Design and Implementation of the Robust Watermarking Technique for the Raw Digital Video based on CDMA

Monica Gupta, Gurashish Singh, Ankit Gupta

***Abstract*— Since a long time, use of Spread Spectrum techniques for watermarking of still images has been prevalent. However working on stationary images involves several complications; subject to which this paper presents a novel approach for implementation of Watermarking on Uncompressed Digital Videos. The choice of this technique is due to the fact that Digital Video, by virtue of its time-space property, fits the direct sequence spread spectrum more readily; hence, working at the bit plane level is suitable. The spread Watermark signal and the noise already present in the image signal bear some resemblance and therefore it is not easy to detect the watermark signal. However several trade-offs have to be done in the area of Digital Video Watermarking. The simulation results obtained from the study clearly show that there is a trade-off between the robustness and the visibility of the selected watermark. For checking the reliability & robustness of the developed technique, several types of attacks have been performed on the Watermarked Video. The recovery of the Watermark from the Watermarked Video has also been performed to see the challenges caused by frame dropping etc. The results show that the attacks in destroying the synchronization at the Watermark detector as well as the noise can be resisted by using the above approach.**

***Index Terms*— Digital-Video, Spread-Spectrum, Steganography, Video-Processing, Watermarking**

I. INTRODUCTION

Ease of capture, transmission, and storage of digital data and the success of the Internet and digital consumer devices has caused a profound change in our daily lives. However, this has raised a big concern of securing the data and preventing unauthorized use. This issue has posed problems in many areas. For instance, due to illegal copying and downloading of copyrighted materials from the Internet, the music and video industry loses billions of dollars per year. As an effect, Digital Watermarking is being used very frequently and has become an attractive research topic. Digital Watermarking is a technology that generates and detects invisible markings, which can be used to trace the authenticity of digital data. Ideally, it should be hard to notice, difficult to reproduce, and impossible to eliminate without destroying the medium they protect. In future, Digital Watermarking will assist in copyright protection, pirate tracking, copying protection, image authentication and major areas of cover-up communication [1][2].

The roots of Watermarking are considered to be in the study of "Steganography". The word comes from the old Greek language and can be translated to "cover writing". Steganography was basically a way of transmitting hidden (secret) messages between allies, being used as early as 1000 B.C. It has initial references in *Homer's "'Iliad"* and *"'Histories of Herodotus'"* (440 B.C.) [3].

Generally by Watermarking, one is hiding a message signal inside a host signal, which is devoid of any perceptual distortion by the host signal. As the word "Watermarking" suggests, the mark itself is "transparent" or unnoticeable for the human perception system. Usually, the host signal is a digital media, like audio, video or images. As we all know, the Human Visual System (HVS) is far from being perfect. Furthermore, for images and videos, it is possible to modify the pixel values without the watermark being visible. Provided that a certain HVS threshold is not exceeded, the modified (watermarked) image or video will be undistinguishable to the human eye in comparison to the original [4].

The main application of Digital Watermarking is in *copyright protection*. The owner of the image or video adds a watermark to his material before it is distributed. In this way, it is possible to track illegal copies of the copyrighted material. Certain popular ones are broadcast monitoring of video sequences (digital TV), audio compact disks (CD's) protection, its access control, database retrieval and robust identification of digital content.

There are different types of Watermarking techniques and methodologies. Depending upon the resources available and the application, the appropriate technique is chosen.

II. DIGITAL WATERMARKING SYSTEM

In Digital Watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information is also carried in the copy. A signal may carry several different Watermarks at the same time [5]. Video Watermarking can be achieved by either applying still image technologies to each frame of the movie or with the application of dedicated methods which exploit

inherent features of the video sequence. There can be various kinds of attacks on the Watermarking system which are discussed in the later sections. Tabassum and Islam have only considered Gaussian and Salt-Pepper noise. No other type of attack has been taken into consideration [6]. The most important unintentional attack is of Lossy Compression. In most cases, the LSB-plane bit distribution is random and can be safely replaced by the Watermark. However, LSB plane is vulnerable to noise and other disturbances as described by Dr. Ajit [7]. The LSB substitution is less robust, prone to distortion and faces security issues. But bit-planes can be used to embed a Watermark with little to negligible effect on quality. Watermark placement in one of the four lower bit-planes does not significantly affect the video quality [8]. Kumari has discussed a method where the number of bits per character is being increased from 8 bits to 12 bits. This means an obvious increase in the overall size of the image. Moreover, it has discussed only about Textual Watermarking while LSB substitution is more viable for Video Watermarking [9][10]. Hence, we have proposed a more robust technique of bit-plane substitution Video Watermarking based on CDMA (Code Division Multiple Access).

If we look at the Watermarking system as shown in Fig.1, it consists of three Subsystems, namely:

- Watermark Insertion Sub-system
- Attacking Sub-system
- Watermark Detection Sub-system

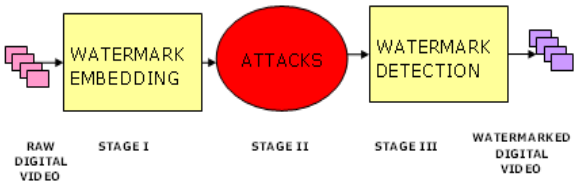

Fig.1. Stages of a Watermarking System

II.I WATERMARK INSERTION SUB-SYSTEM

First, the Video signal is modeled as a sequence of bit-planes, arranged along the third dimension; Time. Watermarking of this sequence is a two layer operation. A controlling m-sequence first picks candidate bit-planes for watermarking. Watermark, defined as m-frames, supplants the tagged bit-planes. It will be shown that the watermark, when limited to the four lowest bit-planes, is unnoticeable. Moreover, attempts in corrupting the image to destroy the watermark render the video useless before damaging the seal itself [11][12].

We model digital video as a function in time and space which is represented by $I(x,y,t)$. $I(x,y,t)$. It is then sequenced along the time axis as bit planes as shown in equation (1):

$$I(x,y,t)=\sum_{j}\sum_{n=0}^{b} i\left(x,y,t-\left(jT_f+nT_b\right)\right) \tag{1}$$

Where *i()* is the *n*th bit plane of the *j*th frame positioned at { *t = jTf + nTb}*. *Tf* and *Tb* are frame length and bit-plane spacing respectively and are related by *T = bTb* where *b* is the number of bit-planes per frame.

We define the Watermark by a bit-plane, *w(x, y)*, with spatial dimensions that match with the video frames. The content of the Watermark plane is selected to conform to varied requirements. It contains a graphical seal, textual information about the source or any other data that is deemed appropriate for Watermarking. In the context of CDMA, *w (x, y)* is treated as the message. This message is then spread using a 2D *m*-sequence or *m*-frames f (*x, y, t)*. To generate *m*-frames, a one dimensional *m*-sequence is rearranged in a 2D pattern. Depending on the period of the *m*-sequence and the size of each video frame, the 1D to 2D conversion may span up to *k* frames and will repeat afterwards. Spreading of the "message", i.e. the watermark *w(x, y)* is now defined by a periodic frame sequence given by equation (2):

$$w_{ss}=w(x,y)\sum_{j=0}^{k-1}\phi_j\left(x,y,t_j\right) \tag{2}$$

Where ϕj (*x, y, tj)* is the ϕj positioned at yet to be determined locations *t= tj*. The *wss* must now be aligned with and inserted into the video bit-plane stream. Fig.2 depicts the General module and Fig.3 depicts the Working Stage I.

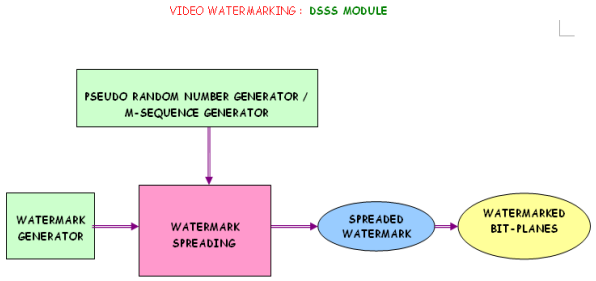

Fig.2. Direct Sequence Spread Module

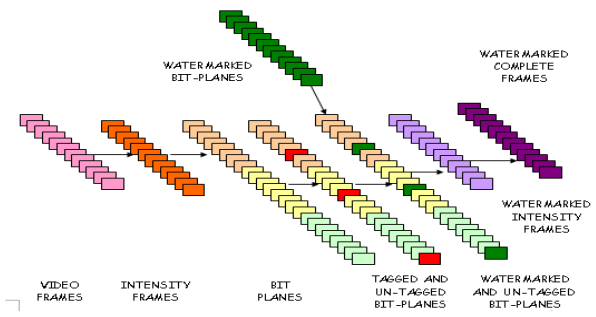

Fig. 3 Working of Stage I

The embedding algorithm works in each frame as shown in Fig.2 and equations (1),(2); the bit-plane at $t= tj$ is tagged, removed and then replaced by ϕj (x, y, tj). We can now align *wss* with the timeline as shown in equation (3):

$$w_{ss} = w(x,y)\sum_{j=0}^{k-1}\phi\left(x,y,v(j)T_b\right) \tag{3}$$

wss is now a spread spectrum version of the watermark at pseudo-random locations determined by *v(j)* .The second task is accomplished by using *v(j) Tb* as pointers to the candidate bit-planes where the Watermark must be inserted. In order to take the last step, the designated bit-planes must be removed and replaced by the corresponding elements of *wss*. The formalism to achieve this goal is through the use of a gate function defined by equation (4):

$$gate\left(t - v(j)T_b\right) = \begin{cases} 0 \text{ for } t = v(j)T_b \\ 1 \text{ otherwise} \end{cases}$$
$$0 \le t \le T_f \tag{4}$$

Multiplying video bit-plane stream by the gate function above removes the bit-plane at *v (j)*. The spread Watermark bit-plane stream is positioned such that the individual planes correspond exactly to the planes just cancelled by the gate function. Putting it all together, the CDMA watermarked video can be written as equation (5).

$$I_{wm}(x,y,t) = \sum_j \left\{ \sum_{n=0}^{b-1} i\left(x,y,jT_f + nT_b\right) gate\left(t - jT_f - v(n)T_b\right) + w(x,y)\phi_j\left(x,y,jT_f + v(n)T_b\right) \right\}$$
$$\phi_{j+k} = \phi_j \tag{5}$$

II.II Attacking Sub-System

The most important attack on a video is Lossy Compression as discussed before. As observed in Fig. 3, in the production chain, compression is usually applied before video broadcasting or before transferring the video to other devices through interfaces such as the IEEE 1394.

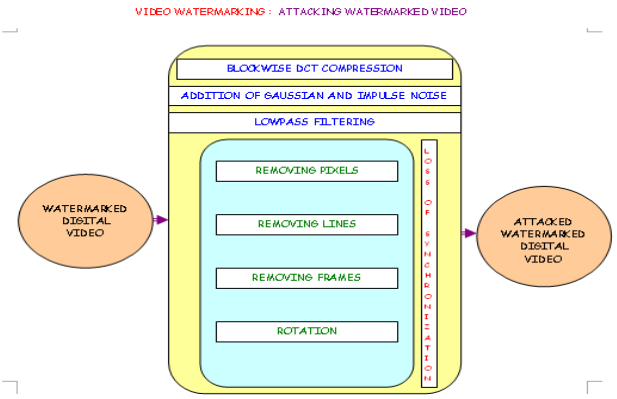

Fig.4. Complete Model Stage II

II.III The Watermark Detection Sub-System

As witnessed in Fig. 4, digital video is paradoxically more difficult medium to watermark than still imagery. Video by its nature is a wideband high bit-rate data carrying complex and dynamic information in the scene. Although complex Watermark embedding and extraction procedures may be practical for a single image, the same cannot be said for video due to the sheer volume of data. For the same reason, it is more difficult to tamper with or completely eradicate a video embedded Watermark [13]. Even a short segment of video contains hundreds of frames, increasing the chance that the embedded Watermark remains unscathed. Also, wideband nature of the data provides additional capacity for the placement of Watermarks with large information contents such as video-in-video applications.

The appeal of Spread Spectrum (SS) in Watermarking is understandable. Spread Spectrum (SS) is in many ways a secure data-hiding algorithm and so is Watermarking [14]. Early examples of SS watermarking goes back to Van Schynold who modified the LSB of each pixel by random amounts produced by an *m*-sequence generator because definition of spread spectrum was rather different. They applied perturbation to the first 1000 largest DCT coefficients of the entire image. The perturbations were drawn from a normal random number generator [2]. The choice of DCT coefficients was further refined to take into account the visual masking of Human Visual System. Smith and Comiskey framed watermarking as a modulation problem and adopted the direct sequence spread spectrum model. The closest work to the present paper is that of Hartung and Girod [15]. They have proposed a CDMA-style approach to video watermarking by first spreading a binary watermark by an *m*-sequence. Video frames are then rasterized and the spread watermark is added, pixel-by-pixel, to produce the watermarked video [16][17].

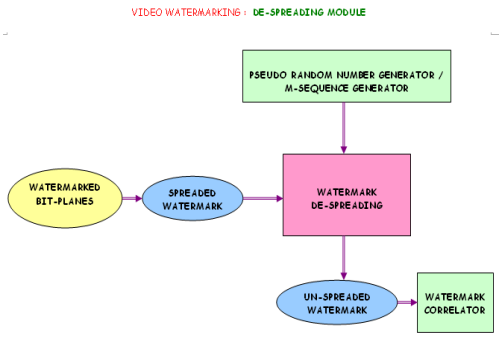

Fig. 5 De-Spreading Module

III. Important Applications

The technique of "Video Digital Watermarking" is one of the vital researches in the field of multimedia as well as in internet copyright protection field. There are various applications of Digital Watermarking (DWM) such as Broadcast monitoring, Owner identification, Proof of ownership, Transaction hacking, Content authentication, Copy control, Device control and so on [18]. Out of these, some important applications are described as follows-

A. Broadcast monitoring:

This application identifies what work is being broadcasted, by recognizing the watermarks embedded in the work. There are different technologies to monitor playback of sound recording. The DWM is an alternative to these technologies due to its reliable automated detection. The system can distinguish between identical versions of songs, which are watermarked for different distribution channels. A single PC-based monitoring station can continuously monitor upto 16 channels over 24 hours with no human interaction. The resultant monitoring is assembled at the central server and is now available to interested ones. Such system requires Monitoring infrastructure and the watermarks to be present in content [19].

Watermarking video or music is planned by all major entertainment companies possessing closed networks.

B. Encoding:

According to the thinking of major music companies and major video studios, encoding happens at the mastering level of sound recording. In such cases, transactional watermarks are also considered. Each song is assigned a unique ID from the identifier database. After completion of all mastering processes, ID is encoded in sound recording. To enhance encoding of audio or video recordings requiring special processing, the human-assisted watermark key is available [20].

C. Copy and playback control:

The data carried by the watermark may contain information about copy and display permissions. We can add a secure module into copy or playback equipment to automatically extract the permission information and block further processing, if required. This approach is being used in Digital Video Disc (DVD).

D. Content authentication:

The content authentication is nothing but embedding the signal information in Content.

This signature can then be checked to verify that it has not been altered. By watermarks, digital signatures can be embedded into the work and any modification to the work can be detected.

IV. Evaluation Study

In this paper, a framework for large scale watermarking of multimedia databases of uncompressed digital video is presented using the formalization of CDMA. Here it is illustrated that video, as a time-space function, is a natural candidate for application of Direct Sequence Spread Spectrum. In particular, CDMA format, by virtue of its multi-user structure, is particularly suitable for a centralized effort for source or destination based watermarking of large multimedia database titles.

V. Experimental Results

For obtaining the requisite results, a Video with frame size of 256x256 pixels for a total of 10 frames is run for 1 second.

The first task is to check for the visibility of the watermark. As can be seen from the watermarked frames and the WPSNR values which are 11.8770499 (dB), 20.4629089 (dB) and 25.5178578 (dB) respectively for MSB region, mid-SB region and LSB region. One can observe that the Watermark is more visible in case when MSB region is chosen for Watermarking. The Watermark becomes less visible as we move from MSB region to mid-SB region and then from mid-SB region to LSB region.

Now let us consider the issue of Watermark robustness. It is determined that the highest 4 bit-plane, that is MSB region, constitutes a safe place to hold the Watermark. Henceforth, It is verified that in this case, the extracted watermark planes correlate much higher with the original watermark planes than the image planes. Robustness of the watermark to noise is of interest. Noise may be added to Video to make the watermark undetectable. This approach of course can be self-defeating since Video quality degrades as well.

For the placement of the Watermark in the Video corresponding to the LSB region (bit-planes 1, 2, 3, 4) one of the 4 lower bit-planes is pseudo-randomly chosen. The 10 bit-planes chosen for 10 frames were {1 4 2 3 1 2 2 2 1 4} respectively, where 1 corresponds to the LSB plane. The watermarked and original video remains virtually indistinguishable even when viewed on a monitor.

For the mid-SB region bit-planes chosen were {3 6 4 5 3 6 4 5 3 4} while for the MSB-region bit-planes selected were {5 7 6 8 8 6 7 5 5 7 }.

The impact of frame drops, random or regular, which may arise either unintentionally or deliberately, is observed. For this phenomenon, Watermark recovery has been tested on the above footage. It is observed that random frame drops pose a more serious challenge. This process is defined by frame removals at random intervals and random frequency. There is an interaction between the times separating frame drops. So, we have shown that results from work in CDMA can be brought to work on Video Watermarking if similarities and differences are properly distinguished. The rich and multidimensional content of video opens up exciting extensions to the traditional signal-based work in CDMA. By the same token, the varied and complex nature of attacks for removing the Watermarking goes beyond the known problems that conventional CDMA signals have to cope with. However, the simplicity of embedding Watermark and then retrieval which happens at bit-plane level makes CDMA watermarking attractive in many multimedia applications. This includes large scale watermarking of multimedia titles by using a family of near orthogonal PN sequences.

Table 1 Comparison Table (Watermarking MSB Planes)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	74031106.	42.76027
2.	COMPRESSED WATERMARKED VIDEO	103.97940	42.62730
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	11.76866	42.33058
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	105.74031	42.75933
5.	AVERAGE FILTERED WATERMARKED VIDEO	7.10603	42.09642
6.	MEDIAN FILTERED WATERMARKED VIDEO	8.69034	42.40184
7.	WIENER FILTERED WATERMARKED VIDEO	11.58644	42.58419
8.	PIXEL REMOVED WATERMARKED VIDEO	105.74031	42.75986
9.	LINE REMOVED WATERMARKED VIDEO	14.00388	42.75753
10.	FRAME REMOVED WATERMARKED VIDEO	100.96910	42.30611
11.	FRAME ROTATED WATERMARKED VIDEO	5.26089	41.46110
12.	FRAME DROPPED WATERMARKED VIDEO	7.83133	41.98779
13.	FRAME SWAPPED WATERMARKED VIDEO	100.96910	42.65890
14.	FRAME INTERPOLATED WATERMARKED VIDEO	100.96910	42.68041
15.	FRAME RESIZED WATERMARKED VIDEO	9.68434	42.49543

Table 2 Comparison Table (Watermarking mid-MSB Planes)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	13.52162	42.75818
2.	COMPRESSED WATERMARKED VIDEO	9.32553	42.53660
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	6.76572	42.11660
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	13.32512	42.75754
5.	AVERAGE FILTERED WATERMARKED VIDEO	6.13199	42.06379
6.	MEDIAN FILTERED WATERMARKED VIDEO	7.77884	42.36815
7.	WIENER FILTERED WATERMARKED VIDEO	8.90655	42.46240
8.	PIXEL REMOVED WATERMARKED VIDEO	13.42684	42.75802
9.	LINE REMOVED WATERMARKED VIDEO	13.19362	42.75593
10.	FRAME REMOVED WATERMARKED VIDEO	10.71090	41.97366
11.	FRAME ROTATED WATERMARKED VIDEO	5.21541	41.47886
12.	FRAME DROPPED WATERMARKED VIDEO	7.20314	41.96130
13.	FRAME SWAPPED WATERMARKED VIDEO	11.08909	42.65455
14.	FRAME INTERPOLATED WATERMARKED VIDEO	12.26828	42.67096
15.	FRAME RESIZED WATERMARKED VIDEO	9.44666	42.50569

Table 3 Comparison Table (Watermarking LSB Planes)

SR. NO.	TYPE OF WATERMARKED VIDEO	WPSNR VALUE (IN DB)	CORRELATION VALUE (IN DB)
1.	UNATTACKED WATERMARKED VIDEO	10.37356	42.60753
2.	COMPRESSED WATERMARKED VIDEO	5.79322	41.97258
3.	NOISY(GAUSSIAN) WATERMARKED VIDEO	5.72204	41.99257
4.	NOISY(SALT & PEPPER) WATERMARKED VIDEO	10.11601	42.58388
5.	AVERAGE FILTERED WATERMARKED VIDEO	5.74295	41.96905
6.	MEDIAN FILTERED WATERMARKED VIDEO	6.49070	42.10196
7.	WIENER FILTERED WATERMARKED VIDEO	5.99368	41.97487
8.	PIXEL REMOVED WATERMARKED VIDEO	10.29709	42.59878
9.	LINE REMOVED WATERMARKED VIDEO	10.21187	42.59620
10.	FRAME REMOVED WATERMARKED VIDEO	9.39642	42.36540
11.	FRAME ROTATED WATERMARKED VIDEO	5.20732	41.48609
12.	FRAME DROPPED WATERMARKED VIDEO	5.87860	42.05949
13.	FRAME SWAPPED WATERMARKED VIDEO	8.49667	42.60600
14.	FRAME INTERPOLATED WATERMARKED VIDEO	9.03793	42.50943
15.	FRAME RESIZED WATERMARKED VIDEO	7.93948	42.36797

ACKNOWLEDGMENT

We would like to extend a word of thanks to Prof. J. Panda, Faculty, Department of Electronics and Communication Engineering, Delhi College of Engineering, New Delhi who guided us throughout this project and with whose constant gi

REFERENCES

[1] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, Feb. 98, p.26

[2] R. G. van Schynold et al, "A digital watermark", ICIP'94, pp.86-90

[3] I.J. Cox et al, "Secure spread spectrum watermarking for images, " ICIP'96, pp.243-246

[4] C. Podilchuk and W. Zeng, "Perceptual watermarking of still images," *IEEE Workshop on Multimedia Signal Processing*, June 1997, Princeton Press.
[5] F. Hartung, B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing* 66 (1998) 283-301
[6] Tamanna Tabassum, S.M. Mohidul Islam, "Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT", University Papers, Computer Science and Engineering Discipline, Khulna University, Khulna, Bangladesh
[7] B. Mobasseri, "Direct sequence watermarking of digital video using *m*-frames", Proc. ICIP'98, October 4-7, Chicago
[8] Dr. Ajit, Preeti Kalra, Sonia Dhull, "Digital watermakring", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013
[9] D. Sarwate and M. Pursley, "Cross-correlation properties of Pseudorandom and related sequences," *Proc. IEEE*, May 1980, pp.593-619.
[10] G. Rosline Nesa Kumari, B. Vijaya Kumar, L. Sumalatha, and Dr V.V. Krishna, , "Secure and Robust Digital Watermarking on Grey Level Images", International Journal of Advanced Science and Technology,Vol. 11, October, 2009
[11] Jonathan K. Su, Member, IEEE, and Bernd Girod, Fellow, IEEE," POWER-SPECTRUM CONDITION FOR ENERGY-EFFICIENT WATERMARKING," IEEE TRANSACTIONS ON MULTIMEDIA, vol. 4, no. 4, December 2002
[12] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Proc., vol. 6, no. 12, pp. 1673-1687, Dec. 1997
[13] M. D. Swanson, M. Kobayashi, A. H. Tewfik, "Multimedia data-embedding and watermarking techniques," Proc. IEEE, vol. 86, no. 6, pp. 1064-1087, Jun. 1998.
[14] J. K. Su, F. Hartung, B. Girod, "Digital watermarking of text, image, and video documents," Computers & Graphics, vol. 22, no. 6, pp. 687-695, Dec. 1998.
[15] F. Hartung, J. K. Su, B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in Proc. SPIE Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 1999, vol. 3657
[16] M. Kutter, F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in Proc. SPIE Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 1999, vol. 3657, pp. 226-239.
[17] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based watermark recovering without resorting to the uncorrupted original image," in Proc. IEEE Intl. Conf. Image Proc., Santa Barbara, CA, USA, Oct. 1997.
[18] J. K. Su, B. Girod, "On the imperceptibility and robustness of digital fingerprints," in Proc. IEEE Intl. Conf. Multimedia Computing and Systems, Florence, Italy, Jun. 1999, vol. 2, pp. 530-535.
[19] M. H. Hayes, Statistical Digital Signal Processing and Modeling, John Wiley and Sons, New York, NY, USA,1996
[20] G. C. Langelaar, R. L. Lagendijk, J. Biemond, "Removing spatial spread spectrum watermarks by non-linear filtering", in Proc. EUSIPCO 98, 1998, vol. 4. 2281-2284.

Monica Gupta is presently working as an Assistant Professor in Electronics and Communication Department of Bharati Vidyapeeth's College of Engineeering, New Delhi. She has completed her Masters in Technology in ECE from Delhi College of Engineering with distinction of merit. Her area of research includes digital image processing and digital system designing.

Gurashish Singh is currently in final year of Bachelors of Technology of Electronics and Communication Department in Bharati Vidyapeeth's College of Engineering. He is a student member of IEEE-HKN and has two published works in the field of Digital Image Processing and Verilog-HDL. The research field of interest broadly includes electronics and communication discipline.

Ankit Gupta is currently in the final year of Bachelors of Technology in Electronics and Communication Department of Bharati Vidyapeeth's College of Engineering, New Delhi. He is a gold medalist from Delhi Public School, RK Puram. He has been awarded twice by the Lambda Eta chapter of IEEE-HKN for academic excellence. The field of interest mainly includes subjects of electronics and communication discipline.

