ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Novel Approach to Image Steganography Using Keys

Sunny Dagar[1], Tariq Rashid[2]

Assistant Professor, Department of CST, Manav Rachna University, Faridabad (Haryana), India[1]

M.Tech. Student, Department of CST, Manav Rachna University, Faridabad (Haryana), India[2]

ABSTRACT: Steganography is an art but especially it is a science of hiding sensitive and secret information inside a file like image, audio or video. This paper proposes a novel approach of hiding secret information inside an image using two secret keys to randomize the bit hiding process. Use of two secret keys increases the security of hidden secret information. This approach uses red, green and blue values of a pixel and performs calculations using these keys. Based on this calculation, secret information bits will be hidden at the random position of the pixels. This approach maintains high data hiding capacity like LSB substitution but maintains a good security level, which is not present in LSB substitution as LSB substitution technique is predictable. As the hidden information is randomized, so it is difficult for attacker to retrieve the secret information from stego image. PSNR value is used to measure the quality of output image and also compared it with other efficient image steganography techniques. The obtained result shows that this algorithm is highly efficient as compared to many other algorithms.

KEYWORDS: Image Steganography, Steganography, Random Bit hiding, Secret Keys, Cover Image, Stego Image.

I. INTRODUCTION

Steganography is an art and science of hiding some data into another data. Steganography is an art because in ancient time steganography was used with some art like message written through invisible ink, Message engraved on the shaved head of slaves and then allow them to grow hair and at the receiver side receiver again shaved their head to read the secret message etc. Steganography is a science because in today‘s world we hide secret information i.e. text, audio, video etc. bit wise [1]. Steganography is a technique of hiding secret messages inside a carrier so that only sender and intended recipient of the message know about the presence of hidden message. Steganography was derived from Greek words whose actual meaning is ―hidden writing (Greek word ―Steganos means ―covered and ―graphei means ―writing).

Steganography utilizes the assumption that if an attacker has the knowledge of presence of any secret data in a file then he/she tries to decrypt it anyhow. But if no one has the knowledge of presence of any secret data, then how and on which an attacker applies decryption algorithm. Image steganography allows two parties to communicate secretly and invisibly. Although many efficient image steganographyalgorithms also ensures security of the hidden information [1, 2 and 3].

Generally secret information is hidden at the specified position of LSB (Least Significant Bit) of the cover image [4, 5, 6, 7 and 8]. As hiding information in LSB is predictable and it is very easy to retrieve secret information by anyone as it doesn‘t require any calculation and guess. Hiding secret information at LSB is the weakest method in this highly advanced digital world. Some permutation and combination must be applied either on the secret data or cover image data so that some level of security can be introduced. Today‘s efficient steganography techniques not only emphasis on efficient hiding but also pattern hiding. This pattern hiding ensures that some unauthorized person is not getting access to the highly sensitive secret information. Steganography is most popular in military operations where highly sensitive war commands and other secret commands must be delivered only to the intended recipients secretly and invisibly [1, 3, 5, 6 and 8].

There are many researchers describing the quality of a good steganography approach. Many efficient image steganography algorithms have been proposed [2, 4, 5, 6, 7, and 8]. Most of these are replacing LSB of the cover image. Although LSB substitution is the simplest steganography approach so far but it is not efficient in terms of security as it is predictable. A very well-known LSB approach is presented in [7] and proposed an adaptive method

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

based on inter pixel relationship. This approach produces very attractive results but its retrieval is very easy by applying retrieval method. There is no need of any secret information or key before retrieval. This makes it vulnerable to attacks. Another efficient approach is presented in [6] which used neighbourhood information to calculate the amount of data that can be hidden in pixels of cover image. In this approach, some pixels are overloaded with data while some pixels remain unchanged. In this approach also, secret information can be easily retrieved easily. There is another efficient approach presented in [4] in which secret key is used only to decide whether the secret information bits will be hidden in green or blue. After deciding this, secret information bits hides in LSB of either blue or green. Although, this approach initially promises security but after that hiding secret bits in LSB is again not secure and secret data can be extracted after putting some efforts.

II. RELATED WORK

The simplest information hiding approach is Least Significant Bit (LSB). In this approach, Least Significant Bit of pixel is replaced by secret bits. Suppose we want to hide „C" in the cover image. So it requires 8 bytes to store C. suppose we have 3 pixels, each of 24 bits. We know that ASCII value of C is 67 i.e. 01000011 in binary. Now this secret data is going to hide in LSB of RGB.

Before Hiding:

	Red	Green	Blue
Pixel 1	10100110	11010100	11111001
Pixel 2	11100011	10001101	10011001
Pixel 3	11100110	01110000	10001100

After Hiding „A" in LSB of RGB

	Red	Green	Blue
Pixel 1	10100110	1101010**1**	1111100**0**
Pixel 2	1110001**1**	10001100	10011000
Pixel 3	1110011**1**	01110001	10001100

As described above, LSB is simple technique of data hiding but it is predictable and hidden information can be retrieved easily. So, an efficient technique is required which is secure as well as efficient.

This paper describes an efficient technique of steganography which uses image as a carrier and secret file as a carried information. Image generated as an outcome of steganography process which contains secret information is called stego image. Peak Signal to Noise Ratio (PSNR) is used to measure the quality of stego image. PSNR is a statistical method for the assessment of the digital image and video quality [6]. PSNR can be easily defined through Mean Square Error (MSE) method.

$$MSE = (1/mn) \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Here, I and K are two monochrome images of m x n. One of the images is considered to be as noisy approximation of the other. Now, PSNR can be calculated using the below mentioned formula.

$$PSNR = 10.\log10 (MAX_I^2 / MSE)$$

$$= 20.\log10 (MAX_I / \sqrt{MSE})$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAX_I is $2B-1$.

A PSNR value shows the distortion in the stego image. Larger the PSNR value, less will be the distortion and hence better will be the quality. A larger PSNR value indicates lesser possibility of visual attacks [6 and 7].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. PROPOSED ALGORITHM

In this proposed approach, three secret keys i.e. Key1 and Key2 and key3 are used to randomize the pattern of but hiding. With the help of these three secret keys, relevant position is decided and at this position, we will hide secret information.

Encryption:
Cover Image + Secret Information + Key1 + Key2 + Key3 = Stego Image

Decryption:
Stego Image + Key1 + Key2 + Key3 = Secret Information

Key1: Key1 is a circular 1D array in which only 0 or 1 value isallowed. It is also forced that number of zero‘s and one‘s in

Key1 is used to achieve better security against statistical attacks. If number of secret information bits is more than the size of array, then the array is circularly shifted to the first position. This provides us freedom to choose the length of the secret Key1.

Key2: Key2 is a 1D array with 8 digits. We can enter digitsbetween 0 and 4. Repetition of digits is allowed but two consecutive digits can‘t be same. This rule must be followed to extract correct information from stego image.

Key3: Key3 is a circular 1D array having n number of digits ranging between 0 and 2. Here ’0’ represents red, ‘1’ represent green and ‘2’ represent blue.

Key1, Key2 and Key3 can be used repeatedly for many steganography processes.

A. *Hiding Process:*

Hiding process repeatedly uses Key1, Key2, and Key3 to place the secret information at the proper place. Process of hiding secret information in one pixel is discussed below:

First of all we choose three secret keys i.e. key1, Key2 and Key3. Now Key1 will decide that first bit of Key2 will be XOR with LSB of red, green or blue. Then LSB of selected colour is XOR with the first bit of Key2 (Key2 and selected colour value of a pixel is used to make decision that the secret information bit will be placed in green or blue or red). Now based on the value of key3, exact position for secret bit in green or blue or red is decided. After hiding the first bit of secret information. This process continues repeatedly until all secret information bits are placed at their respective positions in stego image. This method not only increases the bit hiding capacity bit also randomizes the bit hiding process to obtain a highly competent stego image. This randomization improves security against attacks.

B.*Extraction Process:*
Receiver also has the three keys i.e. Key1, Key2 and Key3 in advance before starting the extraction process. Now receiver side also first bit of Key2 will be XOR with MSB of red, green or blue. Then LSB of selected colour is XOR with the first bit of Key2. Now based on the value of key3, exact position for secret bit in green or blue or red is decided. After extracting the first bit of secret information. This process continues repeatedly until all secret information bits are extracted and stored inside an array.
Although the process of extraction is equal complex as hiding process, extraction process is very important and should be secured from attacks. Extraction process is also known as steg-analysis. Steg-analysis is an opposite process of steganography.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

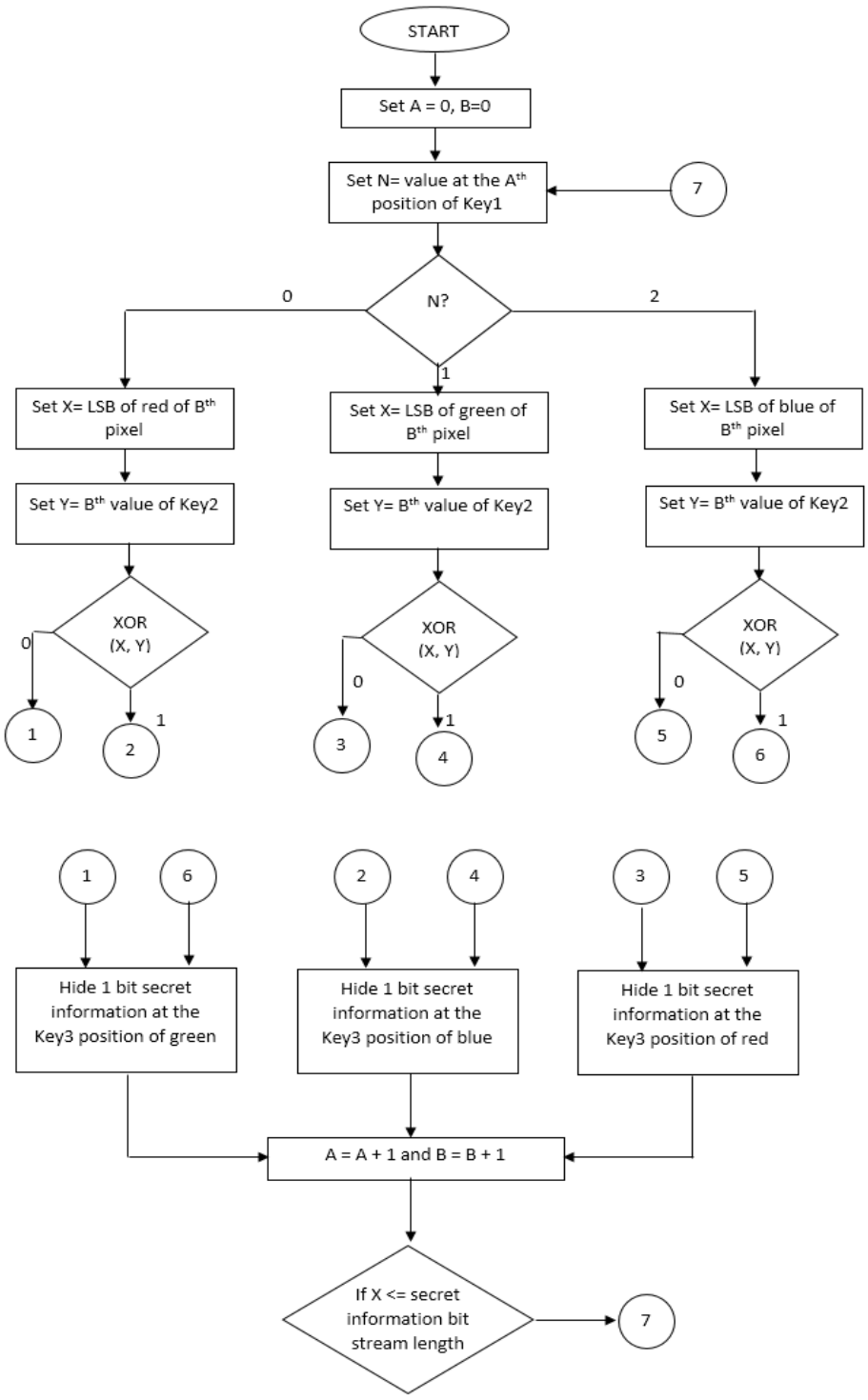

Fig: Hiding Process

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

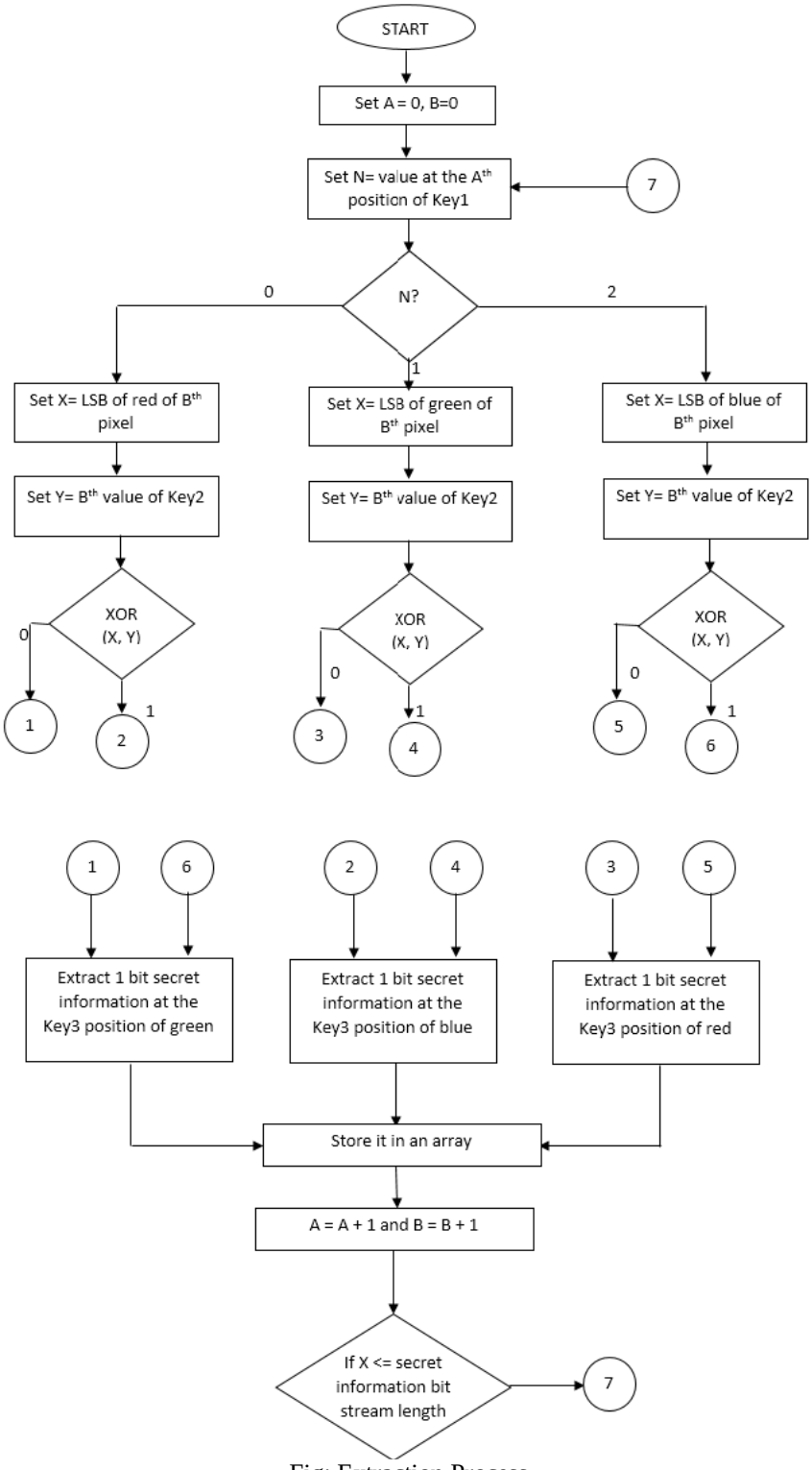

Fig: Extraction Process

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. PSEUDO CODE

Step 1: Set A and B to 0 (Zero).
Step 2: Set N= Value at the A^{th} position of key1
Step 3: Check the below condition for N.
If (N==0)
Set X= LSB of red of B^{th} pixel
Set Y = B^{th} value of Key 2
Check the below condition for XOR (X, Y)
If ((X XOR Y) ==0)
Hide 1 bit secret information at the key 3 position of green
Else
Hide 1 bit secret information at the key 3 position of blue

Else if (N==1)
Set X= LSB of green of B^{th} pixel
Set Y = B^{th} value of Key 2
Check the below condition for XOR (X, Y)
If ((X XOR Y) ==0)
Hide 1 bit secret information at the key 3 position of red
Else
Hide 1 bit secret information at the key 3 position of blue
Else if (N==2)
Set X= LSB of blue of B^{th} pixel
Set Y = B^{th} value of Key 2
Check the below condition for XOR (X, Y)
If ((X XOR Y) ==0)
Hide 1 bit secret information at the key 3 position of red
Else
Hide 1 bit secret information at the key 3 position of green
End if
Step 4: Set A=A+1 and B=B+1.
Step 5: Check the below condition for X
If (X<= Secret information bit stream length)
Go to step 2.
Step 6: End.

V. SIMULATION RESULTS

Here PSNR value of proposed method is compared with the already present efficient techniques. here we compare our results with [4, 6, 7 and 8].

Cover Images	PSNR (in dB) in Na-I Wu's method	PSNR (in dB) in Four Neighbour method	PSNR (in dB) in DWT method	PSNR (in dB) in this method
Lena	34.3962	41.1468	46.8369	49.3321
Baboon	30.413	36.5154	46.5443	49.2215
Pepper	33.7496	41.0315	46.7818	48.1134

Table 1: Comparison with existing methods

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Here in table 1, PSNR value of the proposed algorithm is compared with the three efficient techniques i.e. Na-I Wu's method, Four Neighbour method and DWT method. Results shows that PSNR value of proposed algorithm is better than the other efficient algorithms.

VI. CONCLUSION AND FUTURE WORK

This can be easily conclude that this proposed approach is very beneficial and secure against statistical attacks. Using three keys is slightly difficult but where security is the major concern, this approach is best suited. The experimental result shows that proposed method is effective way of secret information hiding without any visible distortion in the carrier image. It is also very difficult for the unauthorized user to identify the changes in the carrier image. The use of three secret keys protects the secret content from unauthorized user.

This proposed approach opens the new dimensions in the field of image steganography. The use of three secret keys randomizes the hiding process and provides better security to the secret information. It is very difficult to recover the hidden information by the attacker without knowing the three secret keys. This proposed method provides higher PSNR value as higher PSNR value indicates lower distortion.

Future work for this approach includes higher PSNR value, less effort in generating, exchanging and managing three keys.

REFERENCES

1. Kahate Atul (), Cryptography and Network Security, the McGraw Hill Companies, 2nd edition, 2008.
2. A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, "A Novel Technique for Image Steganography Based on Block-OCT and Huffman Encoding". International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.
3. Neil F. Jhonson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE paper of February 1998, available online: http://www.creangel.com/papers/steganografia.pdf
4. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key", 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 201 I, Dhaka, Bangladesh.
5. F. Hartung and M. Kutte "Information hiding-a survey, "Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue: 7, pp. I062-I078, July. 1999.
6. M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.
7. Na-I Wu, "A Study on Data Hiding/or Gray-Level and Binary Images " Available:http://ethesys.lib.cyut.edu.tw/ETD-db/ETD-search/getfile?URN=etd-0707104-144705&filename=etd-0707104-144705.pdf
8. Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006, p.p. 275-290.
9. Jassim Mohmmed Ahmed and Zulkarnain Md Ali "Information Hiding using LSB technique" IJCSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.
10. F. A. P. Peticolas, et al., "Information hiding–a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.
11. S. K. Moon, R. S. Kawitkar "Data Security using Data Hiding" International Conference on intelligence and multimedia Application, vol. 4, 2007, pp.247-251.
12. R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.3, May 2010, p. p 41-47.
13. Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), p.p.561-570.
14. Rajarathnam Chandramouli, Mehdi Kharrazi, Nasir Memon, "Image Steganography and Steganalysis: Concepts and Practice", Second International Workshop, IWDW 2003, Seoul, Korea, October 20-22, 2003 p.p. 35-49.

BIOGRAPHY

Sunny Dagar is an Assistant Professor in the Department of Computer Science and Technology, Manav Rachna University, Faridabad, Haryana, India. He received Master of Technology (M.Tech.) degree in 2013 from IPU, Delhi, India. His research interest includes Steganography, Authenticationand Algorithms.

Tariq Rashidis an M.Tech. Student in the Department of Computer Science and Technology, Manav Rachna University, Faridabad, Haryana, India. His research interests are Steganography and Information Security.