*IEIE Transactions on Smart Processing and Computing*

# An Image Steganography Scheme based on LSB++ and RHTF for Resisting Statistical Steganalysis

**Amitava Nag[1,]*, Soni Choudhary[2], Suryadip Basu[2], and Subham Dawn[2]**

[1] Department of Information Technology, Academy of Technology, Hooghly 721212, India amitavanag.09@gmail.com
[2] Department of Computer Science and Engineering, Academy of Technology, Hooghly 721212, India
{choudhary.soni.0909@gmail.com, suryadip.basu@yahoo.com, knightdawnxp@gmail.com}

***** Corresponding Author: Amitava Nag

*Received July 14, 2016; Revised July 27, 2016; Accepted August 2, 2016; Published August 30, 2016*

** Regular Paper*

***Abstract*:** Steganography is the art and science of secure communication. It focuses on both security and camouflage. Steganographic techniques must produce the resultant stego-image with less distortion and high resistance to steganalysis attack. This paper is mainly concerned with two steganographic techniques—least significant bit (LSB)++ and the reversible histogram transformation function (RHTF). LSB++ is likely to produce less distortion in the output image to avoid suspicion, but it is vulnerable to steganalysis attacks. RHTF using a mod function technique is capable of resisting the most popular and efficient steganalysis attacks, such as the regular–singular pair attack and chi-squared detection steganalysis, but it produces a lot of distortion in the output image. In this paper, we propose a new steganographic technique by combining both methods. The experimental results show that the proposed technique overcomes the respective drawbacks of each method.

***Keywords*:** Steganography, Steganalysis, LSB++, Regular–singular (RS) attack

## 1. Introduction

In recent years, with the enormous advancements in digital communications technology, the difficulty in ensuring the security of transmitted messages is becoming alarmingly high. Various methods have been developed for the security of sensitive information. Cryptography and steganography are two popular techniques to protect secret information. Cryptographic techniques provide many ways for successful conversion of a secret message into an unreadable message. However, an unreadable message can easily attract an eavesdropper's attention. Steganography is more reliable because it enhances communication security by inserting secret information within covert carriers to avoid unwanted suspicion. Steganography, which literally means "concealed writing" [19], is the art of secure transmission of secret information within a cover media to avoid unwanted suspicion. Digital cover media include images [1-5, 28], audio [6, 7, 19], and video [8, 9]. Digital images are most suitable for cover media as they provide many excellent ways to hide information. The messages are included in the cover image to produce a stego-object. The process can be roughly stated as:

**Stego-object = Embedded secret message + Cover media**

In image steganography, many techniques have been proposed in recent years to hide the presence of information in a cover image file. Image steganography techniques can be classified into two main categories: spatial domain [20-22] and transform domain [23-26] techniques. In spatial domain image steganography schemes, a secret message bit stream can be directly implanted in the intensity of the cover image pixels. The least significant bit (LSB) method [1, 2, 16, 17, 20-22] is popular, as is the simplest, spatial domain–steganography technique, in which the secret bit stream is embedded into the LSB of the cover image pixels. This method is widely used for steganographic applications due to its simplicity and high embedding capacity. Some of the common LSB-like steganographic methods are LSB replacement [20, 21], LSB matching (LSBM), LSBM revised (LSBMR) [17], and LSBMR edge-adaptive (LSBMR-EA) [16]. In LSB replacement, the cover LSB plane is replaced with secret information bits. In LSBM, if the message bits do not match the LSB of the cover image, then the corresponding pixel value is randomly changed by +-1. LSBMR considers two pixels at a time and provides less image distortion and better resistance to steganalysis, compared to the other steganographic methods. In LSBMR-EA, the message bits are embedded in sharper edge regions, rather than in smoother edge regions. This method preserves the visual quality of the image [16]. However, LSB-based image steganography schemes are susceptible to statistical analysis [12, 13, 27, 29]. The chi-squared ($\chi^2$) test [29, 30] and regular–singular (RS) analysis [12] are the most effective and widely used steganalysis schemes against LSB replacement algorithms.

## 2. Related Work

The steganographic method proposed by Marcal and Pereira in 2005 is based on reversible histogram transformation functions (RHTFs) [11]. In this method a secret key is used to embed secret information into the LSB of an image. Encoding and decoding secret messages is done using mod functions *f* and *f** defined as:

$$f(x) = x - \left| x/(a+1) \right| \quad \text{and} \quad f^*(x) = x + \left| x/a \right| \qquad (1)$$

where *x* is the cover image, and $a$ is the secret key.

However in Lou and Hu's RHTF [18], the cover image is divided into a number of groups (n groups). Accordingly, the secret key is chosen for each group. Hence, we get a set of *n* secret keys $[a_1, a_2 ..... a_n]$. Encoding and decoding secret messages is done using the mod functions *f* and *f** defined as:

$$f(x) = x - \left| x/(a_i+1) \right| \quad \text{and} \quad f^*(x) = x + \left| x/a_i \right| \qquad (2)$$

where *x* is the cover image and $a_i$ is the secret key for the $i^{th}$ group of the cover image.

Lou and Hu's steganographic method maintains the statistical features of the cover image to resist RS steganalysis attack [12]. However, the changes in the histogram of the cover image after applying the RHTF technique can be used to determine the secret key used in the method. Hence the embedding rate can be determined by extracting the secret key used in the process. Another drawback of this method is that this model is applicable to only specific cover images.

The LSB+ method proposed by Wu et al. [14] embeds some extra bits in the image. This method preserves the image histogram in the spatial domain; however, it results in perceptual and statistical distortions. The LSB++ technique [15] was proposed to improve the LSB+ method by restricting some pixels from changing, which results in reducing the number of extra bits to be embedded. In the LSB++ steganography technique, by using a locking process, some cover elements are prohibited from changing. In this method, each pixel value of the cover element is considered a *bin*, and two adjacent bins are considered a *unit*. Locked cover elements are not to be selected in the embedding process. To select the appropriate cover elements to be locked, at first, the frequency difference of two adjacent bins in a unit are computed. Then, using a lock key, the method locks some cover elements for each unit. Similarly, to extract the embedded message, first, the lock elements are determined using the lock key value. Then, the message bits are extracted using the embedding key. This method is secure against histogram-based attacks, but some steganalysis methods can use higher order statistics to detect the presence of a secret message in a cover element.

## 3. The Proposed Scheme

Embedding a secret message using the LSB++ technique produces less distortion. However, it is less resistant to steganalysis attacks like the RS attack or the chi-squared attack. The reversible histogram transformation function embedding scheme is resistant to both chi-squared ($\chi^2$) detection and RS attack steganalysis schemes, but it produces significant distortion in the image. In this article, the proposed steganographic scheme combines the techniques of LSB++ and the RHTF [18]. The experimental results show that this method improves security and decreases the distortion produced in the stego-image. Figs. 1 and 2 show the complete procedure of the scheme.

Suppose that the cover image is $Ic_{mxn}$, and secret message *msg* is to be embedded. After embedding the corresponding stego-image, $Is_{mxn}$ will be obtained.

## 3.1 Embedding Algorithm

Step 1. Generate lock matrix $L_{mxn}$ to represent the pixels to be locked in the cover image, where

$L_{i,j} = 0$, then the corresponding pixel of the cover image will be locked,

$L_{i,j} = 1$, then the corresponding pixel of the cover image will not be locked,

where $1 <= i <= m$, $1 <= j <= n$.

a) Initialize all elements of L by 1.

b) Generate the histogram of Ic in h.

c) Calculate $A_k = |h_{2k} - h_{2k+1}|$, which represents the frequency difference of the two bins.

d) Initialize with 0 for every $A_k$ elements in $L_{i,j}$, where $Ic_{i,j}$ has the value 2k when $h_{2k} > h_{2k+1}$; else 2k+1 when $h_{2k} < h_{2k+1}$.

e) Repeat these steps for all values of h.

Step 2. Embed *msg* in Ic for every $L_{i,j} = 1$, and the corresponding bits are embedded in each respective $Ic_{i,j}$ to create the stego-image Is.

a) Divide the pixels of Ic into *b* groups, selecting a specific rule, *R*, for each group.

b) The secret key $a_n$ for each group $G_n$ is selected as follows:

i. Successively increase $a_n = a_{n-1} + 1$, until $a_n = a_U$.

ii. Successively decrease $a_n = a_{n-1} - 1$, until $a_n = a_L$.

iii. Repeat the steps until n = b.

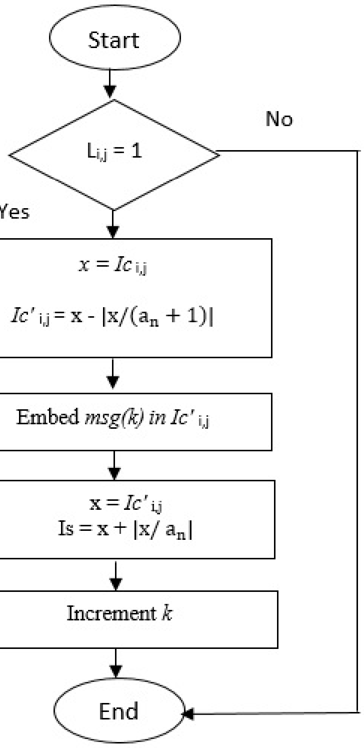


**Fig. 1. Flowchart for the embedding algorithm.**

c) Apply reversible histogram transformation function $f_1$ to group $G_n$ for the respective secret key $a_n$ and, hence, produce image $f_1(Ic)$.
d) Embed the message in $f_1(Ic)$ to produce $Ic'$.
e) Apply the reversible histogram transformation function $f_2$ to group $G_n$ for the respective secret key $a_n$ and, hence, produce the stego-image Is = $f_2(Ic')$ where

$$f_1(x) = x - \left| x/(a_n + 1) \right| \quad \text{and} \quad f_2(x) = x + \left| x/a_n \right|$$

## 3.2 Extraction Algorithm

Step 1.The lock matrix $L_{mxn}$ is taken.
Step 2. Extract *msg* from Is for every $L_{i,j} = 1$.
a) Divide the pixels of Is into *b* groups, selecting a specific rule *R*, for each group
b) The secret key $a_n$ for each group $G_n$ is selected as follows:
  i. Successively increase $a_n = a_{n-1} + 1$, until $a_n = a_U$.
  ii. Successively decrease $a_n = a_{n-1} - 1$, until $a_n = a_L$.
  iii. Repeat the steps until n = b.
c) Apply reversible histogram transformation function $f_1$ to group $G_n$ for the respective secret key $a_n$ and, hence, produce the image $f_1(Is)$.
d) Embed the message, *msg*, from $f_1(Is)$ where

$$f_1(x) = x - \left| \frac{x}{a_n + 1} \right| \quad (3)$$

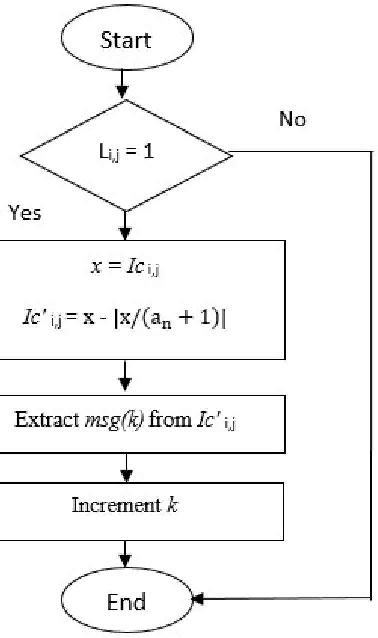


**Fig. 2. Flowchart for the extraction algorithm.**

## 4. Result and Discussion

In order to evaluate the performance improvement achieved by the proposed scheme, we consider the peak signal-to-noise ratio (PSNR). PSNR is applied to compare the visual quality between the cover image and the stego-image. The definition of PSNR is

$$PSNR(dB) = 20\log_{10} \frac{255}{\sqrt{MSE}} \quad (4)$$

MSE is the mean squared error between the original image and the modified image, which is defined as

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left( I(x,y) - I'(x,y) \right)^2 \quad (5)$$

where M and N denote the width and height, respectively, of the cover and stego images.

A comparative study of the proposed method, RHTF [18] and LSB++[15], is given in Table 1. Embedding rate means the number of secret bits that could be used for embedding in each cover pixel. In this paper, we adopted two different 512×512 images as the cover images. Key selection for the RHTF technique and the combined technique follows the same pattern. We performed a similar grouping of pixels. The secret keys were chosen for higher bounds as well.

From Table 1, we can see that the PSNR value of the proposed scheme is close to that of the LSB++ mechanism (decayed less than 0.45 dB). On the other hand, the proposed scheme has better PSNR than the RHTF-based LSB steganography scheme (improved by at least 0.2 dB).

Fig. 3 shows the PSNR curves for different embedding rates of the proposed scheme, RHTF-based LSB, and the LSB++ steganographic scheme. The distortion curve is not

**Table 1. Comparison of PSNR value and embedding rates with different methods.**

| Embedding Rate | Proposed Method | RHTF-based LSB [18] | LSB++ [15] |
|---|---|---|---|
| 0.1 | 64.30903 | 63.85283 | 64.44018 |
| 0.2 | 61.01802 | 60.83018 | 61.45688 |
| 0.3 | 59.28424 | 59.14728 | 59.65106 |
| 0.4 | 57.97435 | 57.81618 | 58.32778 |
| 0.5 | 56.95921 | 56.878 | 57.31823 |
| 0.6 | 56.06102 | 56.0528 | 56.49875 |
| 0.7 | 55.44091 | 55.3684 | 55.82714 |
| 0.8 | 54.76661 | 54.73951 | 55.15584 |


**Fig. 3. PSNR curves for different embedding rates.**

(a) Peppers (b) Lena

**Fig. 4. Cover images.**

significantly changed, but it is an improvement against embedding using RHTF only.

Figs. 4 and 5 shows cover and stego-images, respectively, of the proposed scheme.

Embedding the message should ensure secrecy so that no third party can suspect the presence of information in the stego-object. The embedding, however, leads to distortion of visual and statistical properties of the cover media. Steganalysis [12, 13] is a process that deals with detection of the presence of any secret embedded message within a cover media. Any steganographic method must focus on how to minimize steganographic detectability.

Figs. 6 and 7, respectively, show the probability of detection from an RS attack against the proposed method on Lena, Fig. 5(a), and Peppers, Fig. 5(b).

(a) Peppers (b) Lena

**Fig. 5. Stego-images.**

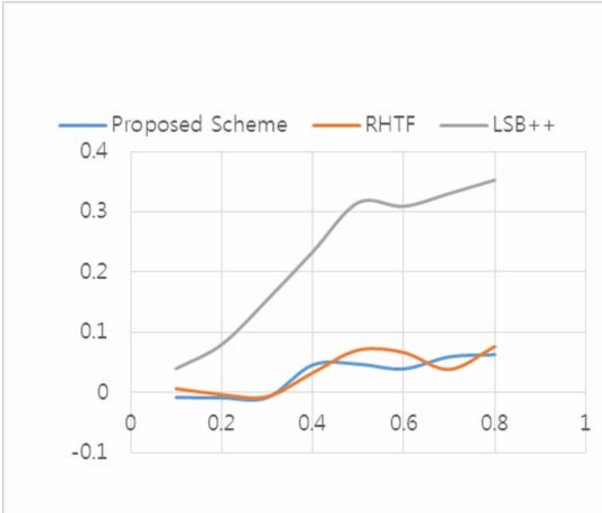


**Fig. 6. Resistance against RS attack analysis for the 256×256 Lena image.**


**Fig. 7. Resistance against RS attack analysis for the 512×512 Peppers image.**

The probability of detection with our proposed scheme is not monotonically increasing because of the successful resistance to RS attack analysis. The combination of the locking mechanism of LSB++ and the modulo function filter effectively disturbs the regular–singular pairs to be

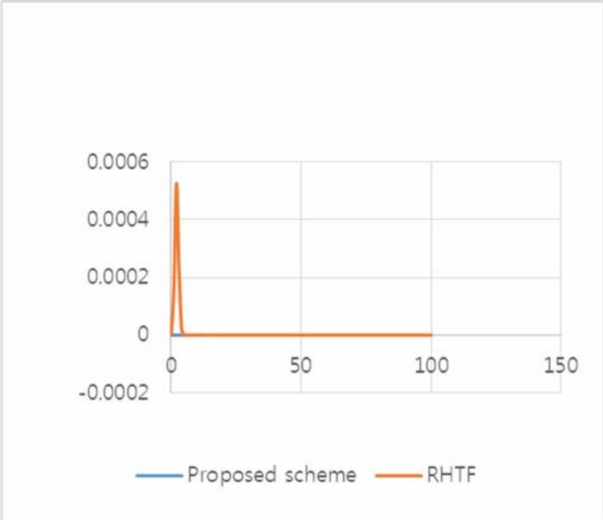


**Fig. 8. Resistance against chi-squared attack analysis for the 256×256 Lena image.**


**Fig. 9. Resistance against chi-squared attack analysis for the 512×512 Peppers image.**

detected.

So even at a high embedding rate, the probability of detection does not increase significantly. Thus, the combined method resists the RS attack better than LSB++ as well as RHTF for certain embedding rates, as is evident in Figs. 6 and 7.

RHTF is a reliable technique to prevent $\chi^2$ detection, as shown in Fig. 8. LSB++ cannot prevent $\chi^2$ detection properly, as shown in Fig. 9. The proposed technique prevents the $\chi^2$ attack as good as the RHTF [18] (see Fig. 8) and better than LSB++ [15] (see Fig. 9).

## 5. Conclusion

In this paper, we proposed a new steganography scheme. In this scheme, security increases significantly when we use the reversible histogram transformation function for embedding in the LSB++ method. It can easily evade the two most popular steganalysis techniques—the regular–singular pair attack (RS attack) and $\chi^2$ detection. Our proposed method produces better results than the RHTF. At the same time, it reduces the distortion produced in the RHTF due to the locking function of LSB++. Although it cannot reduce the distortion as well as LSB++, it is an improvement over the individual drawbacks of the RHTF and LSB++ methods.

## References

[1] C.-C. Chang, T. D. Kieu, "A reversible data hiding scheme using complementary embedding strategy," Inform. Sci., vol. 180, no. 16, pp. 3045-3058, 2010. Article (CrossRef Link)

[2] C.-C. Chang, W.-L.Tai, C.-C. Lin, "A reversible data hiding scheme based on side match vector quantization," IEEE Trans. Circ. Syst. Video Technol., vol. 16, no. 10, pp. 1301-1308, 2006. Article (CrossRef Link)

[3] D.-C. Lou, J.-L.Liu, "Steganographic method for secure communications," Comput.Security, vol. 21, no. 5, pp. 449-460, 2012. Article (CrossRef Link)

[4] D.-C. Lou, C.-H. Sung, "A steganographic scheme for secure communications based on the chaos and Euler theorem," IEEE Trans. Multimedia, vol. 6, no. 3, pp.501-509, 2004. Article (CrossRef Link)

[5] J. Mielikainen, "LSB Matching Revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285-287, 2006. Article (CrossRef Link)

[6] D.-C. Lou, C.-L.Lin, C.-L.Liu, "Novel steganalysis chemes for BPCS steganography," Imaging Sci. J., vol. 56, no. 4, pp. 232-242, 2008. Article (CrossRef Link)

[7] R. Petrovic, J. M. Winograd, K. Jemili, E. Metois, "Data hiding within audio signals," in Proc. of the 4th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, pp. 88-95, 1999. Article (CrossRef Link)

[8] A. A. Hanafy, G. I. Salama, Y. Z. Mohasseb, "A secure covert communication model based on video steganography," in Proc. of the 2008 IEEE Military Communications Conference, pp. 1-6, 2008. Article (CrossRef Link)

[9] B.-S. Ko, R. Nishimura, Y. Suzuki, "Time-spread echo method for digital audio watermarking," IEEE Trans. Multimedia, vol. 7, no. 2, pp. 212-221, 2005. Article (CrossRef Link)

[10] B. Liu, F. Liu, C. Yang, Y. Sun, "Secure steganography in compressed video bitstreams," in Proc. of the 3rd International Conference on Availability, Reliability and Security, pp. 1382-1387, 2008. Article (CrossRef Link)

[11] A.R.S Marcal, P.R. Pereira, "A steganographic method for digital images robust to RS staganalysis," in: International Conference on Image Analysis and Recognition, Toronto, Canada, Lecture Notes in Computer Science, vol. 3656, 2005, pp. 1192-1199. Article (CrossRef Link)

[12] J. Frridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in color and grayscale images," in: Proceedings ACM Workshop Multimedia and

Security, 2001, pp. 27-30. Article (CrossRef Link)
[13] A. Nissar, A. H. Mir, "Classification of steganalysis techniques: A study"
[14] Wu, Dugelay, Cheung," A data mapping method for steganography and its application to images," in: 10th International Workshop on Information Hiding, vol. 5284, USA, May 2008, p. 236-250. Article (CrossRef Link)
[15] KazemGhazanfari, GhaemmaghamiShahrokh, Saeed R. Khosravi, "LSB++: an improvement to LSB+ steganography," in: TENCON 2011-2011 IEEE Region 10 Conference, IEEE, 2011, pp. 364-368. Article (CrossRef Link)
[16] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on lsb matching revisited, IEEE Tans. Inf. Forens. Security.Vol. 5, no. 2, pp. 201-214, 2010. Article (CrossRef Link)
[17] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett.Vol. 13, no. 5, pp. 285-287, 2006. Article (CrossRef Link)
[18] D. C Lou, C. H Hu, "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis" Inform. Sci., vol. 188, pp. 346-358, 2012. Article (CrossRef Link)
[19] Mohsen Bazyar, Rubita Sudirman, A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm, JurnalTeknologi, 74: 6 (2015) 49–53. Article (CrossRef Link)
[20] Wang R, Lin C, Lin J. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognit 2001; 34(3): 671–83. Article (CrossRef Link)
[21] Chang C, Hsiao J, Chan C. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognit, 2003; 36(7): 1583–95. Article (CrossRef Link)
[22] Chan C, Cheng L. Hiding data in images by simple LSB substitution. Pattern Recognit 2004; 37(3): 469–74. Article (CrossRef Link)
[23] El Safy R, Zayed H, El Dessouki A. An adaptive steganographic technique based on integer wavelet transform. In: International conference onnetworking and media convergence (ICNM 2009). IEEE; 2009. p. 111–7. Article (CrossRef Link)
[24] Bhattacharyya S, Sanyal G. Data hiding in images in discrete wavelet domain using PMM. World Acad Sci Eng Tech 2010;68:597–605.
[25] Torres-Maya S, Nakano-Miyatake M, Perez-Meana H. n image steganography systems based on BPCS and IWT. In: 16th International conference onelectronics, communications and computers. IEEE; 2006. p. p. 51. Article (CrossRef Link)
[26] Lin C, Shiu P. High capacity data hiding scheme for DCT-based images. J Inf Hiding Multimedia Signal Process 2010; 1(3): 220–40.
[27] M. Ghebleh, A. Kanso, A robust chaotic algorithm for digital image steganography,Communications in Nonlinear Science and Numerical Simulation, Volume 19, Issue 6, June 2014, Pages 1898–1907. Article (CrossRef Link)
[28] Al-Dmour, Hayat, and Ahmed Al-Ani. "Quality optimized medical image information hiding algorithm that employs edge detection and data coding."Computer Methods and Programs in Biomedicine 127 (2016): 24-43. Article (CrossRef Link)
[29] Westfeld A, Pfitzmann A. Attacks on steganographic systems. In: Third international workshop on information hiding, IH '99. London, UK: Springer; 2000. p. 61–76. Article (CrossRef Link)
[30] Provos N, Honeyman P. Detecting steganographic content on the internet. In: NDSS'02: network and distributed system security symposium. Internet Society; 2002.



**Amitava Nag** is Associate Professor of Information Technology, Academy of Technology, India. He received his B.Tech. and M.Tech degrees University of Kalyani, India and University of Calcutta, in 2003 and 2005, respectively and his Ph.D. from the University of Kalyani in 2015. Dr. Nag served or currently serving as a reviewer and Technical Program Committee for many important Journals, Conferences in Information Security and Cloud Computing areas. His research interests include information security, cloud computing, IoT. He is a member of the ACM.

**Soni Choudhary** received her B.Tech degree in Computer Science & Engineering from Academy of Technology, Aedconagar, Hooghly, India in June, 2016. Her research interests include image processing, information security, cloud computing.

**Suryadip Basu** received his B.Tech degree in Computer Science & Engineering from Academy of Technology, Aedconagar, Hooghly, India in June, 2016. His research interests include image processing and pattern recognition.

**Subham Dawn** received his B.Tech degree in Computer Science & Engineering from Academy of Technology, Aedconagar, Hooghly, India in June, 2016. His research interests include artificial intelligence, optimization techniques, image processing, information security.