International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Pearl Pixel Steganographic Method for Grayscale Images using Location-Array Method

V.Raja, S.Rajalakshmi,

Abstract: ***Nowadays, the user of the internet is growing very fast, in which sends and receiving a messages become very easy using social media applications, meanwhile using these applications, the security is a very big issue. Today providing security for the essential data becomes too hard, intruders become smarter. They are using advanced techniques and models to access our data. For a long period cryptography algorithms were operated to protect the important data, but nowadays these algorithms are easily broken by the intruders. The steganography algorithms are considered as the next generation of cryptography; every user is able to create own algorithms to send and receive the important data. In this method, the secret data will embed into image pixel; many more algorithms are designed by the researcher using this idea. All of these algorithms embed the data into an image and transfer the stego image from one end to another end with stego-key at the receiver end with the help of a stego-key, they do the reverse engineering process in the stego image to get the original data which embedded by the sender side. In most of the algorithms, transfer the stego image and key is a very big concern. Since during the transmission time of stego image and key, anyone can make changes into that; like resize the image or cropping the same. If the receiver gets the damaged version of stego image, they can't get the original message back. In that circumstances transmission of stego-image with stego-key, it needs more space and time to reach the destination as well as need to pay attention to the security. To overcome these problems, the proposed method does not transfer the stego image, due to which it is not required to compare the image before and after data insertion and no need to calculate the peak signal-noise ratio (PSNR). It shares stego key with the proper security key to recognize if any intruder made an attack on that. This method provides good security for the data.***

Keywords: intruder, cryptography, steganography, stego-image, stego-key, PSNR.

I. INTRODUCTION

Digital communication makes it very easy to transfer the message from one end to another end in a very fast manner as well as very easy. The social media plays a vital role to transmit the information, every day the users of social media is increasing very fast and the memory they are utilizing is also becoming very high. India is cheaper in providing data for the internet around the globe. At the same time of transmitting data; the security for the same should be considered.

Cryptography [1-4] was used to take care of the above for a very long time but now these algorithms become very older as well as easily brute-forced by the intruders.

After that many more techniques are introduced and among all steganography [3-7] is very good as well as easy to implement. Steganography was used in the war field very long back, nowadays the same idea will be converted and digitized, in this technology, the secret data will be embedded into four different medium such as images, text, audio, and video.

This paper describes the image steganography. Today many more image steganography algorithms are developed by the researchers. Steganography is considered as a derived class from cryptography.

In general, in the image steganography the secret message will consist of either binary inputs or alphanumeric. If it is binary it will be used directly else alphanumeric content will be converted into ASCII value, then it will be converted into binary. The binary data will be embedded in an image. An image is a collection of pixels [6-10]. While taking a grayscale image the pixel value lies between 0 and 255, and when color images considered, it is a combination of the RGB value. The three different matrices are used to represent the value. Commonly image steganography algorithms [11, 12] build the grayscale images only, due to the quality of the images remains as the original after embedding the secret bits, and for the process of embedding using a specified algorithm the final output stego image with stego key will be transmitted from sender to receiver. Stego key [13, 14] consists of some value, which is used to recover the original secret bits from the stego image at the receiver side [15-19].

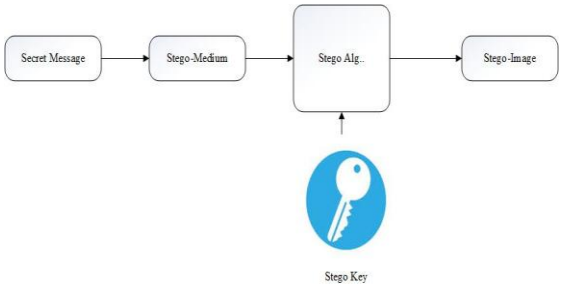

Figure 1: Steganography model

Payload, visual quality and distinguishable are three points to be considered as a major issue while using image steganography; Payload deals about how much bits are embedded into an image.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
V.RAJA*, Research Scholar (Part-time Category – B), Bharathiar University, Coimbatore – India.
S.Rajalakshmi, Department of Computer Science and Engineering, S.C.S.V.M.V, Enathur, Kanchipuram, Tamilnadu – India.

The visual quality difference between before embedding image and after embedding image will be calculated by PSNR value, the higher value is considered to be a good result. After the data embedding process into an image, that should not be detectable by the human eye [18, 19]. In general, the Steganography algorithms are classified into two different methods. They are spatial domain and transform domain which are explained in detail in the following section.

II. LITERATURE REVIEW

Commonly steganography techniques will work in two major domains; they are spatial domain and transform domain. In spatial domain many more models have been developed, in which very few familiar techniques are discussed here, they are.

1. Least significant bit insertion method
2. Pixel value differencing method
3. Exploiting modificationin all direction
4. Multi based notational system
5. Edge-based methods

In the Transform domain, some of the important methods are

1. Discrete Fourier transforms
2. Discrete Cosine transforms
3. Discrete Wavelet transforms

A. Least significant bit (LSB) insertion method:

An image is a group of pixels, having values between 0 and 255 for grayscale image [20]. The binary bits of secret bits are embedding as follows. The pixel value is converted into decimal and the least significant bits will be changed from original bits into secret bits. For example considering 00110010 100 where the first consecutive eight bits are the binary equal of the pixel value and the following three bits are secret bits, then three bits embedded into first eight bits [21,22], now it will change to 00110100. This method is very easy to implement as well as it provides high-level security to the data [23, 24]. After embedding the data into an image it remains the same.

B. Pixel value differencing method:

Wu & Tsai proposed this technique. Image pixels are grouped as two consecutive pixels. The difference between these two pixels is used to determine how many bits are embedded in that pair of pixel [25]. The range table and constant k value also play a vital role in this technique. This method can embed very high payload compared with LSB method, and the payload will be increasing at the edge points. This method is an eye-opener for several research people; and by following this method many more new methods have been invented [26-29].

C. Exploiting modification in all direction:

This is one of the familiar methods in steganography. It will embed high-level bits with minimal changes in the image. The pixel value may change over either +1 or -1.It produced high PSNR value compared with the previous methods.[30] This method describes the high payload procedures HOEMD and ADEMD, which are working as direction based, initially to find which direction is capable to embed more bits, and that direction is used for the same. These procedures also face the problem like as overflow and underflow, to overcome that [31] is introduced formula based insertion, in that lookup matrix also has been utilized in the [32] GMED – Generalized embedding n+1 binary bits that are embedded into an adjacent pixel. These methods provide high-level security to the stego image. The familiar Stego analysis algorithms failed to identify the secret data which is embedded inside the stego image, and they provide good security to the data.

D. Multi base notation system (MBNS):

In general the secret data were converted into binary notation and then it will be embedded into images; but in the MBNS model the binary secret bits were converted into any one of the following numbers system binary, octal or decimal [33].The embedding pixel is selected by the way of the surrounding pixels in all direction; based on the higher difference between the pixels are used to embed the secret bits. Mostly the edge pixels were commonly used to store more data bits. This method also provides good results [34, 35]. In general sender and receiver will select the same base number to convert the secret message bits. This method provides minimal payload as well as a good result, stego key place the major role.

E. Edge based methods:

In generic the steganography methods read the pixel from the selected image and then embed into that the secret bits, but in edge-based methods embedding procedure are differed from other methods, here the secret bits are embedded in two methods they are in a smooth area and another is edge area of the image. The smooth area embeds the small number of bits and in other end edge area more number of bits is embedded in [36] which describes very clearly about the edge detection methods like Canny and Sobal. These methods produce high PSNR value for the stego images. The paper [37] introduces edge adaptive method connected with matrix encoding and this idea produces high payload with minimal distractions compared with simple LSB Technique and PVD method. These methods also give the special protection to the data at the same time it will not be detectable by new steganography analysis algorithms.

Transform domain steganography types are explained as follows.

F. Discrete Fourier transforms (DFT):

In a DFT, 2DFourier transform technique has been used. The selected image is broken down into n corresponding frequency value of sin and cos value in Fourier transformation [38].The selected image has been modulated based as a secret data value.

Using this technique data will be embedded and retrieved from the image. Many more new ideas emerged followed by the DFT technique; many authors [39 - 41] utilizing this model proposed methods which at the time of retrieval of data from the image, if the frequency value does not match then will throw the error due the transform techniques. Using this idea provides a one more additional level of security to the data.

G. Discrete cosine transforms (DCT):

In a DCT converts the selected image into the frequency domain and the co-efficient are altered based on the message bits. The image will be split into three following steps as follow high, middle, and low parts based on that only embedding algorithm has been used in [42]. The image will be split by two pixel paired groups then the pixel value that is nearby to zero is used to embed the secret data bits. These methods produce high PSNR value [43, 44] as well as high data capacity.

H. Discrete wavelet transforms (DWT):

This method mainly overcomes the failure or data retrieve error over the DFT and DCT by the way of using forward and backward transformation. In[45] while using DWT steganography algorithm the following idea is utilized. To embed the secret bit, it moves horizontal, vertical and diagonal and finds the best places for embedding the secret data, but it will embed only the limited data; it produces the high PSNR value like 45.34 [46] [47].In general, the image steganography methods are transferring the data inside the selected image. The image will be split into a different model or scanned in different ways. The embedding procedure uses the image to insert the data and after that processing starts; the image will be called a stego image. Stego image is shared to receiver side from the sender side through the network medium, the safety of the stego image at the time of transferring becomes a very big issue, if any intruder will make change in the image, and then a receiver could not get the original message perfectly. The proposed method overcomes the issue as follows; it will not share the stego image. Without sharing the stego image then how the secret message will be shared by both end, explained in detail below.

III. PROPOSED WORK

This chapter explains the proposed work and algorithm. Initially, the user has to select anyone image from the library, that contains selective images satisfying the condition, that the images have all the values in between 0 – 255.

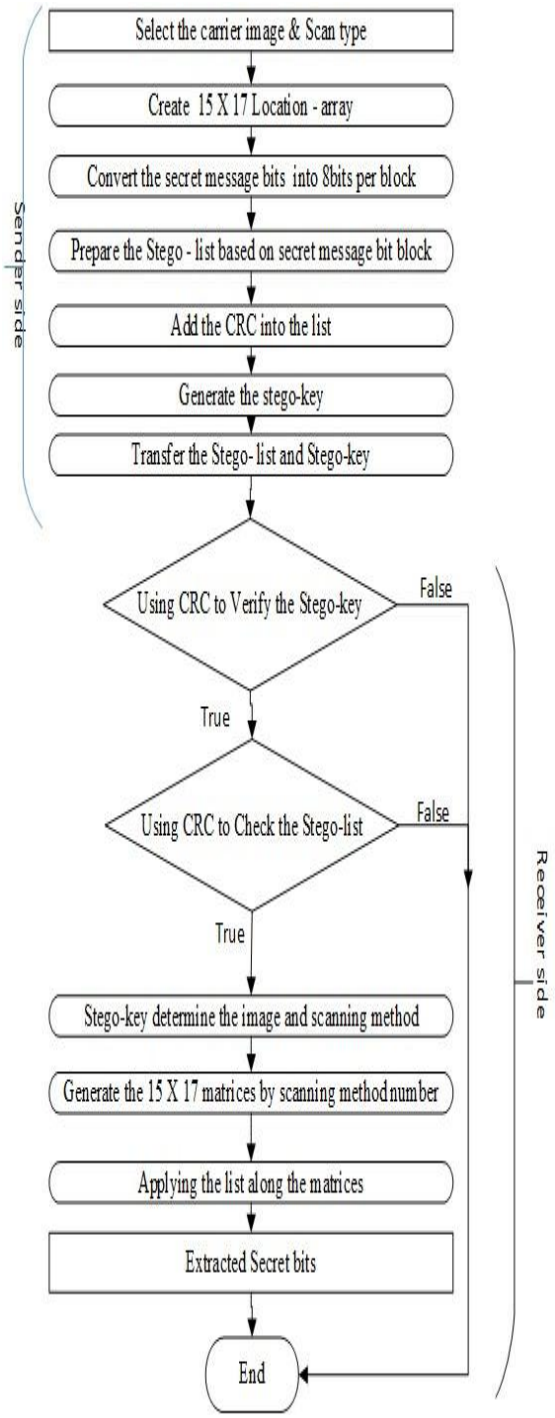

Figure 2: Flow chart

The secret message bits were composed into 8 bits blocks; each block has to be converted into their decimal equivalence as shown in the following diagram.

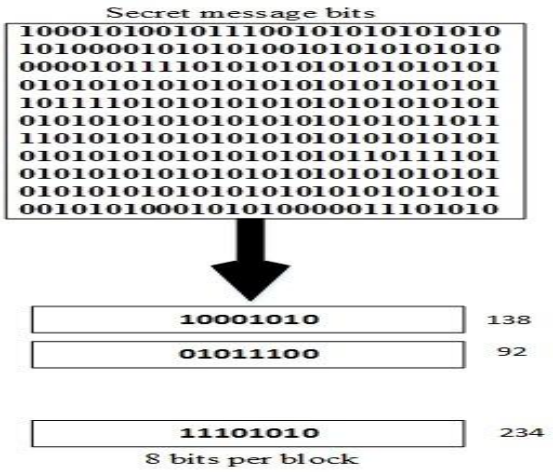

Figure 3: Secret message splitting

The scanning methods are listed as a – d respectively.

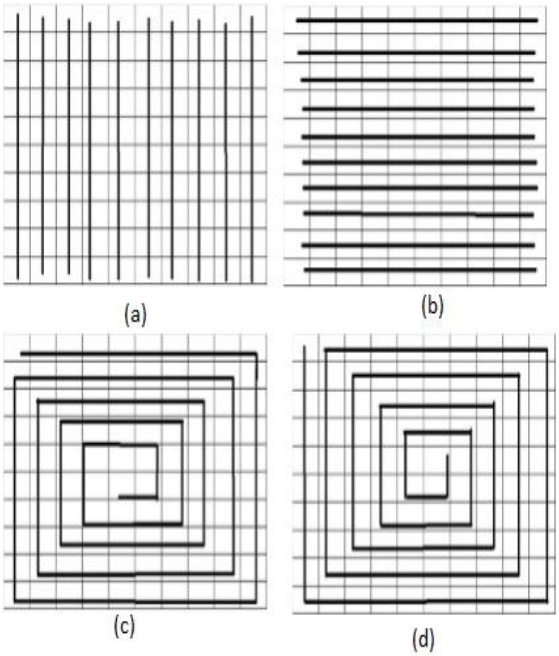

Figure 4: Scan methods

(a) Columnscanning, (b) row scanning, (c) spiral from left to right and (d) spiral right to left.

Scan an image by anyone method from the above description. While scanning the image, the value of each pixel lies between 0 and 255. The value may fall in random order or depends upon the color combination of the selective image. The following procedure is used to store the pixel value in a sequential order like to be a 1 to 255 into 15 x 17 location array. The pixel value 0 is said to be 8bit zero like as 00000000. The first occurrence of every value from 1 to 255 only takeas an account; in this manner, all the numbers are identified and stored into a 15 x 17 location array in a sequential manner. In the location array (1, 1) contains the location of one, (1, 2) contains the location of two and (15, 17) have the location of 255 respectively. At the end 15 x 17 location array has all the values from 1 to 255.The stego list will construct as follows. The decimal equivalence of the secret bit blocks finds the index value in the location array then adds into the stego-list in sequential order. In the list, the cyclic redundancy checker (CRC) value will be inserted for all the values. Stego-key consists of 12 binary bits, they are split as follows; bits (1-3) – represents image index number, (4-6) – denotes scanning method, (7-9) – is CRC value index number and (10-12) signifies CRC bits for the stego-list. At the receiver side, one has to check the stego-list first by using CRC bits; if it returns true then only scan the list from left to right and convert every three binary bits to decimal equivalent, based on the decimal value receiver can know the image index value and scanning method already utilized by the sender. With the help of those values, the receiver selects the image and performs the same scan method, then using a similar procedure to create the same 15 x 17 location array at the receiver end too. The stego-list has been verified by CRC values; if it returns true then, the list has to be read from left to right in a sequential manner. The stego-list contains only the index values of the location array; based on that value, the location array will be referred and the pixel value is got. Finally, these values are arranged in a sequential manner, and the receiver gets the original message sent by the sender side.

IV. RESULTS AND DISCUSSION

The receiver accepts the two different lists only; they are named as stego-list and stego-key. This chapter explains how it is prepared and processed on both sides. The creation of stego-key is explained in the above section, it contains four different fragments named as follows; image index, scan index, CRC index, and CRC value for the list. At the moment of creating a stego-key the first consecutive nine bits are select by the sender; based on these values stego-key is created, then it will be divided by modulo 2 division with common CRC polynomial x^3+x^2+1, which means 1101modulo 2 divides the first successive nine bits; then the remaining three bits will be added in the stego-key at last, by this way the stego-key will be created by sender side. Let's assume the values as follows;

Image index	Scan index	CRC index	CRC value
06	01	01	
$(110)_2$	$(001)_2$	$(001)_2$	$(001)_2$

$(1100010001)_2$ modulo division 2 by $(1101)_2$the remainder is 001, these three bits were treated as CRC value. After all the process the stego-key becomes $(110001001001)_2$.Once the stego-key is obtained by the receiver, it has to be verified by common CRC polynomial value. The continuous 12 binary bits were divided by 1101using modulo 2 division methods; if it produces remainder as 000, then only the retrieving of the secret data bits from the stego-list is processed or else it will not be processed. The creation of stego-list is as follows.

The image, scan method and CRC index selected by the sender, based on the first two values location array 15 x 17 is created. The secret message bits are split into 8 bits blocks, then it will be converted into binary bits to decimal; based on the decimal value, it identifies the location from the 15 x 17 location array, assume that decimal value is 177, it will show in the matrix in the location of (12, 14), and that location have the original position of 177 in the image and say suppose it is (123, 46). If it is to be stored into the location array it needs 8 bits per each row and column respectively to avoid the huge space requirement the location array is created. Instead of that (12,14) will processed as ; that value converted into four-bit binary, and five-bit binary like as (1100,01110); because of the upper limit of the location array is (15,17) the minimum requirement of bits to convert the 15,17 is 4 and 5 bits respectively, due to that reason only 4 and 5 bits were used. The selected CRC polynomial converted into binary notation,suppose the CRC polynomial is x^3+x+1 the binary value for the same is 1011.The binary value of location array is dividing by CRC binary value, that is 110001110 divide by modulo 2 division, the three-bit remainder (001), is shown as follows.

177	(12,14)	1100, 01110	1011	001	110001 110001

Finally, 110001110001 will be added in the stego-list.Receiver accept the stego-list only when all the elements should produce 000 as the remainder while divided by the CRC polynomial value; after that the stego-list scanned from left to right one by one, the first nine consecutive bits were used and the last three bits are omitted, these nine bits are converted into decimal based and the value refers the location array to get the pixel value; this process is done by all the elements in stego-list. The pixel values are arranged in sequential order, and then the original secret message from the receiver side is obtained. Generally,all the image steganography methods compute the PSNR value for the image to show their minimal changes in the same and undetectablefrom the human eye; PSNR value calculates as follows

$$PSNR = 10 \times \lg\left(\frac{255^2}{MSE}\right)$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left[I(i,j) - I'(i,j)\right]^2$$

It finds the difference between the image and stego-image. In the proposed method image is not used to embed the secret the data bits so that, it is not required to calculate PSNR value. This method provides high-level security to the data and ensures that the correct message will be received by the receiver.The proposed method is implemented in MatLab and produces good results. The running time of the program is optimal and the methods user-friendly. The stego-list requires little bit high memory to build, and due to the security concern it is not an issue. The previous methods can't identify any intruder attack at the transmission time, but the proposed method can easily identify the same by CRC value, so it needs the extra memory space for the same. It should be overcome in the future. The pictorial representation of the proposed method is given below.

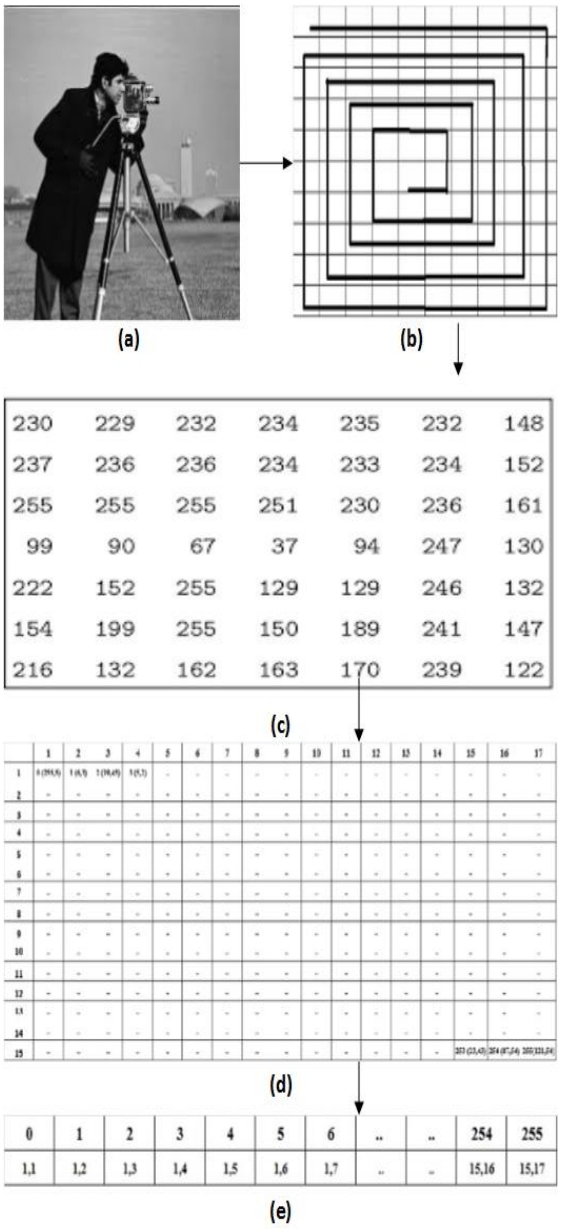

Figure 5: Functions of Proposed work

REFERENCES

1. F.A. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding-a survey, Proc. IEEE87 (1999) 1062–1078.
2. A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography:Survey and analysis of current methods, Signal Process. 90 (2010) 727–752.
3. M.S. Subhedar, V.H. Mankar, Current status, and key issues in image steganography:A survey, Comput. Sci. Rev. 13 (2014) 95–113.
4. M.C. Trivedi, S. Sharma, V.K. Yadav, Analysis of several image steganographytechniques in spatial domain: A survey, in: Proceedings of the Second InternationalConference on Information and Communication Technology for Competitive Strategies,ACM, 2016, p. 84.

5. S.N. Kishor, G.K. Ramaiah, S. Jilani, A review on steganography through multimedia,in Research Advances in Integrated Navigation Systems, RAINS, InternationalConference on, IEEE, 2016, pp. 1–6.
6. F. Djebbar, B. Ayad, K.A. Meraim, H. Hamam, Comparative study of digital audiosteganography techniques, EURASIP J. Audio Speech Music Process. 2012 (2012)1–16.
7. S.J. Murdoch, S. Lewis, Embedding covert channels into TCP/IP: InternationalWorkshop on Information Hiding, Springer, 2005, pp. 247–261.
8. W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, Retransmission steganography, and
9. its detection, Soft Computing. 15 (2011) 505–515.
10. K.N. Santoso, L. Suk-Hwan, W.-J. Hwang, K. Ki-Ryong, Information hiding innon-codingdna for dna steganography, IEICE Trans. Fundam. Electron.Commun.Comput. Sci. 98 (2015) 1529–1536.
11. M.M. Sadek, A.S. Khalifa, M.G. Mostafa, Video steganography: A comprehensivereview, Multimedia Tools Appl. 74 (2015) 7063–7094.
12. E. Zielińska, W. Mazurczyk, K. Szczypiorski, Trends in steganography, Communication.ACM 57 (2014) 86–95.
13. M. Kharrazi, H.T. Sencar, N. Memon, Performance study of common imagesteganography and steganalysis techniques, J. Electron. Imaging 15 (2006). 041104–041104g–041116.
14. A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: survey and analysis of current methods, Signal Processing 90 (2010) 727–752.
15. R.J. Anderson, F.A.P. Peticolas, On the Limits of Steganography, IEEE J. Sel. Ar- easComm (1998) 16 - 20 .
16. D. Artz, Digital steganography: hiding data within data, IEEE Int. Computer (2001) 75–80. [16] M. Juneja, P.S. Sandhu, Designing of robust image steganography technique based on LSB insertion and encryption, in Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, 2009, 302–305.
17. R. Srikumar, C.S. Malarvizhi, Strong encryption using steganography and digital watermarking, in Proceedings of the 22nd Picture Coding Symposium, 2001, 425–428.
18. S.B. Sasi, N. Sivanandam, A survey on cryptography using optimization algorithms in WSNs, Indian J. Sci. Techno 8 (2015) 216–221. [19] N.F. Johnson, S. Jajodia, Exploring steganography: Seeing the unseen, Computer (Long. Beach. Calif) (1998) 31-37.
19. C.-K. Chan, L.-M. Cheng, Hiding data in images by simple LSB substitution, PatternRecognit. 37 (2004) 469–474.
20. B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis,J. Inform.Hiding Multimedia Signal Process. 2 (2011) 142–172.
21. H. Yang, X. Sun, G. Sun, A high-capacity image data hiding scheme using adaptiveLSB substitution, Radioengineering 18 (2009) 509–516.
22. Z.-H. Wang, C.-C.Chang, M.-C. Li, optimizing least-significant-bit substitutionusing cat swarm optimization strategy, Inform. Sci. 192 (2012) 98–108.
23. K.-H. Jung, K.-Y.Yoo, Steganographic method based on interpolation and LSBsubstitution of digital images, Multimedia Tools Appl. 74 (2015) 2143–2155.
24. D.-C. Wu, W.-H.Tsai, A steganographic method for images by pixel-value differencing,Pattern Recognit.Lett. 24 (2003) 1613–1626.
25. K.-C. Chang, C.-P.Chang, P.S. Huang, T.-M.Tu, A novel image steganographicmethod using tri-way pixel-value differencing, J. Multimedia (2008) 37–44.
26. H.-C. Wu, N.-I.Wu, C.-S.Tsai, M.-S.Hwang, Image steganographic scheme basedon pixel-value differencing and LSB replacement methods, IEE Proc.-Vision ImageSignal Process. 152 (2005) 611–615.
27. K.-H. Jung, High-capacity steganographic method based on pixel-value differencingand LSB replacement methods, Imaging Sci. J. 58 (2010) 213–221.
28. C.-H. Yang, S.-J.Wang, C.-Y.Weng, Capacity-raising steganography using multipixeldifferencing and pixel-value shifting operations, Fund. Inform. 98 (2010)321–336.
29. X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modificationdirection, IEEE Commun. Lett. 10 (2006) 781–783.
30. T.D. Kieu, C.-C.Chang, A steganographic scheme by fully exploiting modificationdirections, Expert Syst. Appl. 38 (2011) 10648–10657.
31. W.-C. Kuo, S.-H.Kuo, Y.-C. Huang, Data hiding schemes based on the formalimproved exploiting modification direction method, Appl. Math. Inf. Sci. Lett. 1(2013) 1–8.
32. S. Geetha, V. Kabilan, S. Chockalingam, N. Kamaraj, Varying radix numeral systembased adaptive image steganography, Inform. Process.Lett. 111 (2011) 792–797.
33. M. Tang, W. Song, X. Chen, J. Hu, An image information hiding using adaptationand radix, Optik 126 (2015) 4136–4141.
34. W.-S. Chen, Y.-K.Liao, Y.-T.Lin, C.-M.Wang, A novel general multiple-base dataembedding algorithm, Inform. Sci. 358 (2016) 164–190.
35. W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSBmatching revisited, IEEE Trans. Inf. Forensics Secure. 5 (2010) 201–214.
36. W.-J. Chen, C.-C.Chang, T.H.N. Le, High payload steganography mechanism using a hybrid edge detector, Expert Syst. Appl. 37 (2010) 3292–3301.
37. P. Premaratne, C.C. Ko, Image blur recognition using under-sampled discrete Fourier transform, Electron. Lett. 35 (1999) 889–890.
38. A .S. Khashandarag, A .H. Navin, M.K. Mirnia, H.H. Agha Mohammadi, An optimized color image steganography using LFSR and DFT techniques, Commun. Comput. Inf. Sci. 176 (2011) 247–253
39. A. Soni, J. Jain, R. Roshan, Image steganography using discrete fractional Fourier transform, in Proceedings of the 2013 International Conference on Intelligent Systems and Signal Processing, 2013, pp. 97–100.
40. J. Sang, H. Xiang, H. Hu, Discrete Fourier transform-based information steganography, HuazhongKejiDaxueXuebao (ZiranKexue Ban)/Journal Huazhong Univ. Sci. Technol. 36 (2008) 5–8.
41. G. Savithri, S. Mane, J.S. Banu, Parallel Implementation of RSA 2D-DCT Steganography and Chaotic 2D-DCT Steganography, in Proceedings of the IEEE International Conference on Computer Vision and Image Processing, Springer, 2017, pp. 593–605.
42. C.Y. Weng, C.T. Huang, H.W. Kao, DCT-based compressed image with re- visibility using modified quantization, in Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Springer, 2018, pp. 214–221.
43. W.S. Sari, E.H. Rachmawanto, D.R.I.M. Setiadi, C.A. Sari, A Good Performance OTP encryption image based on DCT-DWT steganography, Telkom- Nika (Telecommunication Comput, Electron. Control. 15 (2017) 1987–1995.
44. M.R.D. Farahani, A. Pourmohammad, A DWT based perfect secure and high capacity image steganography method, in Proceedings of the Parallel and Distributed Computing, Applications and Technologies, 2014, pp. 314–317.
45. S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, B. Gupta, Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain, Multimed. Tools Appl. 76 (2017) 18451–18472.
46. M.S. Subhedar, V.H. Mankar, Image steganography using redundant discrete wavelet transform and QR factorization, Comput.Electr. Eng. 54 (2016) 406–422.

AUTHORS PROFILE

Dr. S.RAJALAKSHMI, is working as a Professor, Department of CSE, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya,(SCSVMV) Enathur, Kanchipuram, India. Her area of research is Network Security. Nine research scholars have completed PhD under her guidance and four more scholars are pursuing research.

V.RAJA, is working as an Assistant Professor, Department of Computer Science and Applications, S.R.M Institute of Science and Technology, Chennai, India. His area of research is Network Security. He is doing Ph.D in Bharathiar University, Coimbatore, India.