World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:5, No:7, 2011

High Capacity Spread-Spectrum Watermarking for Telemedicine Applications

Basant Kumar[1] ,Animesh Anand[2], S.P. Singh[3], and Anand Mohan[4]

Abstract**—**This paper presents a new spread-spectrum watermarking algorithm for digital images in discrete wavelet transform (DWT) domain. The algorithm is applied for embedding watermarks like patient identification /source identification or doctors signature in binary image format into host digital radiological image for potential telemedicine applications. Performance of the algorithm is analysed by varying the gain factor, subband decomposition levels, and size of watermark. Simulation results show that the proposed method achieves higher watermarking capacity.

Keywords**—**Watermarking, spread-spectrum, discrete wavelet transform, telemedicine

I. Introduction

IN recent years image watermarking has become an important research area in data security, confidentiality and image integrity. Despite the broad literature on various application fields, little work has been done towards the exploitation of health-oriented perspectives of watermarking [1]–[7]. Data hiding and watermarking techniques can play important role in the field of telemedicine by addressing a range issues relevant to health data management systems, such as medical confidentiality protection, patient and examination related information hiding, access and data integrity control, and information retrieval. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Security requirements of medical information, derived from strict ethics and legal obligations imposed three mandatory characteristics: confidentiality, reliability and availability [8]. Authentication, integration and confidentiality are the most important issues concerned with EPR (Electronic Patient Record) data exchange through open channels [1, 5]. All these requirements can be fulfilled using suitable watermarks. General watermarking method needs to keep the three factors (capacity, imperceptibility and robustness) reasonably very high [9]. Two common approaches of information hiding using image covers are spatial domain hiding and transform (frequency) domain hiding. Spatial domain techniques perform data embedding by directly manipulating the pixel values, code values or bit stream of the host image signal and they are computationally simple and straightforward. *LSB substitution*, *patchwork*, and *spread spectrum image steganography* are some of the important spatial domain techniques [10, 11].

In transform domain hiding, data are embedded by modulating coefficients in transform domain, such as DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform). Transform techniques can offer a higher degree of robustness to common image processing operations, compared to spatial domain techniques. Wavelet domain watermarking has recently received considerable attention due to its ability to provide both spatial and frequency resolution [12]-[14].Many wavelet based watermarking schemes were proposed for medical images [15]-[18]. Watermarking technique can be further classified into two categories, reversible and irreversible [19, 20]. The main idea behind reversible watermarking is to avoid irreversible distortion in original image (the host image), by developing techniques that can extract the original image exactly. Medical image watermarking is one of the most important fields that need such techniques where distortion may cause wrong diagnosis. The strict specifications regarding the quality of medical images could be met by reversible watermarking, which allows the recovery of the original image without any loss of information. Medical identity theft has been a serious security concern in telemedicine [21]. This demands development of secure watermarking schemes. Therefore, security of the watermark becomes a critical issue in many applications. The problem of watermark security can be solved using spread-spectrum scheme [22- 25]. Spread-spectrum is a military communication scheme invented during World War II [26]. It was designed to be good at combating interference due to jamming, hiding a signal by transmitting it at low power, and achieving secrecy. These properties make spread- spectrum very popular in present-day digital watermarking.This paper proposes a new secure spread- spectrum based watermarking algorithm for embedding sensitive medical information like physician's signature/ identification code or patient identity code into radiological image for identity authentication purposes. This medical information in binary image form is taken as watermarks. The proposed algorithm relies on n distinct pseudo-random (PN) sequence pairs with low correlation, where n is the number of bits that are to be hidden. The rest of the paper is organized as follows. Section II provides a brief overview of spread- spectrum image watermarking schemes in wavelet domain. Working of the proposed spread- spectrum algorithm is explained in section III. Performance of the new algorithm has been analyzed in section IV and section V provides conclusion of overall work.

Basant Kumar is with the Motilal Nehru National Institute of Technology, Allahabad, India (e-mail: singhbasant@ yahoo.com).

II. Spread Spectrum Watermarking In Wavelet Transform Domain

Wavelet-based watermarking has recently gained great attention due to its ability to provide excellent multi-resolution analysis, space-frequency localization and superior HVS modeling [12]. DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple “scale” wavelet decomposition. The dyadic frequency decomposition of wavelet transform resembles the signal processing of the HVS and thus allows adapting the distortion introduced by either quantization or watermark embedding to the masking properties of human eye [27].This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). This domain also offers added benefits like increased robustness, tolerance to various compression algorithms and filtering. In spread-spectrum communications, one transmits a narrowband signal over a much larger bandwidth, such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into single output with high signal-to-noise ratio (SNR). However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures sufficiently small energy in any single coefficient. A watermark that is well placed in the frequency domain of an image will be practically impossible to see. The proposed image watermarking scheme uses spread-spectrum technique in which, different watermark messages are hidden in the same transform coefficients of the cover image using uncorrelated codes, drawn from a Gaussian (*N* (0, 1)) distribution (where N (μ,σ^2) denotes a normal distribution with mean μ and variance σ^2). The choice of this distribution gives resilient performance against collusion attacks. The Gaussian watermark also gives strong performance in the face of quantization [28].Robust and secure watermarking can be achieved by placing the watermark explicitly in the perceptually most significant components of the data.

III. Proposed Algorithm

This paper proposes a new DWT based spread-spectrum watermarking algorithm using medical image cover. Dyadic subband decomposition is performed on the radiological image using Haar wavelet transform. The watermark used in the algorithm is in binary image form. Different watermark messages are hidden in the same transform coefficients of the cover image using uncorrelated codes, i.e. low cross correlation value (orthogonal / near orthogonal) among codes. For each message bit, two different Pseudo Noise (PN) sequence vectors namely of size identical to the size of DWT column vector, are generated. Based on the value of the bit of the message vector, the respective two PN sequence pairs are then added / subtracted to/from the corresponding second level HL and LH coefficients column vectors respectively according to the data embedding rule as follows:

$$W = V + kX \quad \textit{if } b=0$$
$$W = V - kX \quad \textit{if } b=1$$

where *V* is wavelet coefficient of the cover image, W is the wavelet coefficient after watermark embedding, *k* is the gain factor, X is the PN sequence and *b* is the message bit that has to be embedded. The corresponding column of the wavelet coefficient, to which the generated sequence has to be added/subtracted, is decided by the following relation:

P= *R* modulo *N*

where *P* is the column in which sequence has to be added, *R* is index of the sequence generated and *N* is the number of columns in coefficient matrix. Generation of a pair of PN sequences for embedding each bit enhances the security of the watermarking algorithm. Following steps are applied in data embedding process:

A. Data Embedding

(i). Read the host image $I(M,N)$ of size $M \times N$

(ii). Read the message to be watermarked and convert it into binary sequences D_d ($D_d = 1$ to n).

(iii). Transform the host image using “Haar” Wavelet transform and get second level subband coefficients ccA, ccH, ccV, ccD.

(iv). Generate *n* different PN-sequence pairs (PN_h and PN_v) each of size $\frac{M}{4} \times 1$ using a secret key to reset the random number generator

(v). For $D_d = 1$ to n, add r^{th} PN sequence pair to p^{th} columns of ccH and ccV subband coefficients when message = 0, where p = r modulo (N/4), hence 1≤ p ≤ N/4, 1 ≤ r ≤ n.

ccH((p^{th} column) = ccH(p^{th} column) + k * r^{th} PN_h;
ccV((p^{th} column) = ccV((p^{th} column) + k * r^{th} PN_v;

where *k* is the gain factor used to specify the strength of the embedded data.

(vi). Apply inverse “Haar” Wavelet transform to get the final stego (watermarked) image $I_w(M,N)$.

B. Extraction of hidden data

To detect the watermark we generate the same pseudo-random sequence vectors used during insertion of watermark by using same state key and determine their correlation with the corresponding detail subbands DWT coefficient columns. Average of *n* correlation coefficients corresponding to each PN sequence vector is obtained for both LH and HL subbands.

Mean of the average correlation values are taken as threshold T for message extraction. During detection, if the average correlation exceeds T for a particular sequence a “0” is recovered; otherwise a “1”. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered. For extracting the watermark, following steps are applied to the watermarked image:

(i). Read the stego image $I_w(M, N)$

(ii). Transform the stego image using “Haar” Wavelet transform and get ccA1,ccH1,ccV1,ccD1 coefficients

(iii). Generate one’s sequences (*msg*) equal to message vector (from *1* to *n*)

(iv). Generate n different PN-sequence pairs (PN_h1 and PN_v1) each of size $\frac{M}{4} \times 1$ using same secret key used in embedding to reset the random number generator

(v). For *i=1* to n

Calculate the correlations store these values in *corr_H (i)* and *corr_V (i).*

corr_H (i) = correlation between PN_h1(i) and ccH1((jth column)

corr_V (i) = correlation between PN_v1(i) and ccV1 ((jth column)

where j= *i* modulo N/4, hence 1≤ j ≤ N/4 , 1 ≤ i ≤ n.

(vi). Calculate average correlation avg_corr (i) = (corr_H(i)+corr_V(i))/2

(vii). Calculate the corr(mean) = mean of all the values stored in avg_corr (i)

(viii). Extract the hidden bit 0, using the relationship given below:

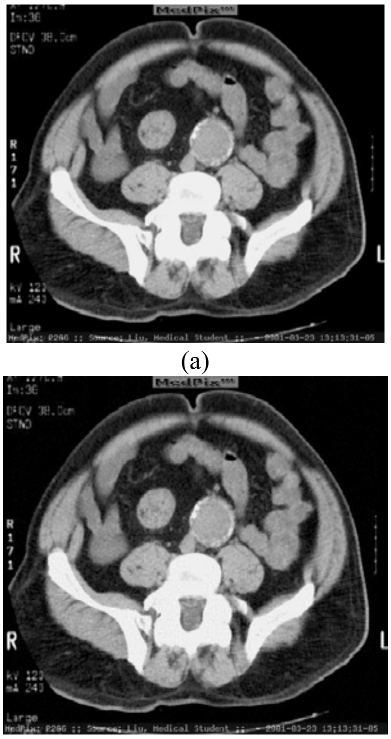
```
For k=1 to n
        if avg_corr (k) > corr (mean)
        msg(k)=0.
```

(ix). Rearrange this extracted message to get the binary matrix representation of the binary image watermark.

(x). Convert the matrix back to image to get the recovered watermark.

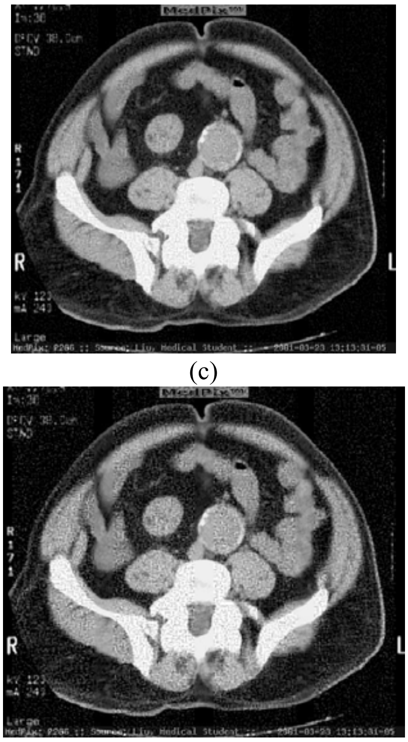
IV. Performance Analysis

Performance of the proposed spread-spectrum watermarking algorithm was tested for telemedicine applications. Experiments were carried-out using 8-bit grey scale CT scan image of size 512x512 available in reference [29]. Medical information such as telemedicine origin centre (watermark1) and doctor’s signature (watermark2) were embedded into host CT scan image as watermarks. These watermarks are in binary image formats which add robustness by allowing recovery of the watermarks even at low correlation between original and extracted watermarks. Strength of watermarking is varied by varying the gain factor in the watermarking algorithm. Perceptual quality of the watermarked radiological image is measured by calculating PSNR between host and watermarked image. At the receiver side, watermark is extracted from the watermarked image. Extracted watermark is evaluated by measuring its correlation with the original watermark. Figure 1. Shows the host CT scan image and watermarked images obtained by applying watermarking algorithm in second level LH and HL subband DWT coefficients at different gain factors. Extracted watermarks along with the original watermarks are shown in figures 2 and 3. It is observed from Table 1 that with the increase in the gain factor, PSNR of the watermarked image decreases and the degree of similarity between original and extracted watermark increases. To show the effect of the decomposition levels, proposed algorithm with gain factor 17 was applied for embedding watermark in the horizontal and vertical subband coefficients of level 1, 2 and 3. With the increase in subband level for embedding, the number of DWT coefficient to be modified, decreases which results into better PSNR performance of watermarked image but relatively lower correlation performance of the extracted watermark. It is observed from Table 2 that the PSNR value of the watermarked image increases and correlation between original and extracted watermark decreases with the increase in subband level for watermarking. Figure 4. Shows the watermarks extracted from different levels of subband DWT coefficients. Performance of the watermarking algorithm also depends on the size of watermark .Table 3 shows the effect of watermark size on the performance of the proposed watermarking algorithm. It is obvious that the PSNR performance of the watermarked image decreases with the increase in the size of the watermark, but subsequently we observe an improvement in the correlation between original and extracted watermarks. It can be also observed from figure 5 that larger size watermarks are more clearly identified during extraction.



(a)

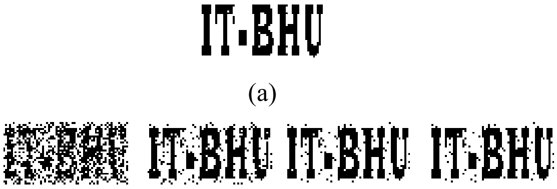
(b)



(c)

(d)

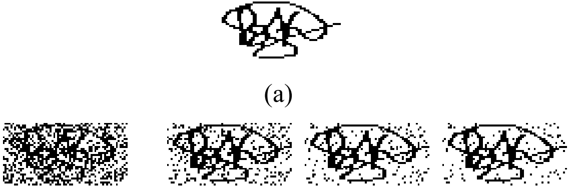
Fig. 1 Original and watermarked CT scan images (a) original image and watermarked images with gain factor (b) 5 (c) 15 and (d) 30



(a)

(b) (c) (d) (e)

Fig. 2 Telemedicine centre watermarks (a) original and extracted watermarks with gain factor (b) 5 (c) 15 (d) 30 and (e) 40



(a)

(b) (c) (d) (e)

Fig. 3 Doctor’s signature watermarks (a) original and extracted watermarks with gain factor (b) 5 (c) 15 (d) 30 and (e) 40

TABLE I
EFFECT OF GAIN FACTOR

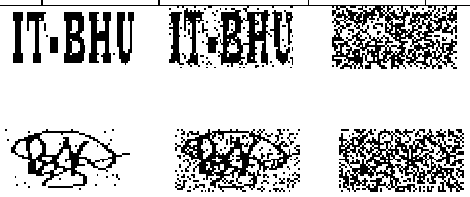
Gain Factor	Watermark1 (Origin centre)		Watermark2 (Doctor’s Signature)	
	PSNR	Correlation	PSNR	Correlation
40	21.5375	0.6387	19.4909	0.6476
30	23.8698	0.6296	21.9897	0.6476
20	27.2492	0.6191	25.5115	0.6389
17	28.594	0.6107	28.0103	0.6303
15	29.648	0.5927	28.0103	0.6303
10	33.0708	0.516	31.5321	0.6054
5	39.0255	0.3572	37.674	0.5233
1	52.0498	0.0805	51.5321	0.2352

TABLE II
EFFECT OF SUBBAND LEVELS (GAIN FACTOR 17)

Levels	Watermark1 (Origin centre)		Watermark2 (Doctor’s Signature)	
	PSNR	Correlation	PSNR	Correlation
1	28.0103	0.676	28.0103	0.6303
2	29.648	0.5927	30.9839	0.4464
3	30.5632	0.307	32.706	0.229

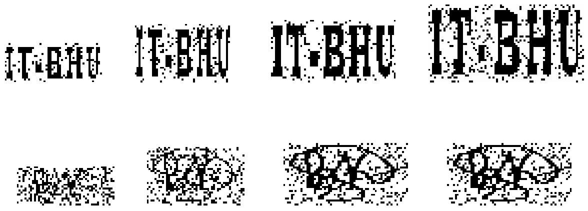
TABLE III
EFFECT OF WATERMARK SIZE

Watermark size	Watermark1 (Origin centre)		Watermark2 (Doctor’s Signature)	
	PSNR	Correlation	PSNR	Correlation
20 X 50	32.472	0.4988	37.0202	0.1808
30 X 50	30.5979	0.5086	33.9414	0.2742
32 X 64	28.594	0.6107	30.9839	0.47
40 X 80	27.2816	0.4925	30.2084	0.2924



(a) (b) (c)

Fig. 4 Extracted watermarks from (a) level 1 (b) level 2 and (c) level 3



(a) (b) (c) (d)

Fig. 5 Extracted watermarks of different size (a) 20 X 50 (b) 30 X 50 (c) 32 X 64 (d) 40 X 80

V. CONCLUSIONS

This paper presented a secure spread-spectrum watermarking scheme with enhanced watermarking capacity in wavelet transform domain. Performance of the scheme was tested for telemedicine applications by watermarking radiological images with sensitive medical information in binary image format.

REFERENCES

[1] H. M. Chao, C. M. Hsu, S. G. Miaou, “A data-hiding technique with authentication, integration, and confidentiality for electronic patient

records," IEEE Trans. Inf. Technol. Biomed., vol. 6, no. 1, pp. 46-53, March 2002.

[2] U. Rajendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, "Compact storage of medical images with patient information," IEEE Trans. Inf. Technol. Biomed., vol. 5, no. 4, pp. 320-323, Dec. 2001.

[3] X. Kong, R. Feng, "Watermarking medical signals for telemedicine," IEEE Transaction on Information Technology in Medicine, vol. 5, no. 3, pp. 195-201, 2001.

[4] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevance of atermarking in medical imaging," in Proc. 3rd Conf. Information Technology Applications in Biomedicine, ITAB'00, Arlington, USA, pp. 250-255.

[5] K.A. Navas, S. Archana Thampy, and M. Sasikumar, " ERP hiding in medical images for telemedicine," Proceedings of World Academy of Science and Technology, Vol. 28, 2008.

[6] B. Planitz and A. Maeder, "Medical image watermarking: a study on image degradation," in Proc. Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing, WDIC 2005, Brisbane, Australia, February, 2005.

[7] G. Coatrieux, L. Lecornu, Ch. Roux, and B. Sankur, "A review of Image Watermarking Applications in Healthcare," IEEE Eng Med Biol. Soc, Vol 1, pp. 4691-4, 2006.

[8] R. C Raul, F. U. Claudia, and T. B. Gershom, " Data hiding scheme for medical images," in Proceedings International Conference on Electronics, Communications and Computers (CONIELECOMP'07), pp.32-32, Cholula, Mexico, February, 2007.

[9] G. C. Langelaar, I. Setyawan, R. L. Lagendijk, " Watermarking digital image and video data. A state-of-the-art overview," IEEE signal processing Magazine , vol. 17, no. 5, pp. 20-46, Sept.2000.

[10] N. Nikolaidis and I. Pitas, "Digital image watermarking: an overview," in Proc. Int. Conf. Multimedia Comput. and Syst., ICMCS99, vol. 1, pp. 1-6, Florence, Italy, June 7–11, 1999

[11] I. J. Cox, Matt L. Miller, " The first 50 years of electronic watermarking ," EURASIP Journal on Applied Signal Processing , Vol.2002, no.2, pp. 126-132 , 2002.

[12] Meerwald P, Uhl A (2001) A survey of wavelet-domain watermarking algorithms. Proceedings of the SPIE security and watermarking of multimedia contents, vol 4314. San Jose, pp 505–516

[13] S. Hajjara, M. Abdallah, and A. Hudaib, " Digital Image Watermarking using Localized Biorthogonal Wavelets," European Journal of Scientific Research, Vol. 26, No. 4, pp. 594-608, 2009.

[14] A. H. Paquet, R. K. Ward, "Wavelet-based digital watermarking for authentication," Proceedings of the IEEE Canadian conference on electrical and computer engineering, vol. 2, pp. 879-884, Winnipeg, Canada, 2002.

[15] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images," Medical Biological Engineering & Computing, Vol. 44, pp. 619-631, 2006.

[16] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, "Multiple image watermarking applied to health information management," IEEE Transactions on Information Technology in Biomedicine, Vol. pp. 722-732, 2006.

[17] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, " A medical image watermarking scheme based on wavelet transform," Proceedings 25th Annual International Conference of IEEE-EMBS, Cancun, Mexico, pp. 856-859, 2003.

[18] S. Dandapat, J. Xu, O. Chutatape, S. M. Krishnan, "Wavelet transform domain data embedding in a medical image," Proceedings 26th Annual International Conference of IEEE-EMBS, San Francisco, CA,USA, pp. 1541-1544, Sept., 2004.

[19] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, " Reversible watermarking: current and key issues," International Journal of Network Security, vol. 2, no. 3, pp. 161-170, May 2006.

[20] S. Lee, C. D. Chang, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transaction on Information Forensics and Security, vol. 2, no. 3, pp.-321-330, Sept. 2007.

[21] M. Terry, "Medical identity theft and telemedicine security," Telemedicine and e-Health, vol. 15, no. 10, pp. 1-5, December 2009.

[22] I. J. Cox, J. Kilian, F. Thomson Leighton, Talal Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, Vol. 6, no. 12 , 1997.

[23] H. S. Malvar and D. A. F. Florencio, "Improved Spread Spectrum: A New Modilation Technique for Robust Watermarking," IEEE Transactions on Signal Processing, vol. 51, no. 4, 2003.

[24] L. Perez-Freire and F. Perez-Gonzalez, "Spread-Spectrum Watermarking Security," IEEE Transactions on Information Forensics and Security, Vol. 4, no. 1, 2009.

[25] G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," IEEE International workshop on multimedia signal processing (MMSP2004), Siena, Italy, 2004.

[26] D. Kahn, "Cryptology and the origins of spread spectrum," IEEE Spectrum, vol. 21, pp. 70-80, Sept. 1984.

[27] M. Unser, A. Aldroubi, "A review of wavelets in bio-medical applications," Proceedings IEEE, Vol. 84, pp. 626-638, 1996.

[28] F. Ergun, J. Kilian, and R. Kumar, " A note on the limits of collision-resistant watermarks," EUROCRYPT99, LNCS, vol. 1592, pp. 140-149, 1999.

[29] MedPixTM Medical Image Database available at http://rad.usuhs.mil/medpix/medpix.html

Animesh Anand is with the Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varanasi, India (e-mail: aanand.itbhu@gmail.com).

S.P. Singh is with the Electronics l Engineering Department, Banaras Hindu University, Varanasi, India(e-mail: suryapal_s@yahoo.co.in).

Anand Mohan are with the Electronics l Engineering Department, Banaras Hindu University, Varanasi, India(e-mail: amohan@gmail.com).