Secure and Robust Digital Watermarking on Grey Level Images

G.RoslineNesaKumari[1], B. VijayaKumar[2], L.Sumalatha[3], and Dr V.V.Krishna[4]

[1]Research Scholar- Dr MGR University Chennai, T.N.India & Associate Professor, Godavari Institute of Engineering and Technology, Rajahmundry, A.P.India
[2]Professor & Head, Department of CSE, Lords Institute of Engineering & Technology, Hyderabad, A.P. India
[3]Associate Professor & Head Department of CSE, University College of Engineering, JNTU Kakinada, A.P.India
[4]Professor of CSE and Principal, Chaitanya Institute of Engineering and Technology, Rajahmundry, A.P., India

rosemaruthu@gmail.com,vijaysree.b@gmail.com,jsasikiranj@yahoo.co.in, vakula_krishna@yahoo.co.in

Abstract

A good watermarking technique embeds information into a carrier image with virtually imperceptible modification of the image. The present paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB), the grey value of the image pixel either remains same or increases or decreases to one. The present paper is focused on this issue and found that such ambiguity of grey level values by LSB method comes between successive even and odd grey level values only. The proposed method inserts hidden message on m x m windows, based on their grey level values and coordinate positions. The present approach allows high robustness, embedding capacity and enhanced security. A detailed algorithm is furnished along with the results of its application on some sample images.

Keywords: *grey level value; watermark; even and odd; robustness*

1. Introduction

The rapid growth of the Internet increased the access to multimedia data tremendously [1]. The development of digital multimedia is demanding as an urgent need for protect multimedia data in internet. Digital watermarking technique provides copyright protection for digital data [2-4]. The digital watermarking technique is proposed as a method to embed perceptible or imperceptible signal into multimedia data for claiming the ownership. A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data. This piece of information known as watermark, a tag, or label into multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video, or text [5]. Watermark enables many applications listed below. A. Copy Control - Watermark may contain information required by the content owner that decides the policy of copying the digital content [1, 6]. B. Digital signatures - Watermarks may be used to identify the owner of the content [6]. C. Authentication - Watermark is used to provide authenticity. D. Broadcast monitoring - Automatic identification of owners of data may be required to be done and used in systems responsible for monitoring the broadcasts.

E. Fingerprinting - Watermarks may be used to identify the content buyers. This may help in tracing illegal copies. F. Secret communication - The technique of watermarking is also used in transmitting secret information from source to destination by a hidden way [7]. Each watermarking application has its own requirements that determine the required attributes of the watermarking system and drive the choice of techniques used for embedding the watermark [8]. This demand has been lately addressed by the emergence of a variety of watermarking methods. Such methods target towards hiding an imperceptible and undetectable signal in the original data, which conveys copyright information about the owner or authorized user. Data hiding usually involves the use of secret keys possessed only by owners or authorized users. In order to verify the multimedia content owner and thus protect his copyrights, detection is performed to test whether the material in question is watermarked with his own secret key [26 -28]. Recent research trend in watermarking technique is focusing more on image data [9, 10, 11, 12, 13]. But watermarking is not limited to only images; but there are also watermarking techniques for audio [14, 15], video [16, 17, 18], and text [19, 20, 21, 22, 23, 24] data. Watermarking for black and white text data; e.g., electronic documents and manuscripts, is so-called binary watermarks [25]. Watermarks and Watermarking techniques can be divided into various categories. The watermarks can be applied either in spatial domain or frequency domain. The spatial domain watermarking schemes have less computational overhead compared with frequency domain schemes. The process could be adjusted to the image components or feature vectors to achieve a higher level of invisibility. In general, the watermark W(X) is integrated into the image components C(x, y) by a factor that allows amplification of the watermarking values in order to obtain the best results. LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Considering a basic grey scale image, the pixel and its values can be sliced up into significant and irrelevant levels. Because the significant levels merely represent a digital noise pattern, it could be easily used for digital watermarking. In changing the selected pixel values of the noise pattern using a special or key-based algorithm, the watermarking information can be easily integrated.

The present paper proposes a new architecture platform for secure grey level modification watermarking system, which embeds binary data with in the spatial domain of the grey scale images by modifying the grey level values. This paper is organized as follows: In section II methodology is given. The results and discussions are given in section III and the final section gives conclusions.

2. Methodology

Any image is represented by a two dimensional array of values $f(x_i,y_j)$ where $0 \leq(i, j)\leq N$. The present paper divides the image into non overlapped window of a predefined size. Any window of size m x m will be having m^2 pixels. Each pixel in the window is represented by a location (x_i,y_j) and a grey level value p_i. By embedding a bit in LSB, the p_i value will have the following three cases. Case: 1 p_i values may be same, if the corresponding LSB of p_i and embedded bit is same i.e., 1 or 1 and 0 or 0. Case: 2 p_i values may be incremented by one, if LSB of p_i is zero and embedded bit value is one. Case: 3 p_i values may be decremented by one if LSB of p_i is one and embedded bit value is zero.

If the p_i is even, its LSB is zero there fore its value will be changing as represented in Case1 or Case 2. If the p_i is odd, its LSB is one, therefore its value will be changing as represented in Case1 or Case 3. Based on above three cases, the present method found that the ambiguity of pixel values will be arising at the time of reconstruction between successive even and odd values. To overcome this present method treated the successive even and odd values of the window as same, i.e., n_i and n_i+1, where n_i is an even number, and the difference of n_i+1 and n_i is always one. While embedding the watermark the order of selection of the hit pixels in the window is based on the least co-ordinate position. The entire process of embedding the information is given in the form of flowchart in figure: 1.

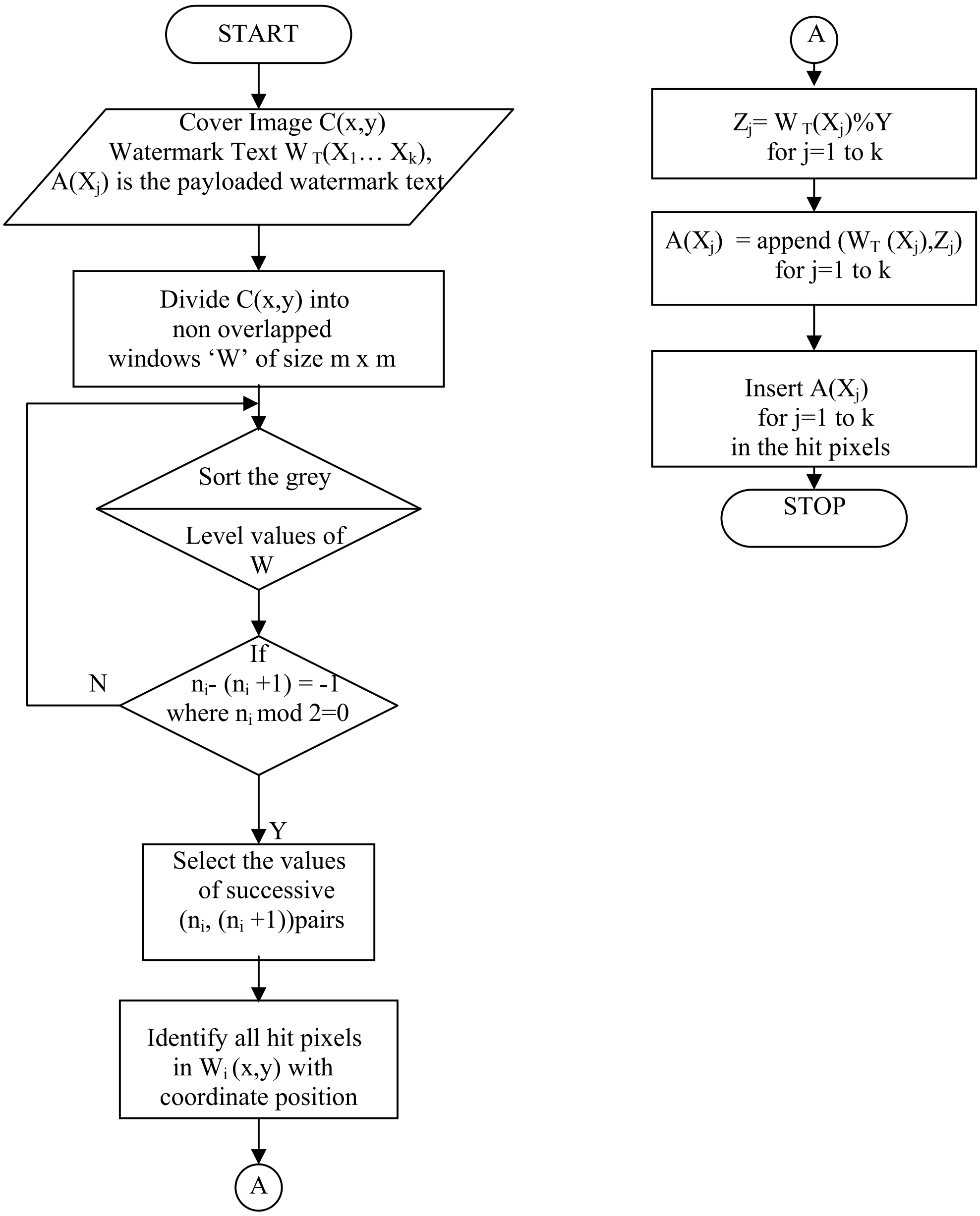
START
Cover Image C(x,y)
Watermark Text W T(X1… Xk),
A(Xj) is the payloaded watermark text
Divide C(x,y) into non overlapped windows 'W' of size m x m
Sort the grey Level values of W
If ni- (ni +1) = -1 where ni mod 2=0
N
Y
Select the values of successive (ni, (ni +1))pairs
Identify all hit pixels in Wi (x,y) with coordinate position
A
A
Zj= W T(Xj)%Y for j=1 to k
A(Xj) = append (WT (Xj),Zj) for j=1 to k
Insert A(Xj) for j=1 to k in the hit pixels
STOP

Figure 1. Flow Chart for the Proposed Scheme.

The present method is explained for the grey level image of figure2. The Table1 gives the sorted list of grey level values with the co-ordinate position of figure2. For the image of figure 2 the present method considers the pair of values (80,81), (78,79),(76,77), and (74,75) as same in the ascending order. To over come the further ambiguity between the successive even and odd values the hit pixel will be selected based on the least x co-ordinate position. Based on this the first hit pixel will be selected from the coordinated position (0,3) for the image of figure2 as shown in Table 1.

78	75	79	80	81
81	80	81	81	80
76	75	76	75	80
78	77	79	78	75
80	81	75	74	73

Figure 2. Grey Level values of the image 5X5.

Table 1. Sorted grey level values with the coordinate position of figure2.

Coordinate positions		p_i (x_i,y_j)
x_i	y_j	
4	4	73
4	3	74
0	1	75
2	1	75
2	3	75
3	4	75
4	2	75
2	0	76
2	2	76
3	1	77
0	0	78
3	0	78
3	3	78
0	2	79
3	2	79
0	3	80
1	1	80
1	4	80
2	4	80
4	1	80
0	4	81
1	0	81
1	2	81
1	3	81
4	1	81

The present method considers the watermark text as “srinivasa ramanujan research forum giet rajahmundry”. Each watermark character value is divided by mod Y, and the remainder is appended to the watermark text character. Appending may be carried out in left side, right side or at any position of the watermark text character. The present paper appends the remainder values on the right side of the watermark text character.

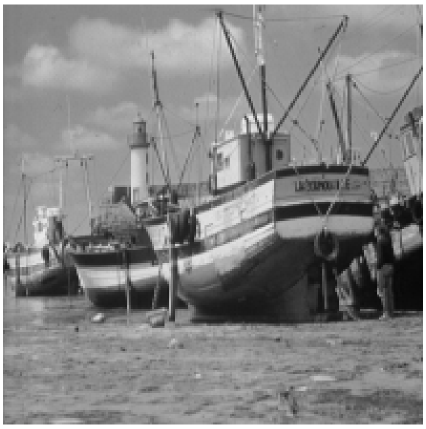

Figure 3(a)

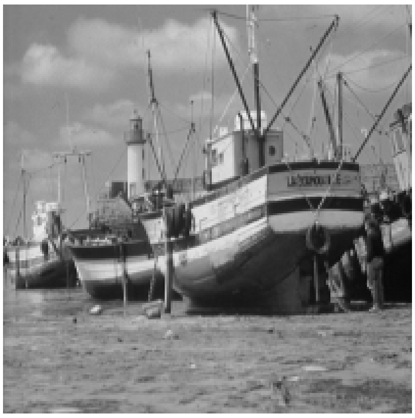

Figure 3(b)

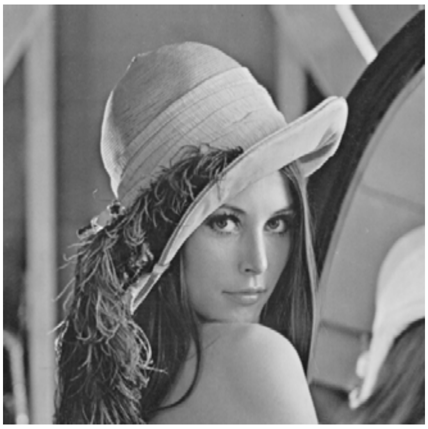

Figure 4(a)

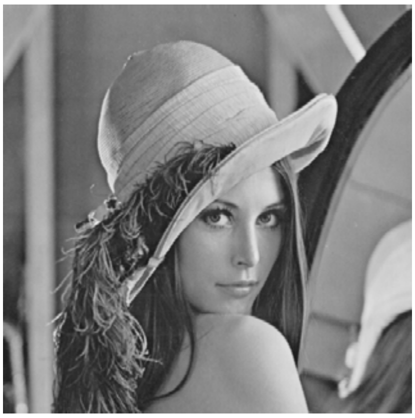

Figure 4(b)

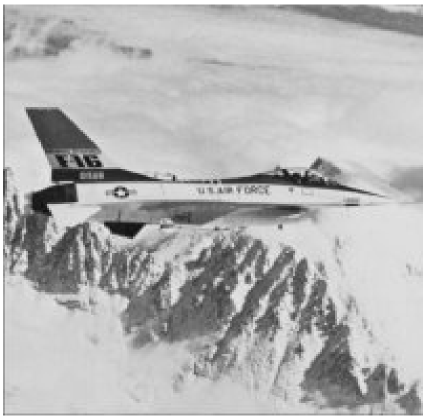

Figure 5(a)

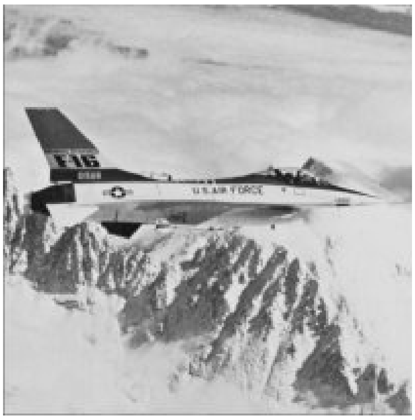

Figure 5(b)

3. Results and Discussions

The proposed method is applied on more than 32 different images with different sizes. However the present paper shows four of them of size 100X100.The figures 3(a),4(a),5(a), 6(a) indicates the original or cover image of fishing boat, lena, flight and peppers image respectively. The figures 3(b),4(b),5(b),6(b) indicates the watermarked image with the text "srinivasa ramanujan research forum giet rajahmundry" inserted on the cover image. The results clearly indicate the imperceptibility, obtrusiveness, robustness and unambiguous nature of the present method. The present paper converted each character of the watermarked text as 12 bit code by dividing each character value by mod9. The four bit remainder is appended to make 8 bit text character, as 12 bit character.

Figure 6(a)

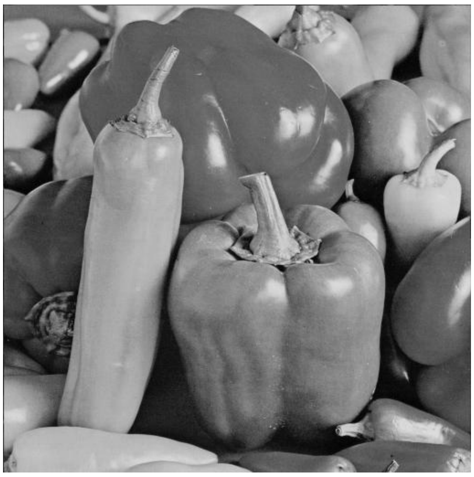

Figure 6(b)

Figure 3(a), 4(a),5(a),6(a) : cover images

Figure 3(b),4(b),5(b),6(b) : watermarked images with watermark text as "srinivasa ramanujan research forum giet rajahmundry".

4. Conclusion

The proposed watermarking method is having high robustness, embedding capacity and enhanced security because watermark text is inserted based on the grey level values and its co-ordinate position. The present method identified and would overcome with a solution for the ambiguity of grey level values, which arose between successive even and odd values after inserting the watermark using LSB. Future work includes extending the method based on descending order of pixel grey level values and appending more number of bits for each character, which makes the method as more dynamic. And it will become more difficult to break the watermark. The present method can also be applied on any window irrespective of its size.

References

[1]Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6,pp. 1673–1687, Dec. 1997.

[2] N. Nikolaidis and I. Pitas, " Copy right Protection of images using robust digital signatures", in proceeding , IEEE International Conferences on Acoustics, Speech and signal processing , Vol.4, May 1996,pp. 2168-2171.

[3] Houng.Jyh Wang and c.c, Jay Kuo, " Image protection via watermarking on perceptually significant wavelet coefficient", IEEE 1998 workshop on multimedia signal processing, Redondo Beach, CA, Dec, 7-9,1998.

[4] S.Craver, N. Memon, B.L and M.M Yeung "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implication", IEEE Journal on selected Areas in communications. Vol.16 Issue:4, May 1998, pp 573-586.

[5] S.Katzenbeisser and F.A.P. Petitcolas, Information Hiding Techniques for steganography and Digital Watermarking. Norwood,MA: Artech House,2000.

[6] M.Swanson, B.Zhu, and A. Tewfik, "Transparent Robust Image Watermarking", Proc. IEEE Int. Conf on Image Processing, Sept.1996, Vol.III.pp 211-214.

[7] I.Pitas, "A method for signature casting on digital images", Proc. IEEE Int. Conf on Image Processing, Sept.1996, Vol.III.pp 215-218.

[8] Ravik. Sharma, and SteveDecker," Practical Challenges for Digital Watermarking Applications", Proc. IEEE,2001.

[9] G. Braudaway, "Results of attacks on a claimed robust digital image watermark," In Proceedings of the IS&T/SPIE Symposium onOptical Security and Counterfeit Deterrence Techniques, SPIE, pp. 122-131, 1998.

[10] G. Braudaway, K. Magerlein, and F. Mintzer, "Color Correct Digital Watermarking of Images," U.S. Patent 5 530 759, June 25, 1996.

[11] H. Gladney, F. Mintzer, and F. Schiattarella, "Safeguarding digital library contents and users: Digital images of treasured antiquities," DLIB Mag., 1997; see www.dlib.org/dlib/july97/vatican/07gladney.html.

[12] F. Mintzer, G. Braudaway, and M. Yeung, "Effective and ineffective image watermarks,"In Proceedings of the IEEE ICIP'97, pp. 9-12, 1997.

[13] J. Zhao, and E. Koch, "Embedding Robust Labels into Images for Copyright Protection," Proceedings of the KnowRight'95 conference, pp. 242 – 251, 1995. [14] L. Boney, A.H. Tewfik, and K.N. Hamdy,

"Digital Watermarks for Audio Signals," Proceedings of MULITMEDIA'96, pp. 473- 480, 1996.

[15] M. Swanson, B. Zhu, A.H. Tewfik, and L. Boney, "Robust Audio Watermarking using Perceptual Masking," Signal Processing, (66), pp. 337-355, 1998.

[16] M. Swanson, B. Zhu, and A.H. Tewfik, "Data Hiding for Video in Video," Proceedings of the IEEE International Conference on Image Processing 1997, Vol. II, pp. 676-679, 1997.

[17] M. Swanson, B. Zhu, and A.H. Tewfik, "Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation," Proceedings of the IEEE International Conference on Image Processing 1997, Vol. II, pp. 558-561, 1997.

[18] M. Swanson, B. Zhu, A.H. Tewfik, "Object-based Transparent Video Watermarking," Proceedings 1997 IEEE Multimedia Signal Processing Workshop, pp. 369-374, 1997.

[19] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying," IEEE J. Select. Areas Commun., Vol. 13, pp.1495-1504, Oct. 1995.

[20] S. Low, N. Maxemchuk, J. Brassil, and L. O'Gorman, "Document Marking and Identification Using Both Line and Word Shifting," In Proc. Infocom'95, 1995.

(Available WWW: http://www.research.att/com:80/lateinfo/projects/ecom.html.)

[21] N. Maxemchuk, "Electronic Document Distribution," AT&T Tech. J., pp. 73-80, Sept. 1994.

[22] SysCoP, http://www.mediasec.com/products/products.html.

[23] P. Vogel, "System For Altering Elements of a Text File to Mark Documents," U.S. Patent 5 338 194, Feb. 7, 1995.

[24] J. Zhao and Fraunhofer Inst. For Computer Graphics (1996). [Online]. Available WWW:

http://www.igd.fhg.de/~zhao/zhao.html.

[25] A. Shamir, "Method and Apparatus for Protecting Visual Information With Printed Cryptographic Watermarks," U.S. Patent 5488664, Jan. 1996.

[26] J. Hernandez, F. Perez-Gonzalez, Statistical analysis of watermarking schemes for copyright protection of images, Proc. IEEE 87

(7) (1999) 1142}1166.

[27] N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain (special issue on copyright protection and access

control), Signal Processing 66 (3) (1998) 385}403.

[28] G. Voyatzis, I. Pitas, The use of watermark in the protection of digital multimedia products, (special issue on identi"cation and

protection of multimedia information), Proc. IEEE 87 (7) (1999) 1197}1207.

Authors

G Rosline NesaKumari received her M.E., from Sathyabama University Chennai in 2005. She is having nine years of teaching experience. She is now with Godavari Institute of Engineering and Technology Rajahmundry India as an Associate Professor. She is pursuing her Ph.D in Computer Science and Engineering at Dr MGR University Chennai under the Guidance of Dr V VijayaKumar. Her research interest includes Image processing, Digital Watermarking, Steganography and Security. She is a life member of ISCA, IAENG.

B Vijaya Kumar completed his M S in CSE from DPI, Donetsk, USSR in 1993. He worked as Software Engineer in Serveen Software Systems pvt. Ltd. Secunderabad, India for four years (1993-1997). After that he worked as Sr. Assistant Professor in JBIET, Hyderabad for three years later joined in Royal Institute of Technology & Science, Hyderabad as Associate Professor and worked there for four years. Presently he is working as Professor & Head of CSE Department in Lords Institute of Engineering & Technology, Hyderabad, India. He is pursuing his Ph.D. in Computer Science under the guidance of Dr Vakulabharanam Vijaya Kumar. He is a life member of CSI, ISTE, NESA and ISCA. He has published more than 10 research publications in various National, Inter National conferences, proceedings and Journals.

L. Sumalatha completed her B.Tech from Acahrya Nagarjuna University and M.Tech CSE from JNT University Hyderabad. She is working as Head Departement of CSE College of Engineering JNT University Kakinada. She is having nine years of teaching experience. She is pursuing her Ph.D from JNT University Kakinada. Her research areas includes network security, digital imaging and digital watermarking.

V Venkata Krishna received B.Tech. (ECE) degree from Sri Venkateswara University. He completed his M. Tech. (Computer Science) from JNT University. He received his Ph.D in Computer Science from JNT University in 2004. He worked as Professor and Head for ten years in Mahatma Gandhi Institute of Technology, Hyderabad. Later he worked as a principal at VVCE, Hyderabad and CIST Kakinada. Presently he is working as Principal for Chaitanya Institute of Engineering and Technology, Rajahmundry. He is an advisory member for many Engineering colleges. He has published 20 research articles. Presently he is guiding 10 research scholars. He is a life member of ISTE and CSI.