ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Model for Legal Document Authentication (MLDA)

Nabin Ghoshal
Department of Engineering and Technological Studies
University of Kalyani
Kalyani, Nadia, Pin. 741235, West Bengal, India
nabin_ghoshal@yahoo.co.in

Abstract: This paper deals with the achievement of proposed study of steganographic field. The author devised some algorithm to authenticate various images/documents in both spatial and frequency domain using 1-bit-, 2-bit-, and 3-bit-steganography. Major achievements of the proposed study are enhancement of Pick Signal-to-Noise Ratio, Image fidelity and considerable amount of lower MSE, inspite of large volume of data hiding. Most of data hiding technique obtained better/comparable results compare to existing technique. The chronological achievement in terms of PSNR, IF and MSE are shown in this paper.
Keywords: Steganography, MSE, IF, PSNR, Legal document.

I. INTRODAUCTION

Digital images are transmitted over popular communication channels such as the Internet. For secured communication, image authentication techniques have gained more attention due to their importance for a large number of multimedia applications. Military, medical and quality control images must be protected from alteration so as to maintain their authenticity, a number of approaches have been proposed for this including: conventional cryptography [16], fragile and semi-fragile watermarking and digital signatures. Digital watermarking is the process of hiding the watermark imperceptibly in the content. This technique was initially used in paper and currency as a measure of authenticity. Steganography [7, 12, 15] within the image has become an important technique for proving image authentication and identification. Data hiding primarily refers to a digital watermark which is a piece of information hidden in a multimedia content, in such a way that it is imperceptible to a human observer, but easily detected by a computer. The principal advantage is that the watermark is inseparable from the content. Ownership verification [8, 9, 17] and authentication is the major task for military people, research institutes, and scientists.

Information security and image authentication has become very important to protect digital image document from unauthorized access. In steganographic [1, 2, 3, 4, 5] applications, the hidden data may be a secret message, hologram or video whose presence within the host data is generally undetectable. Data hiding represents a useful alternative to constructing a hypermedia document or image, which is more difficult to manipulate.

Prior research into this area has focused on:

a. Identifying bits that can be used for Steganography. Pavan et al. [13] and Nameer N. EL-Emam [6] used entropy based technique for detecting the suitable areas in the image where data can be embedded with minimum distortion.
b. Methods of implementing the Steganography. Chandramouli et al. [10] developed a useful method for making such alterations by masking, filtering and transformations of the least significant bit (LSB) on the source image. H. H. Pang [14] used hash value obtained from a file name, password and position of header of hidden file. Ker [18] and C. Yang [19] presented a general structural steganalysis framework for embedding in two or more LSBs. H. C. Wu [20] and Cheng-Hsing Yang [21] constructed a method of LSB replacement into the edge areas using pixel value differencing (PVD) where PVD was used to distinguish between the edge and smooth areas.
c. Methods of detecting Steganography. Dumitrescu et al. [11] constructed an algorithm for detecting LSB steganography.

Recent studies [1, 2, 7, 11, 17, 18, 19, 20, 21] have shown that digital data can be effectively hidden in an image with imperceptible degradation to the host image but less protection against various attacks. Most of the approaches including PVD based LSB substitution techniques have not been tested on colour images; moreover, some of them did not consider the principle that the deep colored edge areas are able to tolerate more changes than light colored edge areas [18, 19, 20, 21].

The aim of this paper is to present a model that would facilitate legal document authentication using a data hiding procedure which embeds the data adaptively by considering the concept of human vision, with features of high capacity and low distortion. The Adaptive Steganography [22, 23] for legal document Authentication based on hiding principle places an emphasis on:

i. Information and image protection against unauthorized access
ii. Inserting secrete messages/image data into the source image for legal document identification
iii. Transmitting secure messages within the image

Here proposed a model for authentication of passport and voter ID card for our nation which is most relevant and burning area of interest for the building of nation has been proposed. In this model various developed techniques are used to authenticate legal document like passport, copyright document, voter ID card, ration card and title deed.

Section II of the paper deals with the proposed technique. Results, and discussion are given in section III. Section IV of the paper deals with the authentication process of passport

and viter ID card. Conclusions are drawn in section V, References are given in section VI.

II. THE TECHNIQUE

Here proposed a model for authentication of passport and voter ID card. By this model ownership verification and copy right protection for all legal documents is possible. With the help of different proposed techniques the secrete data can be embedded within the image passport or voter ID card holder. Also for different level of security a key of message digest MD generation is possible using proposed algorithm. Here describing the working principle of one technique among all the proposed technique. The proposed model is applied to authenticate passport and voter ID card.

Model generates message digest MD of length 128 bits from the original source image of passport holder or voter ID holder. Prior to generate this MD from source image, the bits of the insertion position initialized by zero and then a bit swap operations on each byte of the source image is performed. Inter-bit swapping is done for each byte, the rule is, for each of the first 6 bits (from LSB to MSB), if the value of a bit is zero interchange (swap) the values of the next 2 bits towards MSB, else leave the values of those two bits unchanged. After swap operation for all bytes of initialised image the XOR operation is perform between first two 128 bits stream of swapped image. Next XOR operations are performed between the resultant 128 bits from 1st two 128 bits and third 128 bits from swapped image. After continuing the same process for all 128 bits stream of swapped image, finally MD will be generated with 128 bits long. In the final step the bit wise XOR operation is performed with the inserted bits at the insertion positions and this 128 bits MD key of the signature image. Hence the key MD will be repeated after 128 such positions while executing the bit wise XOR operation. Any change of source image the generated message digest MD will differ from the original one which has been generated during the process of authentication at the destination. As a result any attempt in tempering the document during transmission across the network can be identified. The signature of appropriate authority is also fabricated as an authenticating image using same principle. The strength in embedding is high without changing visible property. Figure 1 shows the processed of model.

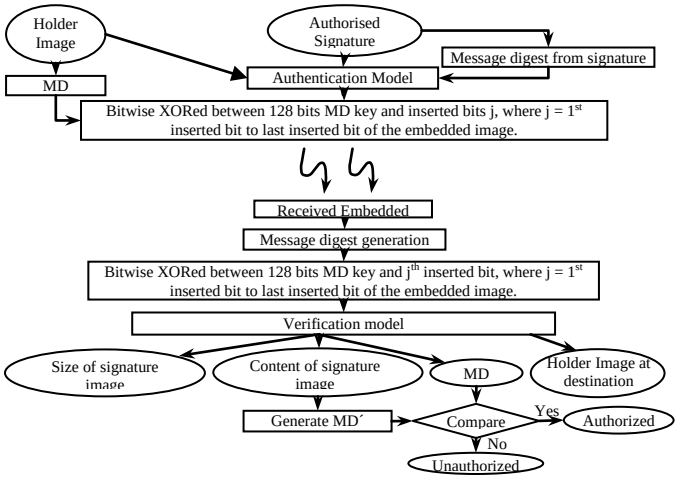

Figure 1: Schematic diagram of authentication

III. RESULT AND DISCUSSION

Fig. 2, 3 and 4 are shows the growth of PSNR, IF and MSE in spatial domain algorithms BLIA/SMTT [2], MDHIAT [3], AI/HLVD [24], IAHLVDSMTTM [4], FBIA [26], ATILD [25] developed by me and existing technique S-Tools. The Fig. 2 indicates the PSNR increasing in different proposed algorithms and S-Tools generates low PSNR. IF is increasing in the different developed algorithm which shows in Fig. 3, Fig. 4 shows the exact scenario of noise integration on embedding in different technique. Fig. 5 is showing the growth of PSNR value in proposed frequency domain algorithms IAFDDFTT [1], IATFDDFT [27], CDHTCIAFD [28] and DFTMCIAWC [29] all are developed by me. In frequency domain the PSNR values are increasing in different algorithm. Hence in terms of above analysis it reveals that using proposed techniques and methodology, authenticity and security in transmitting secrete message/image through wired/wireless communication system may be enhanced.

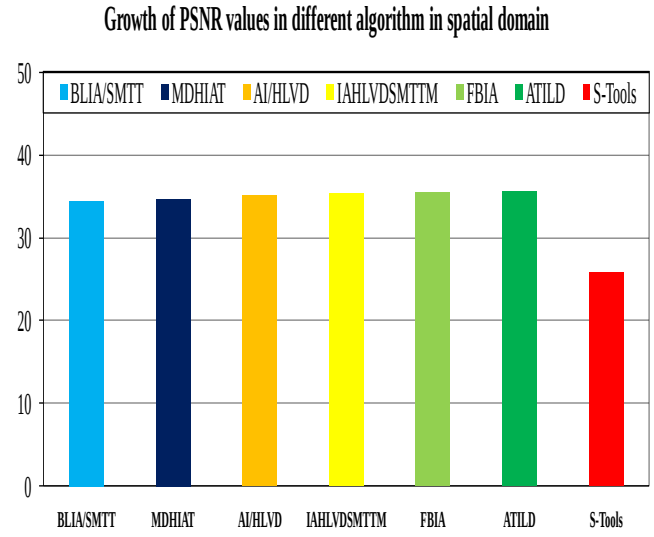

Figure 2: The Growth of PSNR

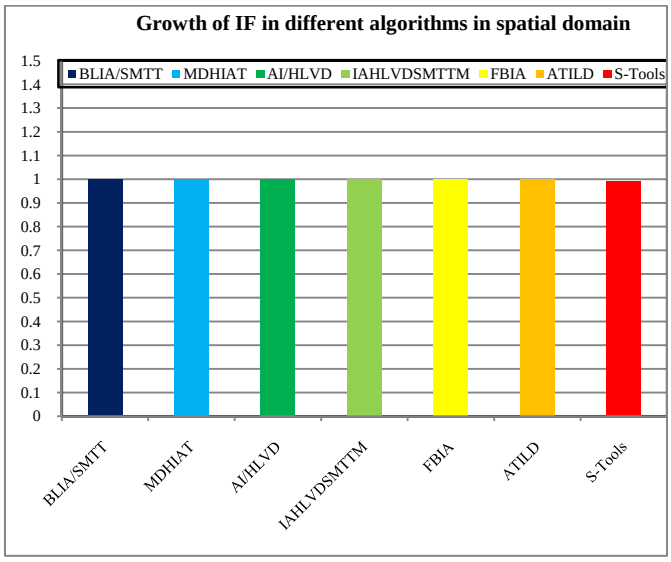

Figure 3. The Growth of IF

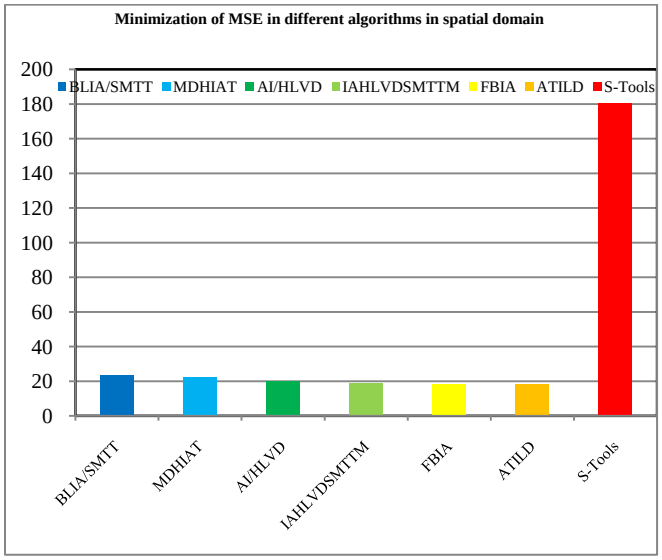

Figure 4: The growth of MSE

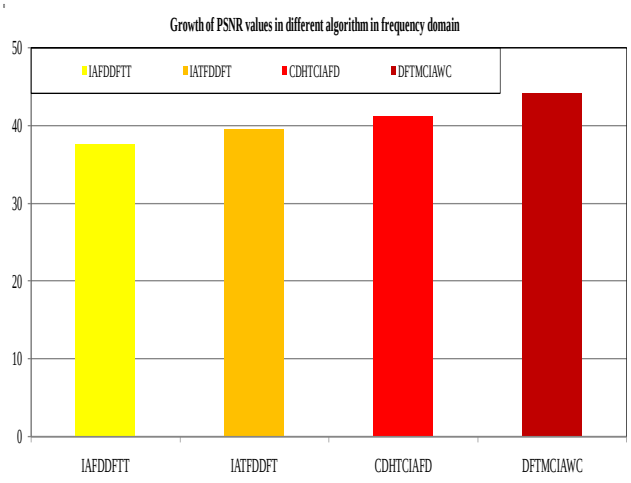

Figure 5: The growth of PSNR

IV. AUTHENTICATION PROCESS OF PASSPORT AND VOTER ID CARD

In the process of passport (Fig. 6) and voter ID card (Fig.10) authentication is done by different level of soft computing process. Here holder image (Fig. 7) is considered as the secrete carrier for authentication. This image should be authenticated by the signature of issuing officer and the signature of owner. Fig. 7 is authenticated by the signature of regional passport officer (Fig. 9) and the signature of the passport holder (Fig. 8). Fig. 11 is authenticated by the signature of electoral registration officer. With the help of any one proposed algorithm the embedding of signatures within the source image can be done. Before embedding of signature the dimension of signature and message digest from source image should be embedded within the holder image. At the other end all embedded data can be extracted successfully by the reverse procedure. As a result authority can identify the original one and also can be able to identify any impaired one.

Figure 6: Authenticated passport with embedded signature for verification using soft tools

Figure 7: Original photograph of passport holder with stamp

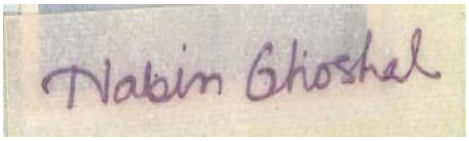

Figure 8: Signature of passport holder to authenticate passport

Figure 9: Signature of regional passport officer to authenticate passport

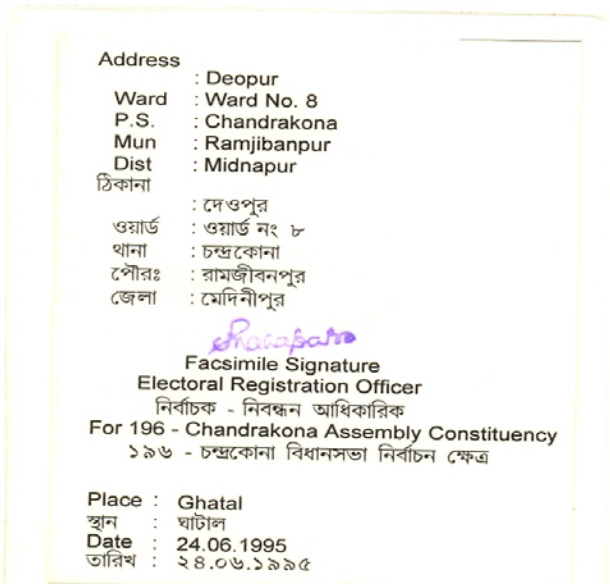
Address
: Deopur
Ward : Ward No. 8
P.S. : Chandrakona
Mun : Ramjibanpur
Dist : Midnapur
ঠিকানা
: দেওপুর
ওয়ার্ড : ওয়ার্ড নং ৮
থানা : চন্দ্রকোনা
পৌরঃ : রামজীবনপুর
জেলা : মেদিনীপুর
Facsimile Signature
Electoral Registration Officer
নির্বাচক - নিবন্ধন আধিকারিক
For 196 - Chandrakona Assembly Constituency
১৯৬ - চন্দ্রকোনা বিধানসভা নির্বাচন ক্ষেত্র
Place : Ghatal
স্থান : ঘাটাল
Date : 24.06.1995
তারিখ : ২৪.০৬.১৯৯৫

Figure 10: Authenticated voter ID card with embedded signature for verification using soft tools

Figure 11: Original photograph of voter ID card holder with stamp

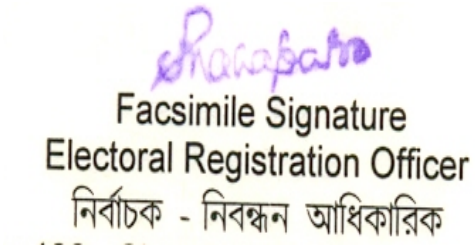

Figure 12: Signature of authorised person to authenticate ID card

V. CONCLUSIONS

Proper utilization of proposed techniques ownership verification can be possible like title deed, agreement copy, passport, voter ID card and ration ID card authentication. Application of security and authenticity for sensitive document is necessary to keep the copyright protection. For the proliferation of autonomy in different level of administrative work the protection of important document is needed to resist any kind of scamp. With the help of the proposed model the originality checking is easily possible for the legal documents.

VI. ACKNOWLEDGEMENTS

The author expresses the deep sense of gratitude to the Department of Engineering and Technological studies, University of Kalyani, West Bengal, India, where the work has been carried out.

VII. REFERENCES

[1]. N. Ghoshal, J. K. Mandal, A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT), Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, 2008pp, 24-32.

[2]. N. Ghoshal, J. K. Mandal, A Bit Level Image Authentication / Secrete Message Transmission Technique (BLIA/SMTT), Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, ISSN 1240-4543, Vol. 51, No. 4, 2008, pp. 1-13.

[3]. N. Ghoshal, A. Sarkar, D. Chakraborty, S. Ghosh J. K. Mandal, Masking based Data Hiding and Image Authentication Technique (MDHIAT), Proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University, Chennai, India, URL:- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4760437&tag=1, 2008, pp. 119-122.

[4]. N. Ghoshal, J. K. Mandal, A. Sarkar, D. Chakraborty, S. Ghosh, Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM), Proceedings of IEEE International Advanced Computing Conference IACC'09, ISBN: 978-981-08-2465-5, March 6-7th, Thapar University, Patiala, India, URL:- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04809168, 2009, pp. 3177-3188.

[5]. R. Radhakrishnan, M. Kharrazi, N. Menon, Data Masking: A new approach for steganography, Journal of VLSI Signal Processing, Springer, Vol. 41, 2005, pp. 293-303.

[6]. N. N. EL-Emam, Hiding a large Amount of data with High Security Using Steganography Algorithm, Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, 2007, pp. 223-232,.

[7]. P. Amin, N. Lue and K. Subbalakshmi, Statistically secure digital image data hiding, IEEE Multimedia Signal Processing MMSP05, Oct. 2005, Shanghai, China, pp. 1-4.

[8]. B. Chen and G. W. Wornnel, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. On Info. Theory, vol. 47, no. 4, May 2001, pp. 1423-1443.

[9]. C.Y. Lin and S. F. Chang, A robust image authentication method surviving JPEG lossy compression, Proc. SPIE, vol. 3312, San Jose, Jan. 1998, pp. 296-307.

[10]. R. Chandramouli and N. Memon, Analysis of LSB based image steganography techniques, Proc. of ICIP, Thissaloniki, Greece, 2001, pp. 1019-1022.

[11]. S. Dumitrescu, W. Xiaolin and Z. Wang, Detection of LSB steganography via sample pair analysis, IEEE Trans. on Signal processing, Vol. 51, no. 7, 2003, pp. 1995-2007.

[12]. P. Moulin and J. A. O'Sullivan, Information-theoretic analysis of information Hiding, IEEE Trans. On Info. Theory, vol. 49, no. 3, March 2003, pp. 563-593.

[13]. S. Pavan, S. Gangadharpalli and V. Sridhar, Multivariate entropy detector based hybrid image registration algorithm, IEEE Int. Conf. on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, March 2005, pp. 18-23.

[14]. H. H. Pang, K. L. Tan and X. Zhou, Steganographic schemes for file system and B-tree, IEEE Trans. On Knowledge and Data Engineering, vol. 16, Singapore June 2004, pp. 701-713.

[15]. P. Moulin and M. K. Mihcak, A framework for evaluating the data-hiding capacity of image sources, IEEE Transactions on Image Processing, vol. 11, Urbana, Illinois, Sept. 2002, pp. 1029-1042,.

[16]. C. Rechberger, V. Rijman and N. Sklavos, The NIST cryptographic Workshop on Hash Functions, IEEE Security & Privacy, vol. 4, Austria, Jan-Feb 2006, pp. 54-56.

[17]. A. H. Al-Hamami and S. A. Al-Ani, A New Approach for Authentication Technique, Journal of computer Science, ISSN 1549-3636, Vol. 1, No. 1, 2005, pp. 103-106.

[18]. A. Ker, Steganalysis of Embedding in Two Least-Significant Bits, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 2, No. 1, 2008, pp. 46-54.

[19]. C. Yang, F. Liu, X. Luo and B. Liu, Steganalysis Frameworks of Embedding in Multiple Least Significant Bits, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 4, 2008, pp. 662-672.

[20]. H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, Proc. Inst. Elect. Eng., Vis. Images Signal Process., Vol. 152, No. 5, 2005, pp. 611-615.

[21]. C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, Adaptive Data Hiding in edge areas of Images With Spatial LSB Domain Systems, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 3, 2008, pp 488-497.

[22]. M. Kutter and F. A. P. Petitcolas, A fair benchmark for image watermarking systems, Electronic Imaging '99, Security and Watermarking for Multimedia Content, San Josh CA, vol. 3657, 1999, pp. 226-239.

[23]. Allan G. Weber, The usc-sipi image database: http://sipi.usc.edu/services/database/Database.html, October 1997, Signal and Image Processing Institute at the University of Southern California.

[24]. Ghoshal N., Mandal, J. K. "A Novel Technique for Authentication of Image/Hiding Large Volume of Data (AI/HLVD)", Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), International journal of Signal Processing and Pattern Recognition, ISSN 1240-4543, Vol. 53, No. 2, pp. 1-13, France, 2009.

[25]. Ghoshal N., Mandal J. K. "A Novel Authentication Technique for Image/Legal Document (ATILD)", International Journal of Signal Processing Systems, ISSN (Print) 1939-8018, ISSN (Online) 1939-8115, Springer Verlag. Accepted November 2010 and published online.

[26]. Ghoshal N., Mandal, J. K. et al., "A Framework for Block based Image Authentication (FBIA)", Proceedings of 4th IEEE International Conference on Industrial and Information Systems, ICIIS09, ISBN: 978-1-4244-4837-1, Peradeniya University, Sri Lanka, pp. 343-348, December 28th -31st, 2009.

[27]. Ghoshal N., Mandal J. K., "Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT)", International Conference on Computer and Systems, ICCS-2010, ISBN: 93-80813-01-5, University of Burdwan, West Bengal, India, pp. 144-150, November 19-20, 2010.

[28]. Ghoshal N., Mandal, J. K., "Controlled Data Hiding Technique for Color Image Authentication in Frequency Domain (CDHTCIAFD)", 2nd International Conference on Emerging Applications of Information Technology, EAIT-2011, CSI Kolkata Chapter at Science City, Kolkata, India, February 19-20th, pp. 284-287, 2011

[29]. Ghoshal N., Mandal, J. K. "Discrete Fourier transform based Multimedia Color Image Authentication for Wireless Communication (DFTMCIAWC)",2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Le Royal Meridian Chennai, India, 28th Feb.- 3rd March, 2011

