizing piecewise linear chaotic map and proposed a stream cipher algorithm for colour image encryption based on on-time keys and robust chaotic maps [12]. A symmetric key image encryption algorithm is proposed by the author [13] in which additive and affine encryption technique using six schemes of key sequence derived from random sequence of cyclic elliptic curve points is discussed. The result concluded that the proposed cryptosystem is secure from statistical, brute-force and cryptanalytic attacks. A combination of one-time key based on crossover operator, chaos and secure hash algorithm (SHA-2) is employed to design a cryptosystem for the colour image encryption [14]. In the paper [15], the proposed encryption method utilized the magic rectangle in addition to traditional public key cryptography algorithm such as RSA.

III. PROPOSED METHOD

An algorithm is proposed to encrypt/decrypt a given image using another plain image. Before applying encryption function, images are converted into three matrices of red, green and blue color pixels respectively. The algorithm consists of two major steps to achieve higher level of security.

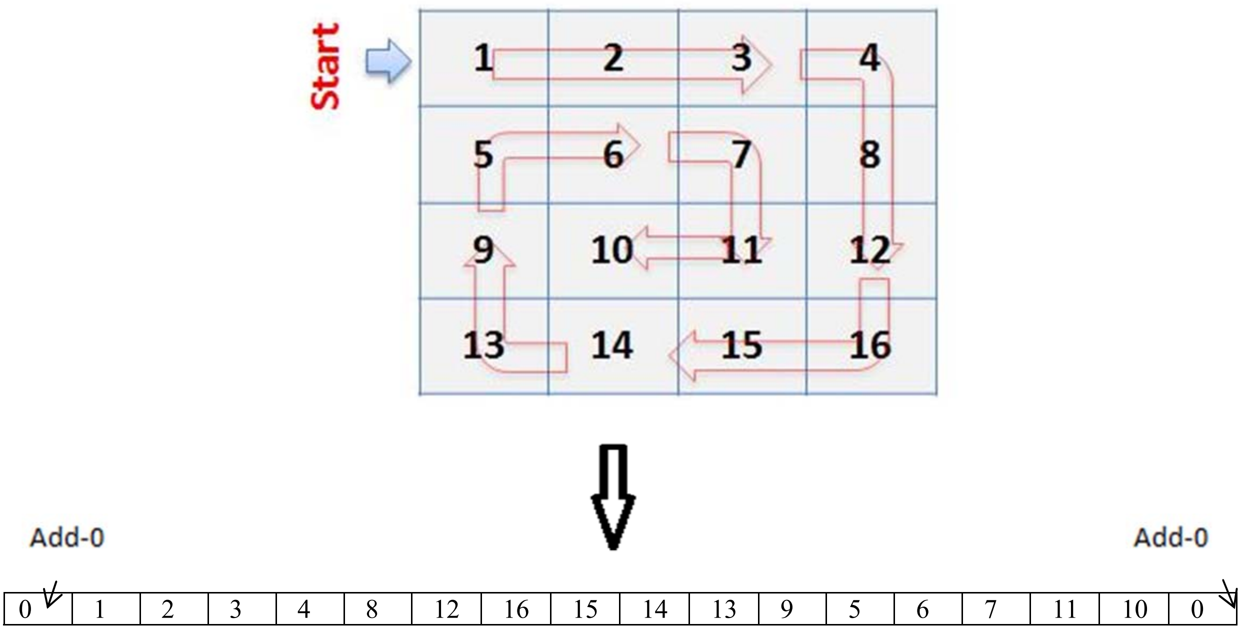
A. *Curved Scrambling*

Fig 1 displays that how curved scrambling process executes using eight bits' binary digits of each pixel value of image used to encrypt the given image.

The process of scrambling is as follows:

First convert the plain image into RGB intensity value, and then convertRGB matrix into R layer, B layer and G layer matrix separately.After that decode each element value of the matrix into binary number of eight bits. The process of curved scrambling executed on the bit value of each and every pixel of all three layers independently. Let's assume for R layer the current pixel value is X, the previous pixel (backward) value of the current pixel value is Y and the next pixel (forward) value of the current pixel value is Z. Add extra index having value zero(0) with the first and last index of the matrix for making calculation easy of forward and backward pixel values.

R layer matrix-



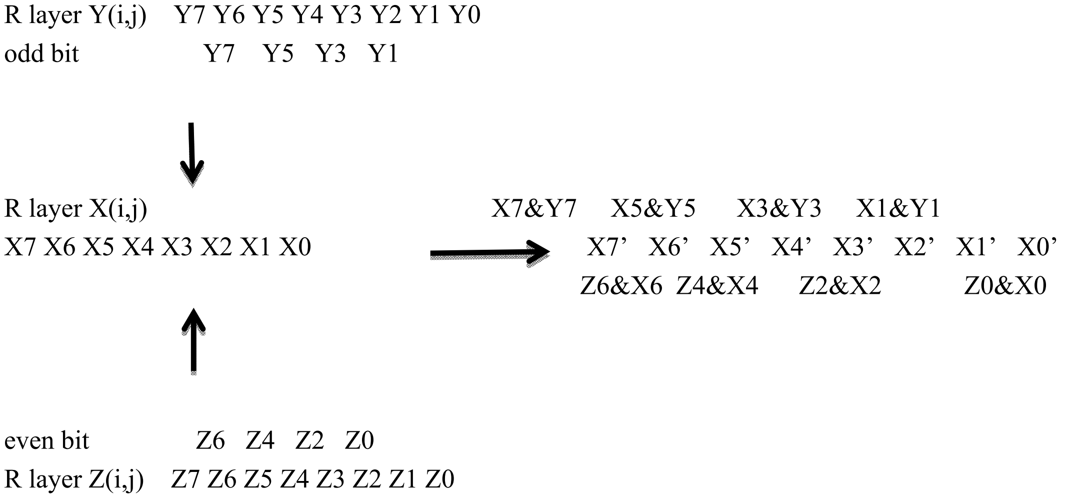
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

0	1	2	3	4	8	12	16	15	14	13	9	5	6	7	11	10	0

Index-0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Fig. 1. Pictorial representation of curved scrambling process

The bit values of pixels X, Y, and Z in R layer are denoted by (*X7 X6 X5 X4 X3 X2 X1 X0*), (*Y7 Y6 Y5 Y4 Y3 Y2 Y1 Y0*) and (*Z7 Z6 Z5 Z4 Z3 Z2 Z1 Z0*) respectively. In the process, the odd bits of X are calculated through an AND operation with Y, and the even bits of X are calculated in the same way with Z. After completion, the bit values of pixel X in R layer are reset.



R layer Y(i,j) Y7 Y6 Y5 Y4 Y3 Y2 Y1 Y0
odd bit Y7 Y5 Y3 Y1

R layer X(i,j)
X7 X6 X5 X4 X3 X2 X1 X0

X7&Y7 X5&Y5 X3&Y3 X1&Y1
X7' X6' X5' X4' X3' X2' X1' X0'
Z6&X6 Z4&X4 Z2&X2 Z0&X0

even bit Z6 Z4 Z2 Z0
R layer Z(i,j) Z7 Z6 Z5 Z4 Z3 Z2 Z1 Z0

Fig. 2. Curved scrambling process

The used function is:

$$Xi = \begin{cases} Xi\ and\ Yi\ where\ i = 1,3,5,7 \\ Zi\ and\ Xi\ where\ i = 0,2,4,6 \end{cases} \qquad \text{Eq(1)}$$

For example, let the current pixel value of X in R layer is 142 *i.e.* 10001110 in binary, Y is the backward pixel having value 178 i.e.10110010 in binary and Z is forward pixel having value 75*i.e.* 01001011 in binary. Now after applying Equation (1), we will get new value of X *i.e.*130 in decimal. Update the new value of X in the R layer with of current value of X. Similarly continue the process for each pixel value in R layer as well as for pixels of G layer and B layer matrices.

B. *Encryption with Diffusion*

After applying curved scrambling to the plain image, obtained image will be treated as encryption key to encrypt the given image. The following equation is used to encrypt the plain image with the scrambled encryption key and got the temporary cipher image

$$e'_{ij} = (e_{ij} + d_{ij})\ mod\ l\text{Eq(2)}$$

where e_{ij} is the pixel value of (*i,j*) coordinate of given image, d_{ij} is pixel value of scrambled image and e'_{ij} is pixel value of temporary cipher image which is obtained after encryption process. The color of used image in this experiment is 256-color *i.e.l*=256.

Diffusion process is nothing but rearrangement of the pixels by performing some calculations within the block so that an unauthorized person could not be able to access the information in transit.

The process starts with the RGB matrices of temporary cipher image obtained in the previous step. In this phase encrypted cells of previous and current matrices are XOR-ed with one-another according to given function.

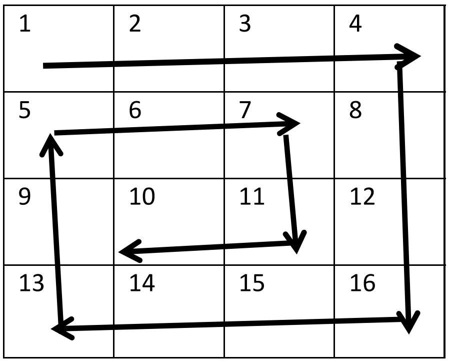
Encryption Function: Cell C' can be obtained from Cell C as,

$$Cell\ C' = \begin{cases} Cell\ C\ XOR\ Cell(C-1)', & If C! = 1 \\ Cell\ C, & If\ C = 1 \end{cases} \qquad \text{Eq(3)}$$

Example:

The sequence of applying diffusion process and corresponding output is depicted in the given fig 3.

Before XOR Operation **After XOR Operation**



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1	3	0	4
16	22	17	12
21	16	26	0
28	17	31	16

Fig.3. Diffusion Process

Start with the first pixel value of cell C *i.e.*1, so according to given function the value of cell C' will be same as cell C. Next pixel value from left to right in the cell C is 2, after calculation the value of cell C' will be 3 *i.e.* 00000010XOR00000001. Likewise, all values will be calculated for the given layer as well as for the other two layers according to given sequence.

C. Decryption

At the receiver end, decryption process is implemented just reverse of encryption process because of symmetric nature of algorithm. The decryption process starts with the anti-diffusion in the reverse direction and the function used is:

$$Cell\ C = \begin{cases} Cell\ C'\ XOR\ Cell(C-1)', & If C! = 1 \\ Cell\ C', & If\ C = 1 \end{cases}$$

Eq(4)

After successfully applying the above function, Cell C is obtained from Cell C' which is the temporary cipher image. Next step is to execute reverse modulo operation to get the actual given image. The equation is as follows:

$$e_{ij} = (e'_{ij} - d_{ij})\ mod\ l \text{Eq(5)}$$

IV. ALGORITHM

The encryption and decryption process can be stated in the following steps:

(1) Select a plain image which will be used to generate encryption key and a given image which is to be transmitted in encrypted form and then enlarge both images to the size of *M**N*.

(2) Convert both images into three layer matrices *i.e.* red, green and blue and represent each pixel to its eight bits' form (binary).

(3) Apply curved scrambling process to the plain image pixels and generate key used to encrypt the given image.

(4) Encrypt the given image by modulo operation with the encryption key obtained from the previous step.

(5) Execute diffusion process to the obtained temporary cipher image and finally got a cipher image.

(6) To decrypt, perform anti-diffusion to the cipher image in reverse direction (reverse of diffusion).

(7) Now apply reverse modulo operation to get the original given image back.

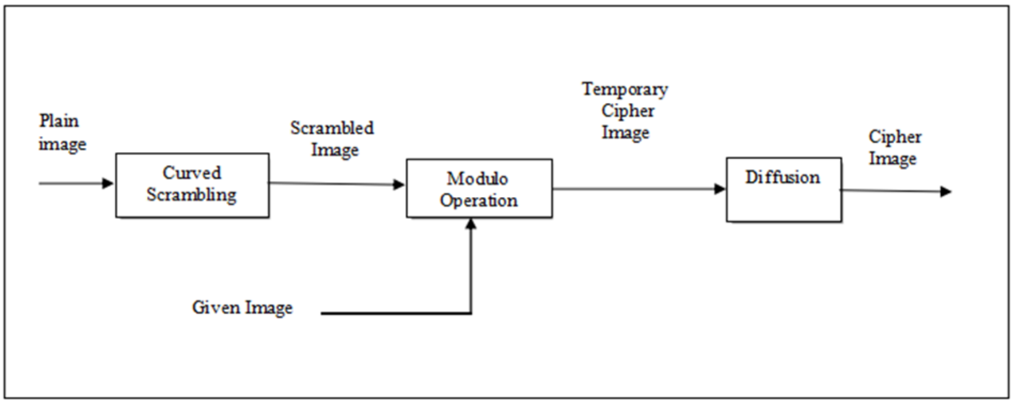


Fig. 4. Encryption Process

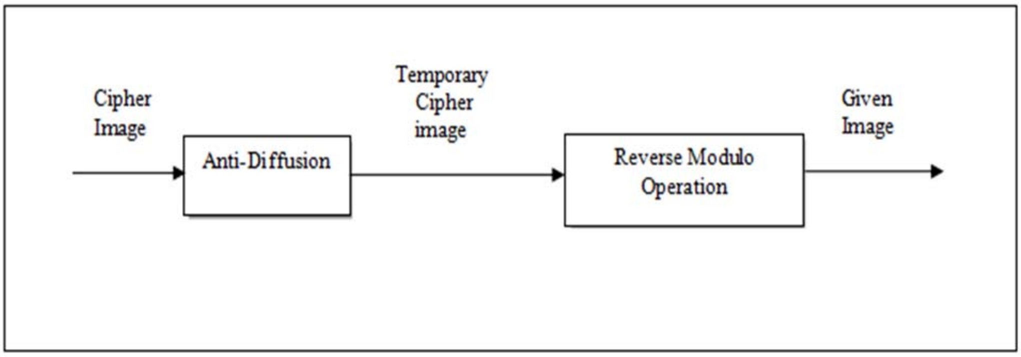


Fig. 5. Decryption Process

V. Result and Discussion

The proposed algorithm is implemented using JAVA_{TM} and used miscellaneous images to work upon. The thing is to be considered is that the both images i.e. plain image and given image must be of same size. The whole algorithm runs in one iteration and produced the desired output. Here fig 6 is the given image which is to be transmitted in encrypted form and the encryption key is derived using the plain image given in fig7.After performing curved scrambling and modulo operation, a cipher image is obtained as in fig8 and transmitted to the receiver.

At receiver end, convert this cipher image into RGB matrix and perform anti-diffusion process to get the temporary cipher image. Finally, as resultant original image in fig 9 is obtained after executing reverse modulo operation.

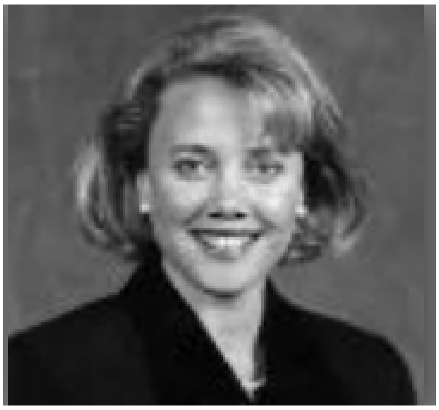


Fig.6. Given image

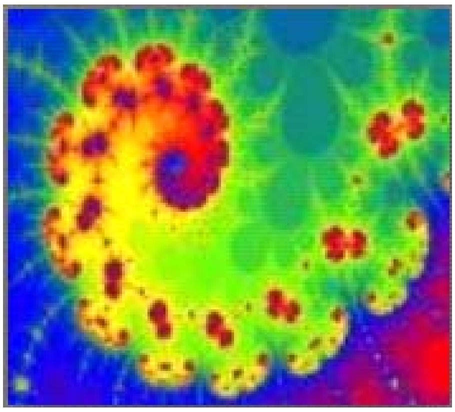


Fig.7. Plain image

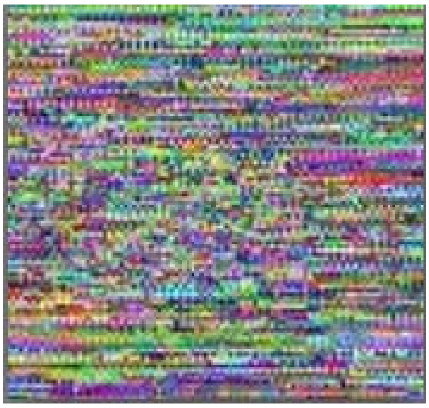


Fig.8.Cipher Image

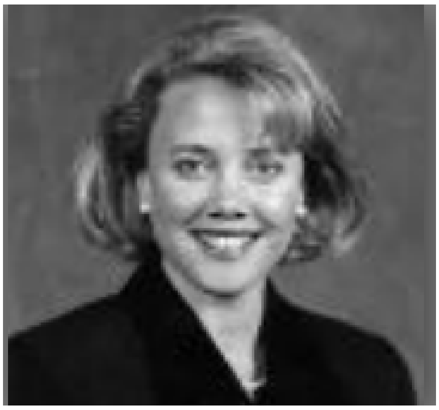


Fig.9. Given image

VI. CONCLUSION

An image encryption algorithm has been proposed to provide a secure cryptosystem to transmit variety of images. A new curved scrambling method increased the complexity of key generation process, therefore difficult to decode by the hacker. Further diffusion process changes the corresponding pixel values thus avoiding repeated permutation. All these techniques help to design a more complex and secure cryptosystem to transmit the data over the insecure network. Being anintricate system, decryption process requires accurate information regarding anti-diffusion process to recover the given image.The proposed encryption method utilized larger key space hence increases the robustness and make it secure from brute force attack. We concluded that the described algorithm can be used for efficient and secure transmission of images over the unsecured network.

AUTHOR CONTRIBUTION

Conceived and designed the experiment: Shafali Agarwal

Performed and analyzed the experiment: Neha Dwivedi and Rishi Kumar Gupta

Wrote the paper: Shafali Agarwal and Neha Dwivedi

REFERENCES

[1] M. Khan &T. Shah,"A Literature Review on Image Encryption Techniques", © 3D Research Centre Kwangwoon University and Springer-Verlag Berlin Heidelberg, 5(4), DOI 10.1007/s13319-014-0029-0, Page 1, 2014.

[2] F. S. Abed, "A New Approach to Encoding and Hiding Information in an Image", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, ISSN (Online): 1694-0814, 2011.

[3] Y. Sun, L. Chen, R. Xu, R. Kong, "An Image Encryption Algorithm Utilizing Julia Sets and Hilbert Curves". PLoS ONE, 9(1): e84655. doi:10.1371/journal.pone.0084655, 2014.

[4] Q. Zhang, S. Zhou and X. Wei, "An Efficient Approach for DNA Fractal-based Image Encryption", Applied Mathematics & Information Sciences, 5(3), pp 445-459, 2011.

[5] G.A. Sathishkumar, Dr. K. BhoopathyBagan and Dr. N. Sriraam, "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security and its Applications, DOI: 10.5121/ijnsa.2011.3214, Vol. 3 No. 2, pp 181-194, Mar 2011.

[6] Y. Xu, H. Wang, Y. Li, B. Pei.,"Image encryption based on synchronization of fractional chaotic systems" Communications in Nonlinear Science and Numerical Simulation, 19(10), 3735–3744, 2014.

[7] M. Ahmad, U. Shamsi, and I. R. Khan, "An enhanced image encryption algorithm using fractional chaotic systems," Procedia Computer Science, vol. 57, pp. 852–859, 2015.

[8] M. Kumar, P.Powduri, A. Reddy, "An RGB image encryption using diffusion process associated with chaotic map", Journal of Information Security and Applications, Elsevier, Vol.21, 20-30, 2015.

[9] N. K. Pareek, V.Patidar and K. K Sud, "Substitution-diffusion based image cipher", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[10] M. Prasad and K.L.Sudha, "Chaos Image Encryption using Pixel shuffling", published in D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, 169–179, 2011.

[11] N. K.Pareek, "Design and analysis of novel digital image encryption scheme", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[12] H.J. Liu, X.Y. Wang, "Colour image encryption based on one-time keys and robust chaotic maps", Computers & Mathematics with Applications 59 (10), 3320–3327, 2010.

[13] S. Sathyanarayana, M. Kumar, and K. Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points", International Journal of Network Security, vol. 12, no. 3, pp. 137–150, 2011.

[14] R.Guesmi, M. A. B. Farah, A.Kachouri, and M.Samet, "Hash key - based image encryption using crossover operator and chaos", Multimedia tools and applications, pages 1– 17, 2016.

[15] D.I. G.Amalarethinam, J.S.Geetha, "Image encryption and decryption in public key cryptography based on MR", International Conference on Computing and Communications Technologies (ICCCT,15), 2015.

AUTHOR PROFILE

Neha Dwivedi, has done graduation from UPRTOU (Uttar Pradesh Rajarshi Tandon Open University) Allahabad. Currently she is pursuing master of computer applications (MCA) at JSS academy of technical education, Noida. She is very keen to learn new aspects in the area of image cryptography and cyber security.

Rishi Kumar Gupta, is pursuing master of computer applications (MCA) at the JSS academy of technical education, Noida. He has received his B.Sc(Mathematics) from Mahatma Gandhi Kashi Vidyapith University, Varanasi. His area of interest is image processing and cryptography.

Shafali Agarwal is associated as an assistant professor with JSSATE, Noida, formerly she worked with NIET, Greater Noida. Her research areas are Image cryptography and fractal analysis. She has published papers in national conference, International conference and International journal which are indexed by ACM, Springer, Thomson Reuters, ProQuest, Index Copernicus, EBSCO, Scribd and many more. She has completed master in computer applications (MCA) in 2004, MPhil in 2013 and Ph.D. degree in 2014. She got published a book titled “Data Structure using C” for engineering students.