International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Hybrid Frequency Domain Based Robust Digital Video Watermarking Technique Exploiting Fast Motion Frames

Rakesh Ahuja, Mohd Junedul Haque

Abstract*: *The rapid development of speedy internet bandwidth transfers the multimedia video objects from one system to another almost immediately. In addition, the digital technology has a capability to produce exact multiple copies of the original video data. This technique can be exploited by unauthorized user to create and distribute multiple identical copies of the original video in an unauthorized way. These productive technologies arise serious concern of copyright protection and to trace the unauthorized user. The proposed technique extracts the motion frames of the video. These extracted frames are used to embed the copyright information as watermark using hybrid techniques as Singular Value Decomposition and Discrete Wavelet Transform. The experimental results show that the scheme is robust to unintentional and intentional video specific attacks considered being frequently occurring attacks.

Keywords : ***Copyright Protection, DWT, Digital Video Watermarking, Motion Frames, Multimedia Security, SVD***

I. INTRODUCTION

The rapid development of internet bandwidth exploded the propagation and spreading of digital data across the globe instantaneously. This digital video data can be effortlessly imitated and speedily transferred from one system to another over just a regular internet connection. Thus, several issues like data authenticity, copyright protection, confidentiality and ownership identification came into existence and their prevention became the major concern in the field of multimedia security [1]. In order to secure the multimedia data, various information hiding schemes like cryptography, steganography and watermarking were developed.

The cryptography technique secures the content when the bit stream is in transit phase in such a manner that unauthorized user neither read nor modify the content before reaching to the destination workstation. Yet, this method cannot secure the content from the receiver to reproduce and transfer the content illegally once it will be decrypted at the destination end. So, a vital demand arises to develop the technique to secure the content from the receiver itself. Thanks to the watermark technology which solve this serious concern. Digital watermarking inserts the copyright information into the original video content in an imperceptible manner so that no unauthorized users neither create the multiple copies nor claim for having copyright for the same multimedia contents. The type of application decided that the type of embedding information. For example, if there is a requirement to protect the copyright then copyright image or text will be embedded into the host signal otherwise if the requirement is to claim the ownership then the owner information as watermark is inserted into the cover object. Other categories of implanted signature are serial number, logo, copy control signal, gray level image, binary images, color pictures, distributor information, text, client name, date of transactions and any type of possible digital formats. Therefore, digital watermarking was recognized as the most secure method as it utilizes techniques to implant the data stealthily into original multimedia contents in noisy channels [2]. On the other hand, a watermark is embedded into data file to guarantee the genuineness of the multimedia data as required in several important applications like e-health, fingerprinting, forensic, protection of social digital contents, e-voting and driver licenses, military, remote education, media file archiving, broadcast monitoring and digital cinema[3]. Thus, there is need to develop effective watermarking methods that can offer good trade-off between the benchmark parameters for the above considered applications. Nowadays, there is wide usage of video content in diverse areas like advertising, video conferencing, movies, video calling, video chatting, online video games etc. which leads to wide interest in the field of information and multimedia security [4]. Thus, the concept of digital video watermarking became popular which could be implemented by embedding a specific image or bitmap prototype in the video content to ensure the protection of copyrights as well as ownership identity. One should also focus on the basic characteristics of the video are termed as robustness [5] , perceptibility, capacity and security. There are other areas of relevance of digital video watermarking like fingerprinting which uniquely identifies the fingerprint by software that distinguishes, extracts and then compacts the several components, copy control which refers to illegal copy prevention system, broadcast monitoring is considered as the activity of monitoring the output of print, online and broadcast media and video authentication is a process which ascertains that the content in the given video is authentic and exactly same as when captured. These watermark signals are used in a wide variety of watermarking applications [6] includes broadcast monitoring, fingerprinting, copyright protection, ownership protection,

Revised Manuscript Received on May 15, 2020.
* Correspondence Author
Rakesh Ahuja, Computer Science & Engineering, Chitkara University, Rajpura, Punjab, India. Email: rakesh.ahuja@chitkara.edu.in
Mohd. Junedul Haque*, Computer Science & Engineering, Chitkara University, Rajpura, Punjab, India. Email: jundel.haque@chitkara.edu.in

copy control, authentication, integrity and many more. Such applications applied to multimedia objects like images, audio and video. There are numerous digital video watermarking techniques have been anticipated for almost all types of cover signals especially for image and video. It is well established fact that the exhaustive and successful task has been carried out for image watermarking but lot of issues still requires attention for video watermarking. The more challenging issue is that which type of watermarking would be appropriate for which type of video signal. The types of video signal [7] may be original or compressed exploited for watermarking. If original video signal is considered then frequency domain base watermarking techniques as contrast to spatial domain would be better way otherwise compression standard like MPEG-2, MPEG-4, H.264 will be exploited to implement wide variety of applications of video watermarking.

An extensive survey about video watermarking features, applications, design principles, embedding and extraction methods, type of original or compressed video signals, transformed video signal or even the watermark could be inserting while applying the compression of video are best described by [8]. A noteworthy research has already been done for all three categories of video objects but the issues of balance trade off among robustness, perceptibility and capacity are still a major challenge to achieve in an effective manner for specific intentional and unintentional attacks. The geometric attacks are resizing, rotation and cropping yet other image processing attack includes filtering, sharpening, brightness, contrast and blurring and histogram equalization attacks. The robustness must also check for Type-1 and Type-2 collusion, JPEG compression, de-noising, cryptographic attacks, quantization, scanning and lot more. In this series, intentional and unintentional video specific attacks are also judge that are not carried from digital image watermarking. Inserting frames from other video clips like inserting advertisement into the movie includes unintentional video specific attacks. The sensor may cut down the vulgar scene from the video data covers frame deletion unintentional video specific attacks. The intentional video specific attacks are to be evaluate for frame averaging and frame replacements attacks. All above mentioned attacks must include to provide the strengthens of video watermarking algorithm. Two other parameters of imperceptibility and capacity are also having equally importance while designing the video watermarking. Yet, it is not always been easy to make balance tradeoff among these requirements as they are conflict in nature. The reason is that while providing the strengthen to any one of parameters other parameters may require to compromise. Hence there is always a challenge to implement correct balances among these three features.

The structure of the paper is organized as follows. Section 2 described the literature review linked to digital video watermarking. The preliminaries are explained in Section 3. The digital video watermarking algorithms are illustrated in Section 4. Section 5. is set for simulation results and discussion. Section 6 conclude the delivered the video watermarking process.

II. RELATED WORK

Yogesh [9] suggested a method in order to identify the watermark from the distorted video with the use of barrel distortion model and helps in its accomplishment. In order to protect the video and manage the security, there exists several issues and out of all, the issue of distortion is highly observed. The reason of distortion in the source component may be sometimes superfluous and the outcome is that the watermark cannot be detected from the original video. There are several models in order to handle this issue but the authors worked on the said approach to discern the watermark from the distorted video by calculating various parameters like correlation, structural similarity index (SSIM) and mean square error (MSE) to notice the accurate watermark signal.

Tejas [10] proposed a methodology for advanced video watermarking dependent on hybrid wavelet transform (HWT) composed of Cosine, Haar, Kekre, Walsh, Slant and Sine transforms. Earlier, it had been suggested by the researchers that the use of hybrid wavelet transforms was superior in comparison to orthogonal transforms. In this strategy, initially the frames of the original video were extracted and the HWT is technique was applied on both the components of the video i.e., frame as well as the watermark. The altered watermark was then embedded in the video frame. The authors performed the experiment on 15 different videos and watermarks. The outcome of the experiment showed that the Kekre and Haar transform approach gave improved output as compared to amalgamation of the other transforms. It was verified by computing the parameter mean square error (MSE) between the source and resultant watermark which comes out to be minimum for the said combination. Shahid [11] mentioned that due to the usage of high-speed internet worldwide, the huge amount of digital content being shared and transferred from one place to another. In this transmission of digital data, a variety of intentional and unintentional attacks can damage the digital information like noise addition, compression, frame cropping and averaging etc. Thus, there exist a need to propose some techniques to make the digital data safe and sound from illicit replication and ownership theft. In order to protect the digital videos, the concept of watermarking had been introduced which was proven to be the best methods for maintaining security in videos till now. This method was executed by hiding some information in the form of an image, audio or text in the frames of the video to uphold genuineness. It involved the usage of various kinds of equations to implement the given method in the still frames of a video. This paper presented a detailed review with the important features, applications and challenges faced by the research scholars in the video watermarking. Patel [12] suggested a more secure and strong watermarking scheme which was based on scene identification. The initial step of the approach was to take out the original video into different scenes. Discrete wavelet transforms (DWT) technique was implemented on every scene of the video to convert it to the wavelet field. Similarly, the jumbled watermark was also decomposed and inserted into the coefficients of different frames of the video.

Retrieval Number: D8945049420/2020©BEIESP
DOI: 10.35940/ijeat.D8945.069520
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The author compared the proposed scheme with other available watermarking techniques. It was observed that the strength computed by a parameter normalized coefficient (NC) of the given approach against several familiar attacks is improved. Neena [13] focused on the e-learning system where the mentors put the file repositories and videos on the web. Here, the main issue is to protect the data from copying which can be overcome by the method of digital watermarking. In the proposed approach, three different methods of video watermarking were used for watermark insertion with the help of various frequency domain transforms i.e., discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete Fourier transform (DFT). The parameters Peak signal-to-noise ratio (PSNR) and Bit Error Rate (BER) were computed to access the effectiveness of the watermarking scheme. Several spatial and compression attacks were implemented on the video and the output was compared which showed that the DWT technique was extra proficient and tough against the attacks.

A lot more digital video watermarking techniques were suggested based on the techniques of scene change based [14], frequency transform domain [15], combination of various frequency domain. spatial domain and it is found that none of the techniques accomplished adequate to fulfil all three characteristics of watermarking. Both, motion and motionless frames are used to insert the watermark by using scene change methods. This technique has serious issues especially when motionless frames are used to embed the watermark because such type of video frames may statistically average or compared these areas in order to remove the watermark. Another issue arises with these types of watermarking method is that if the occurrence of video scenes is frequent in nature or have many different rapid scenes, then further it is not logical to implement the scene based video watermarking. The only solution is to have only motion frames for watermarking purpose by using robust hybrid frequency technique and for more security the watermark must be encrypted before embedding into the video bit stream.

In order to resolve all the issues related to video watermarking purposes, the current paper suggested to implement the watermarking technique for video multimedia objects by considering only motion frames. These key frames are first extracted to be exploited for watermarking purpose and passes through two major transformation as discrete wavelet transform (DWT) and singular value decomposition (SVD). The key features of the proposed scheme is that the different segment of encrypted watermark are embedded into different frequency sub-bands of motion frames only. The relation between motion frame and part of scrambled watermark image is varied for each individual video.

This technique provides the high toughness due to revealing only few frames not entire video frames as watermarking process never includes motionless frames which are much greater in number as compared to motion frames. As few frames are updated therefore higher perceptibility is obtained. This approach is suitable for those application where original video as well as original watermark are available hence the proposed technique comes under nonblind video watermarking.

III. PRELEMINARIES

A. Partitioning The Encrypted Image

Typically, the watermark object is encrypted to provide the double security before embedding into the video object in order to make the plain watermark image worthless. An encryption technique of double column transposition method [16] is used to scramble the binary watermark image. Encrypted watermark is partitioned into number of sub-images as per the number of elements in the symmetric key and then rearrange and combined them as per the following equations:

Key=[k_{16}, k_1, k_{14}, k_{03}, k_{12}, k_5, k_{10}, k_8, k_{15}, k_7, k_6, k_{11}, k_4, k_{13}, k_2, k_9]; (i)

The image is transposed to get the intermediate encrypted image. Th process is iterated thirty-two times to get the concluding encrypted image to be embedded into the potential video frames. The watermark image Cameraman.tif and encrypted image are shown in Fig. 1. and Fig. 2 respectively. It is obvious that the shape of the scrambled image becomes meaningless and can never be extracted to get the unscrambled watermark until and unless knowing the encryption key and algorithm.

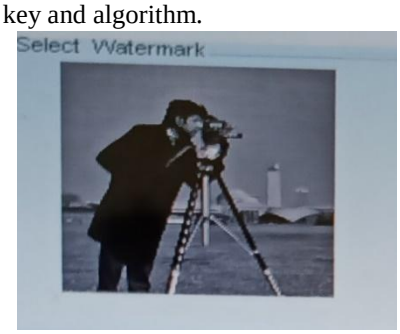

Fig .1. Original watermark

Fig. 2. Scrambled watermark

The number of partitioned scrambled watermark image is directly proportional to the number of motion frames and inversely proportional to the number of elements in the symmetric key as defined below.

- Partitioned Image ∝ Motioned Frame/Number of Key elements
- Partitioned Images = C x Motion Frames/Key Elements, where C ∈ constant

$$= \left\lfloor \frac{Frames\ having\ Motion}{Elements\ in\ Symmetric\ Key} \right\rfloor_4 \quad \text{if } C=1/4 \qquad (1)$$

The proposed scheme utilized *Gemini* video sequence having 300 frames with 200x230 frame size and watermark image *Cameraman* is used for embedding purpose. An algorithm defined in section 3.2 is used to extract the motion frames.

Once knowing the number of motion frames and elements in symmetric key, the number of encrypted watermark images can be calculated from equation (i) and shown in Fig 3.

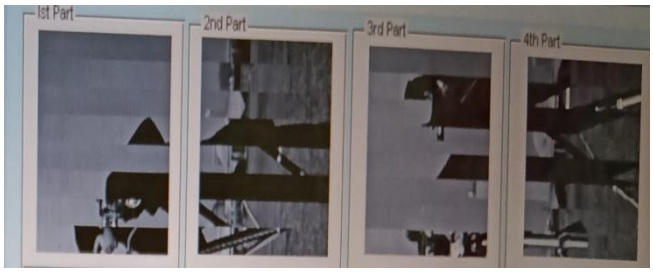

Fig. 3. Four parts of scrambled images

B. Extraction of Motion Frames

All Calculate the histogram of two adjacent frames in the original video. Then, evaluate the absolute difference between these two histograms and store the difference into the buffer. Evaluate the sum of elements stored in the buffer and check if the final sum is exceeded than the pre-decided threshold then the second frame shall be treated as motion frame and buffered the same into newly generated array. This process is repeated for all the frames to extract all the motion frames and stored into separate video file MotionFrameVideo.

The proposed algorithm extracted 10 frames as motion frames from the dynamic video Akiyo if the threshold set to 4000.

IV. VIDEO WATERMARKING SCHEMES

The projected algorithms described a unique technique to embed the copyright information as watermark into video object. The watermarked video object is constructed by embedding the different parts of encrypted watermark into different motion frames and then watermarked motion frames are replaced with their corresponding original position of non-watermarked motion frames without changing the sequence of motionless video frames. If the number of motion frames are more than the number of partitioned encrypted watermark images, then the insertion process will continue to embed the watermark from scratch.

A . Watermark Embedding Scheme

Read each RGB frame from the MotionFrameVideo and convert the RGB frame into three chrominance channel (Y, Cb and Cr). Applying two times HAAR wavelet transform to extract the lower frequency energy component (LLLL) from the luminance component (Y). start the embedding process by converting the Motion Frames into luminance (Y) and chrominance components (Cb, Cr) by means of the Equation [15]. Applying SVD operation on LLLL to find three components as two orthogonal (ULLLL, and VLLLL) and one diagonal component (SLLLL). Pick the first encrypted watermark and resized to LLLL and apply the SVD to generate three Matrix (UWM, SWM, VWM). Adjust SLLLL with SWm in the following ways

$$S_{AA} = S_{LLLL} + \mu S_{WM} \quad (2)$$

Where μ is set to 0.01 by considering different videos and different watermark to make balance tradeoff between the perceptibility and robustness. Reconstruct the watermarked frame by applying inverse SVD and inverse DWT operation.

The process is continued for all motion frames. Finally, all these watermarked frames are replaced with their corresponding non-watermarked motion frames without changing the sequence of motionless frames to generate the watermarked video.

B. Watermark Extraction Scheme

Extract all the Motion Frames from the watermarked video and make separate file WtrMotionFrames. Read each frame from the WtrMotionFrame then convert into luminance and chrominance components (Y Cb, Cr). Apply DWT twice time on luminance component Y' component to generate lower level coefficient LLLL' followed by SVD to get UWA , SWA and VWA.

SWC ' =(SAA - SWA)/ μ (3)

Estimate the part of encrypted watermark object

ExWt1= UW * SWC ' * VW (4)

Similarly extract 2nd part of encrypted watermark from 2nd frame. The above process is continued to extract entire parts of encrypted watermark. Encrypted watermark image is combined by summing up entire extracted images divided by total number of Motion Frames.

V. SIMULATION RESULTS

The color video sequence Gemini consisting 300 video frame with frame size 176 * 144, used for simulation purpose. The image used for inserting the watermark is Cameraman.tif of size 50 * 100. Two major parameters perceptibility (PSNR) and robustness (NC)are evaluated

Peak Signal To Noise Ratio (PSNR) =

20 log10(maxi / √MSE) where (5)

$$MSE = 1/MxN \sum_{i=1}^{M} \sum_{j=1}^{N} ||WV - WV'|| \quad (6)$$

MSE is defined as Mean Square Error between the watermarked and original and frame. An instance of 25th frame of original video Akiyoi and related watermarked frame shown in Fig 4.1a and Fig. 4.1b respectively.

Fig. 4.1a Original frame from Foreman

Fig. 4.1b Corresponding watermarked frame

S.No.	Attack	NC
1	Rotation	0.8923
2	Cropping	0.9221
3	Frame Averaging	0.9312
4	Frame swapping	0.9412
5	Frame Replacement (10%)	0.9100
6	Frame Deletion(10%)	0.9245
7	Speckle	0.8120
8	Poisson	0.4932
9	Gaussian	0.8605
10	Salt and Pepper	0.8732
11	Lossy Compression	0.8251

A robustness is obtained between original and extracted watermark defined as

NC=

$$\frac{\sum i \sum j . W_{ij} * W'_{ij}}{\sqrt{\sum i \sum j (W_{ij})^2} \sqrt{\sum i \sum j (W'_{ij})^2}} \qquad (7)$$

where Wij and W'ij are the pixel intensity of the ith row and jth column of extracted watermark respectively. The robustness and perceptibility of the proposed scheme are 0.996432 and 52 dB respectively. The watermark and its four parts are showing in the Fig 5.1a. The scrambled watermark at source and destination and unscrambled watermark are shown in Fig. 5.1b1, 5.1b2 and 5.1b3.

Fig. 5.1a Original Watermark and its Four Sub-Parts

Fig 5.1b1 **Fig. 5.1b2** **Fig. 5.1b3**

5.1b1 Encrypted watermark at Source End,
5.1b2 Extracted Scrambled Watermark at Receiver End,
5.1b3. Decrypted Version of The Extracted Watermark

A. Robustness Evaluation

Numerous experiments have been conducted to the watermarked video to get the degree the sturdiness of the projected theme. Most of the robustness evaluation are based on the properties of video. The essential property of video is known as temporal characteristic defined as sequence of video frames. Malicious user can swap some of the adjacent frames corrupt the added information while maintaining the perceptibility of video object. The second distinguish feature of video is to have High redundancies is another property of video may also use by malevolent user to perform frame averaging, dropping, deletion and insertion and swapping to destroy the watermark embedded in the watermarked video. Other categories of attacks are genetic from image watermarking. These are geometric attacks covers scaling, cropping and rotation. Some are noise attacks as Poisson, Gaussian, Salt and Pepper, Speckle noise. Unintentional attacks are compression, contrast adjustment, filter attack may disturb the inserted watermark. Hence, the simulation results estimate the toughness of watermark system by covering all above defined attacks.

VI. CONCLUSION

The scheme eliminates the issues caused by scene-based video watermarking. In general, the compression algorithms eliminate the motionless part of the movie. Hence, the presented algorithm survives against compressions of lossy types. Yet, insertion of watermark in the motion regions is rarely noticed by viewer as HVS is less delicate to motion sections. Furthermore, this algorithm is implemented by considering two powerful mathematical transformations.
The watermarking algorithm exploited DWT technique to get low frequencies sub-bands, a rich source of energy, provides high level of robustness against intentional and unintentional attacks. A little alteration in these frequencies doesn't affect the perceptibility, reflect high quality of watermarked video is obtained. This technique is well suited for those application where original video and watermark both available hence to retrieve the watermark hence used for private watermarking application. The future work shall also cover more robustness against collusion, ambiguity and compression attack to protect the copyright and authorization both in a single scheme.

REFERENCES

1. A K Singh, B Kumar, M Dave, S P Ghrera and A Mohan, Digital Image Watermarking: Techniques and Emerging Applications, B. B. Gupta et al. (Eds.) Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, USA, pp. 246-272, 2016
2. Joo Lee and Sung-Hwan Jung, A survey of watermarking techniques applied to multimedia,Proceedings 2001 IEEE International Symposium on Industrial Electronics (ISIE2001), Vol. 1, pp. 272 -277, 2001
3. Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A, Multiple watermarking technique for securing online social network contents using back propagation neural network, Future Generous Computation System 86, pp.926–939, 2018
4. Mrs. Rashmi G. Dukhi, Watermarking: A Copyright Protection Tool, Proc. of the IEEE, pp. 36-39, 2011
5. J.-P. Linnartz, The Ticket concept for copy control based on embedded signaling, in: Proceeding of the Fifth European Symposium on Research in Computer Security. Lecture Notes in Computer Science, Vol. 1485, Springer, Berlin, pp. 257-274, 1998
6. Doerr, G. and Dugelay, J.L., 2003. A guide of video watermarking. Signal processing: Image communication, 18(4), pp. 263-282,2003
7. Ahuja Rakesh, S. S. Bedi, Compressed Domain Based Review on Digital Video Watermarking Techniques. Information Technology of Elixir International Journal, 101, pp. 43622-43633,2016
8. Ahuja, R. and Bedi, S.S. All Aspects of Digital Video Watermarking Under an Umbrella. International Journal of Image, Graphics and Signal Processing, 7(12), p.54, 2015
9. Yogesh Verma , Manjit Singh , Implementation the Effects of Barrel Distortion in field of Digital Video Watermarking, International Journal of Science, Engineering and Technology Research (IJSETR) Vol. 6, Issue 6, 2017
10. Tejas s. Kulkami, Jaya H. Dewan, Digital Video watermarking using Hybrid Wavelet Transform with Cosine, Haar, Kekre, Walsh, Slant and Sine transforms, International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, 2016
    Md Shahid and Pradeep Kumar, Digital Video Watermarking: Issues and Challenges, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 4, ISSN: 2278 – 1323, 2018.
11. Snehal V. Patel, Arvind R. Yadav, Invisible Digital Video Watermarking Using 4-level DWT, National Conference on Recent Trends in Engineering & Technology, 2011
12. Neena.P.M, Athi Narayanan.S, Kamal Bijlani, Copyright Protection for E-Learning Videos Using Digital Watermarking, Fifth International Conference on Advances in Computing and Communications, IEEE, pp. 447-450,2015
13. Chan, P.W., Lyu, M.R. and Chin, R.T., A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation. IEEE transactions on circuits and systems for video technology, 15(12), pp. 1638-1649, 2005
14. Abdallah, E.E., Hamza, A.B. and Bhattacharya, P., 2010. Video watermarking using wavelet transform and tensor algebra. Signal, Image and Video Processing, 4(2), pp. 233-245, 2010
15. Ahuja, R. (2019). Design of Digital Video Watermarking Technique Based on Motion Frames. Journal of Computational and Theoretical Nanoscience, 16(10), 2019

AUTHOR PROFILE

Dr. Rakesh Ahuja is PhD in Computer Science & Engineering. He is having 24 years of experience in Academic, Research and Industries. His areas of expertise are Information Hiding, Digital Right Management, Multimedia Security and Pattern Recognition. His areas of interest include Database Management System, Real Time System, Distributed System, Software Engineering and Operating System. He has supervised several ME Scholars in the areas of Information Hiding.

Dr. Mohd. Junedul Haque is Ph.D. in Computer Science and Engineering. He is having 8 years of experience in Academic, Research and Industries. at UG and PG levels of Computer Science & Engineering. His areas of interests are image processing, data warehousing, data mining and multimedia technology, computer networks. The author has published four books.