International Journal of Computer and Electrical Engineering, Vol. 1, No. 4, October, 2009
1793-8163

Imperceptible Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding

S.Poonkuntran, R.S.Rajesh, and P.Eswaran

***Abstract*— This paper proposes an imperceptible watermarking scheme for digital fundus images. It is a pooled approach of two schemes proposed in [1] and [2]. Hiding a large amount of data (image, audio, text) file into color BMP images proposed in [1].It could achieve the better capacity in irreversible way which is not suitable for fundus images. The difference expanding method proposed for medical images in [2]. It suffered from imperceptibility. Hence, these two schemes were combined in the proposed scheme by addressing better capacity, imperceptibility, reversibility and robustness. The embedding process in the proposed scheme involves two steps. First step selects the pixel according to the color characteristics of the fundus images. Second step embeds the secret information into selected pixels by using the difference expanding method of the two pixels from different color planes. It is known as intra-plane difference expanding. It embeds more than one bit at each byte in one pixel of the fundus image and give us imperceptible results. This scheme is robust to statistical and visual attacks. The comparison results showed the improvement of imperceptivity to 15% in the proposed scheme with respect to the scheme proposed in [1]. It also identified that that 30000 bits is the optimum size of the watermark with good level of imperceptibility which is above 60 dB at an average.**

***Index Terms*— Fundus image processing; image watermarking; image authentication; integer transforms.**

I. INTRODUCTION

The security of medical images is attained from strict ethics and legislative rules which can be classified in three fixed characteristics: confidentiality, reliability and availability [3] [4] [5] [6] [7] [8] [9].

Confidentiality: It means that only the entitled users should have access to the images in the scheduled system.

Reliability: It is specified by two features. i) Integrity: Ensuring that the images have not been modified by unauthorized person. ii) Authentication: Ensuring the confirmation of the image belongings to the correct patient and correct source.

Availability: It is the capability of an image to be used by the permitted users in the normal scheduled conditions of access and exercise.

Providing security for medical imaging is very important, when the images are exchanged in inter and intra hospital networks. In such case, the first two characteristics have mainly to be considered. The watermarking scheme has been recognized as technique to control the image reliability by accentuating its integrity and authenticity [3] [8]. In general, watermarking modifies the grey level of the pixels of an image, to embed a secret message in it. For the image reliability, a proof of the image like digital signature and Image Identification Number (IIN) specified by the DICOM standard [3] [10]) are also embedded in the image. Other features of images can also be embedded by adding meta-data over the pixels without changing the image format. A digital watermark is a secret key represented as signal that is inserted into digital data (images, sound, and texts) and which can be later detected and extracted in order to verify. The location of watermark in the image determines two kinds of methods: The spatial domain methods which embed watermark information directly into images pixels. The frequency domain methods which embed watermark information in the transform domain. In medical images, modifications due to the insertion process are not accepted by physicians for diagnosis [3].Hence, the requirements in medical images are differed from multimedia applications [3] [11] [12]. A watermarking scheme can be defined by three properties:

Capacity: It refers to the number of bits per pixel (bpp) that can be used to embed the information.

Robustness: It refers to the survival ability of the embedded message to the insertion problems such as alteration in the pixels and information loss.

Invisibility: It refers that no external artifacts are generated due to the insertion process. The embedded information should be invisible under normal vision.

From the few studies conducted in the area of medical imaging security, the three possible solutions have been identified [3]. The first solution is embedding the watermark in Regions of Non-Interest [4] [11]. In these cases, regions of non-interest correspond to the black areas of the image. For example, In CT scan images, the background regions are used for embedding watermark. In this way, the watermark will not interfere with the information in foreground regions considered during the diagnosis. The second solution is based on reversible watermarking. Once the watermark has been detected or read, the reversibility guarantees that the watermark can be completely removed from the image, allowing retrieving the original image pixel values [12] [13] [14] [15] [16] [17] [18] [19]. The third solution is based on

Manuscript received April 9, 2009.

F. S.Poonkuntran is with the Royal College of Engineering and Technology, Akkikavu, Thrissur-680604, Kerala, India. He is working as an assistant professor in the department of computer science and engineering. He is currently doing his research studies in Manonmaniam Sundaranar University, Tirunelveli-627012, Tamilnadu, India. (Corresponding Author, Phone: 91-4885-271175; mobile: 91-9894432890 fax: 04885-289043;).

S. Dr.R.S.Rajesh is with the Manonmaniam Sundaranar University, Tirunelveli-627012, Tamilnadu, India. He is working as reader in the department of computer science and engineering. (Phone: 91-462 – 2330935, Mobile: 91-94438 69904).

T. P. Eswaran is with the Manonmaniam Sundaranar University, Tirunelveli-627012, Tamilnadu, India. He is working as research scholar in the department of computer science and engineering. (Mobile: 91-9865022233).

non-reversible watermarking method that will introduce reasonable modification as in lossy image compression methods. However in such case, there will be a proof which makes sure that the watermark will not introduce any suspicion during image verification. Always, there is a trade-off between capacity rate and the quality of the watermarked image at the embedding step. In [1], a new data hiding scheme has been proposed using color characteristics of the pixels. It hides the data into unwanted areas of the images that will be identified with many color differences. It gave high capacity rate and survived against visual and statistical attacks. But, it is irreversible. Hence, this cannot be applied to medical images. It requires reversible solutions which brings the originality of the images without any loss of information to its diagnosis. In [2], multiple layer data hiding scheme has been proposed to medical images. It uses the difference between the neighbor pixels for embedding the secret data and produces the reversible solutions. But, it failed to provide a reliable and confidential communication. Because, it generates high distortion when embedding takes place in multiple layer. Therefore, we developed a new reversible watermarking scheme for fundus images using the approaches in [1] and [2]. In this paper, we propose a reversible watermarking scheme for digital fundus images based on low distortion at high capacity rate in the embedding step. It gives no evidence for the intruders to suspect about the authentication mark in the images. It ensures the reliable and confidential communication.

The paper has been organized as follows. Section I gives the introduction to watermarking in medical imaging. Section II presents details on digital fundus images. The proposed water marking scheme is explained in Section III. Section IV shows the experimental results conducted on digital fundus images. Section V gives conclusion.

II. Digital Fundus Images

Ophthalmology is the branch of medicine which studies about the diseases and surgery of the visual pathways, including the eye, brain and areas surrounding the eye, such as eyelids. The fundus is the interior surface of the eye, including the retina, optic disc and macula. The fundus can be viewed with an ophthalmoscope. The fundus images are taken using a special camera called fundus camera. A fundus camera is a specialized low power microscope with an attached camera designed to photograph the interior surface of the eye. The example of fundus images is shown in fig.1 Fundus photograph is usually taken using a green filter to acquire images of retinal blood vessels. Green light is absorbed by blood and appeared darker color in the fundus photograph than the background and the retinal nerve fiber layer. Hence, the green channel of the fundus images posses the valuable information for diagnosis than other channels [3]. This was the key point which motivated us to develop a reversible watermarking scheme for digital fundus images using only red and blue channels of the images.

Retinal fundus images are useful for the early detection of a number of ocular diseases. If it is not treated that will lead to blindness. Examinations on retinal fundus images are cost effective and are suitable for mass screening. In this view, retinal fundus images are obtained in many health care centers during medical checkups. The increase in the population increases the workload of ophthalmologists in ocular health care. Therefore, modern health care systems are designed with Computer Aided Design (CAD) and networking for analyzing retinal fundus images. It can also assist with ophthalmologists towards reducing their workloads and improving the screening accuracy. Such modern health care systems require highly secure communication techniques for exchanging information from one place to other. In the point of security, the authentication is a fundamental step whose success prevents many problems in network. Developing user authentication is very much important in medical images, when it can be sent through network for getting suggestions and judgments from the medical science experts who are all in various geographical locations. Hence, this paper attempts to develop a secure authentication scheme for digital fundus images using reversible, multilayered watermarking scheme.

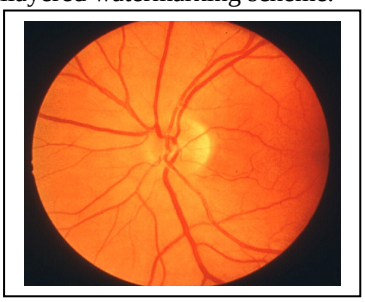

Figure 1. Digital Fundus Image.

III. The Proposed Scheme

The pixels of fundus image in the proposed scheme are in 24-bits or 3 bytes of RGB color. Each byte contains two nibble. The left nibble contains the highest value in the byte while the right nibble contains the lowest value in the byte. Therefore, any changes in the right nibble will cause a minimal change in a byte value.

Since, the nibble value is given in the interval [0, 15], it gives 16 levels. These levels are used for creating the priority of the colors. Thereby, we get 16 main color indexes *(MCindex)*. The main color index of the pixels is given by

$$MCindex = floor\ (ColorValue\ /16) + 1 \qquad (1)$$

Where ColorValue = {Red, Green, Blue}. The main color index values are used to create the priority values in order to embed the data in the proper pixels. The priority value Pr (MCindex) is calculated as follows:

$$Pr\ (MCindex) = MC - 17 \qquad (2)$$

The main color of the pixel is given by highest priority. Then, the rest colors of the pixels (RC) are chosen for embedding by using Eqn.3, the main color of the pixel is untouched.

$$MC = \min\ \{Pr\ (MCindex_i)\} \qquad (3)$$

The rest colors of the pixels are taken to integer transform for embedding. The integer transforms works as follows. For an 8-bit grayscale-valued pair (x, y), x, yεZ, 0$\leq$Z$\leq$255, the

integer average M and difference D are defined as follows:

$$M=\text{floor}((x+y)/2)$$

$$D=x-y \quad (4)$$

The inverse transform is defined as:

$$x'=M+\text{floor}((D+1)/2)$$

$$y'=M-\text{floor}(D/2) \quad (5)$$

The difference is expanded by using Eqn.6 for embedding.

$$D'=2*D+b \quad (6)$$

Where D′ is modified difference after embedding the embedded bit (b). The modified difference (D′) is calculated by satisfying the following condition in order to prevent the over flow or under flow during embedding process.

$$|D'| \le 2*(255-M) \quad \text{If } 128 \le M \le 255$$

$$|D'| \le 2*(M+1) \quad \text{If } 0 \le M \le 127 \quad (7)$$

If D' satisfies the Eq. (7), the D is expandable, otherwise D is unexpandable. An expandable difference can be used to hide secret information. If all the expandable differences are selected for data embedding, the capacity rate will reach its maximum limit [2]. Let N and Ne denote the number of difference and the number of expandable differences, respectively.

The hiding capacity of an image is defined as:

$$C=Ne/N \quad (8)$$

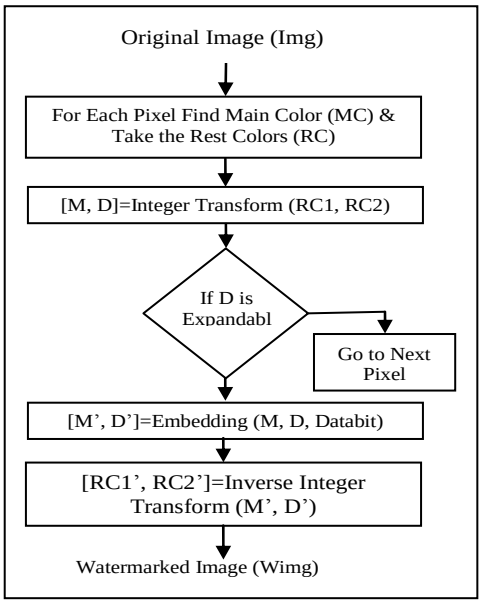

Figure 2. The proposed Watermarking process

Therefore, the hiding capacity of the image is proportional to the number of expandable difference. Thus, the proposed scheme embeds the secret data into the fundus image. The extraction process is reversible and which extracts the secret data and original image without any loss of information. For multilayer embedding, the same pixel pairs are selected for further data embedding. Here some of the differences may not be expandable for longer time [2].The proposed watermarking scheme is shown in fig.2.

IV. RESULTS AND ANALYSIS

The proposed watermarking scheme has been simulated in MATLAB 6.5 using around 150 digital color fundus images. These images were taken from DRIVE and STARE public databases [3] [4]. The images in the databases were in different formats. We brought it to the fixed size of 512×512×3, 8 bits per pixel in color channel and represented in TIF format.

A. Imperceptibilty and Reversibility

Medical sciences are very strict with the quality of images. Therefore, it is often not allowed to alter in any way the bit field representing the image. Hence, the watermarking method is designed as reversible, in that the original pixel values can be exactly recovered after extracting the watermark. This limits significantly the capacity and imperceptibility [8].

Figure 3. Secret Information embedded in the image

The secret information is a binary image of size 40×40 that represents identification mark (logo) as shown in fig.3. It has been used to authenticate the images. The image is then converted in to a binary sequence of length 1600.

To evaluate the proposed scheme quantitatively, we used peak signal to noise ratio(PSNR) in decibel (dB) between original image(I) and its watermarked version image(Iw).It has been found as best parameters in measuring the fidelity of the method [3].

$$PSNR(I, Iw) = 10\,Log_{10}\,[(2^p-1)^2/MSE] \quad (9)$$

For the comparative analysis, we have taken the algorithm given in [1]. This algorithm hides the large amount of data with high distortion and it is non-reversible. To minimize the distortion and bring the reversibility, it is modified in proposed scheme by using integer transform proposed in [2].

From the experiment, it is found that the proposed scheme improves imperceptibility to 15% at an average with respect to the algorithm in [1]. The sample images used in the test bed are shown in Figure 4 and whose PSNR values in both previous algorithm [1] and proposed scheme are tabulated in tab.1 and tab.2 respectively. As already mentioned, the imperceptibility and size of watermark are in tradeoff. To identify the best size of the watermark, the experiment conducted on a set of 100 fundus images and the corresponding imperceptibility has been calculated using PSNR (Peak Signal to Noise Ratio) between original image *(I)* and watermarked image *(Iw).*

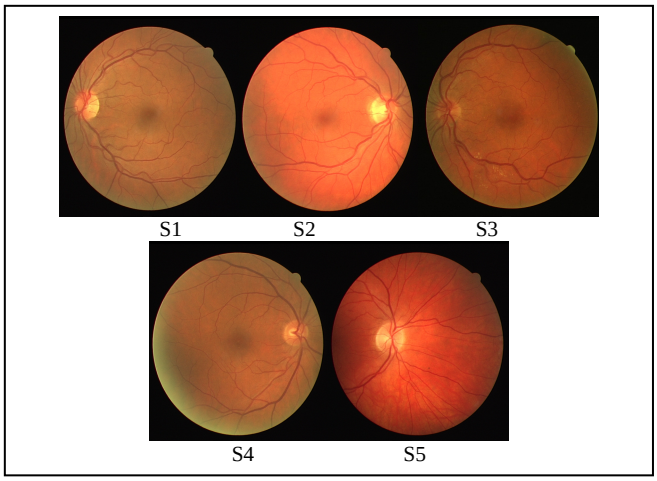

Figure 4. Sample Images used in the test bed

TABLE I. PSNR VALUES OF PREVIOUS ALGORITHM IN [1]

Sample Images	PSNR at Red	PSNR at Green	PSNR at Blue
S1	77.3747	77.4448	67.745
S2	77.2783	77.4026	67.5435
S3	76.9506	79.0324	67.4775
S4	76.9506	77.0399	67.4775
S5	77.0014	77.1179	67.5147

TABLE II. PSNR VALUES OF PROPOSED ALGORITHM

Sample Images	PSNR at Red	PSNR at Green	PSNR at Blue
S1	70.9458	100	96.2956
S2	70.9206	100	99.3059
S3	64.8608	100	69.5585
S4	70.9206	100	100
S5	71.1206	100	100

TABLE III. IMPERCEPTIBILITY OF PROPSED ALGORITHM

Size of Watermark	PSNR at Red	PSNR at Blue
Size 10000	81.46387	61.08983
Size 20000	78.06911	50.1236
Size 30000	76.30848	45.73024
Size 40000	74.75822	41.48165
Size 50000	72.99918	37.96801
Size60000	71.91828	36.63454
Size 70000	70.92042	35.88567
Size 80000	70.40995	35.31327
Size 90000	70.08852	34.86395
Size 100000	69.55787	34.45396

In this process only red and blue color planes of the images taken for measuring the PSNR, since the green plane is untouched in the proposed scheme. As shown in the tab.3 and fig.5, the red plane is able to produce good PSNR (around 70 dB) values to the watermark size of 100000 bits. At the same time blue planes are not able to produce good PSNR .In the blue plane for the size of 20000bits, PSNR reaches below 50dB.Therefore, by the number test, it is concluded that 30000 bits will be the best maximum size of the watermrk which will not introduce any visual artifacts. It is clearly shown in fig.6.When, the size of the watermark is crossing 30000bits, the visual artifacts are introduced. Moreover, 30000bits is achevied with PSNR of 60dB at an average and it is best suited for authentication [3].

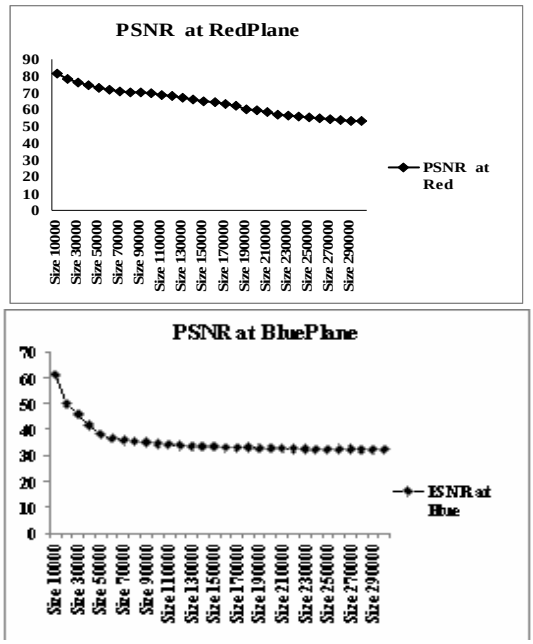

Figure 5: Imperceptibility at Red and Blue Color Planes

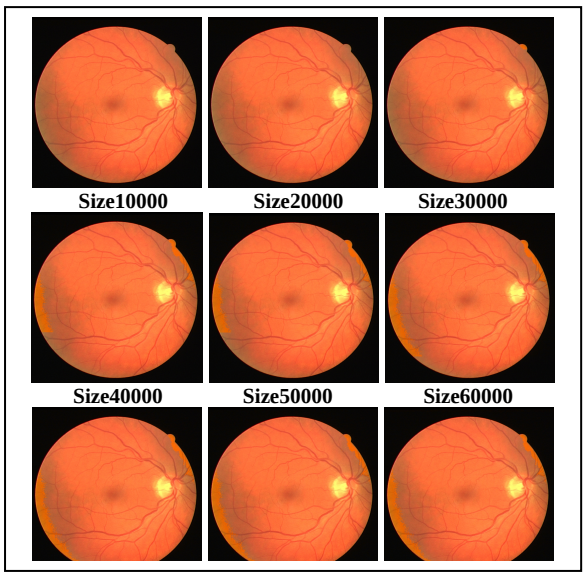

Figure 6: Imperceptibility Vs Size of Watermarking

V. CONCLUSIONS

In this paper, we proposed a reversible, multilayered watermarking scheme for fundus images using intra-plane difference to assure the confidentiality and reliability of the communication. The proposed scheme allows an individual to hide secret data inside the fundus image with hopes that the communication process will be so obscure. It will not give any rooms for suspicion about the contents of the file. The

proposed scheme in the paper can be extended to provide the multi level security by combining with cryptosystems.

REFERENCES

[1] Nammer N, EL-Emman, "Hiding a Large Amount of Data with High Security using Stegnography Algorithm", Journal of Computer Science ,Vol 3, Issue 4, Page No 223-232, 2007.
[2] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology 13 (8) 890–893, Aug. 2003.
[3] Poonkuntran Shanmugam, Rajesh R S, Eswaran Perumal, "A Reversible Watermarking With Low Warping: An Application to Digital Fundus Images", Proceedings of the IEEE Int. Conf. on Computer and Communication Engineering, pp. 472-477, 2008.
[4] S.Poonkuntran, D.Aju, C.Anitha, "A Smart system for retinal blood vessel identification and width computation", Proceedings of International conference on Trends in Intelligent Electronic Systems, Nov 2007.
[5] S.Poonkuntran,R.S.Rajesh,P.Eswaran,"A Robust Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding" , Proceedings of the IEEE Sponsored International Conference on Emerging Trends in Computing (ICETIC2009), 8-10 January 2009, Virudhunagar, Tamilnadu, India.Page.No:433-436.
[6] S.Poonkuntran,R.S.Rajesh,P.Eswaran,"Wavetree Watermarking : An Authentication Scheme for Fundus Images", Proceedings of the IEEE Sponsored International Conference on Emerging Trends in Computing (ICETIC2009), 8-10 January 2009, Virudhunagar, Tamilnadu, India.Page.No:507-511.
[7] S.Poonkuntran,R.S.Rajesh,P.Eswaran, "Reversible, Multilayered Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding", Proceedings of the IEEE International Advanced Computing Conference (IACC 2009), 6-7March 2009, Patiala, Punjab. Page. No: 2583-2587. ISBN: 978-981-08-2465-5.
[8] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging", Information Technology Applications in Biomedicine, IEEE-EMBS Conf. pp. 250-255, 2000.
[9] G. Coatrieux, M. Lamard, W. Daccache, J. Puentes and C. Roux, "A Low distortion and reversible watermark: application to angiographic images of the retina", Proce. of the IEEE 27th Annual Conf. of Engineering in Medicine and Biology, China, September 2005.
[10] F.A.Allaert and L.Dusserre, "Security of Health System in France. What we do will no longer be different from what we tell", International Journal of Biomedical Computing, vol. 35, no. 1, pp. 201-204, 1994.
[11] G. Coatrieux, B. Sankur, and H. Maitre, "Strict integrity control of biomedical images", Electronic Imaging 2001, Security and Watermarking of Multimedia Contents III, SPIE, CA, USA, pp. 229-240. Jan. 2001.
[12] Y.Q.Shi, N.Zhicheng, Z.Dekun, L.Changyin, X. Guorong, "Lossless data hiding: fundamentals, algorithms and applications", Proce. of Int. Symposium on Circuits and Systems, Vol. 2, pp. 23-26, May 2004.
[13] J. Tian, "High capacity reversible data embedding and content authentication", Proce. of IEEE Int. Conf. on Acoustics, Speech and Signal Process. Vol. 3, pp. 6-10, 03.
[14] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Trans. on Image Processing, Vol. 13, Issue. 8, pp. 1147-1156, Aug. 2004.
[15] J. Fridrich, J. Goljan, and R. Du, "Invertible authentication", Proceedings of Security and Watermarking of Multimedia Content, San Jose, CA, pp. 197-208, Jan. 2001.
[16] C. W. Honsinger, P. Jones, M. Rabbani, J. C. Stoffel, "Lossless recovery of an original image containing embedded data", US Patent:6, 278-791, 2001.
[17] B. Macq, "Lossless multiresolution transform for image authenticating watermarking", Proceedings of EUSIPCO 2000, Tampere, Finland, Sept. 2000.
[18] C. De Vleeschouwer, J.F. Delaigle, B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management", IEEE Trans. on Multimedia, Vol. 5, Iss. 1, pp. 97-105, 2003.
[19] N. Zhicheng, Y.Q. Shi, N. Ansari and S. Wei, "Reversible data hiding", Proceedings of Int. Symp. Circuits and Systems, Vol. 2, pp. 25-28, May 2003.

S. Poonkuntran received B.E in Information Technology from Bhrathidasan University, Tiruchirapalli, India in 2003, M.Tech in Computer and Information Technology from Manonmaiam Sundaranar University, Tirunelveli, India in 2005.He is currently doing his doctorate programme (PhD) in the department of computer science and engineering, Manonmaiam Sundaranar University, Tirunelveli, India. He is having around 5 years of experience in teaching and research. He was the student member in IEEE. He is a life time member of Computer Society of India and IACSIT. Currently, working on "Medical image processing -security models". His areas of interest are digital image processing, soft computing and energy aware computing in computer vision.

Dr. R. S Rajesh received the B.E and M.E degrees in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, India in the year 1988 and 1990 respectively, Ph.D degree in Computer Science and Engineering from Manonmaniam Sundaranar University in the year 2004. He is currently as reader with the department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India. He has published several research papers in the areas of Digital image processing, Wireless networks, Pervasive computing and Parallel Computing. He is having the more than 17 years of teaching and 12 years of research experience. He is currently leading a team of Image processing research unit in the department of computer science and engineering at this university.

Eswaran Perumal received the M.Sc degree in Computer Science & Information Technology from Madurai Kamaraj University, Madurai India, in 2003, and the M.Tech degree in Computer & Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2005. He is currently pursuing the Ph.D degree in the department of Computer Science & Engineering, Manonmaniam Sundaranar University Tirunelveli, India. His areas of research include digital image processing and Computer Vision System.