



# **Tampering Detection and Localization in Video Using Fragile Watermarking**

Shital Divekar<sup>1</sup>, Prof. Nitin Dawande<sup>2</sup>, Prof. Suresh Rode<sup>3</sup>

Student, Dept. of E & TC Engineering, DYPSOEA, Ambi, Pune, India<sup>1</sup>

Associate Professor, Dept. of E & TC Engineering DYPCOE, Ambi, Pune, India<sup>2</sup>

Assistant Professor, Dept. of E & TC Engineering, DYPSOEA, Ambi, Pune, India<sup>3</sup>

**ABSTRACT:** The popularity of the internet is increased and due to which use of digital multimedia data is increased more rapidly. On many websites the user upload and share multimedia objects such as audio, images, and videos. It is necessary to add security to information to verify the authenticity of the uploaded multimedia objects so the digital watermarking protects the information against the illegal changes in the form of images, videos and audios. It is the process of embedding watermark in a signal such as an audio, video or image data which identify ownership of the copyright of such signal. There are three essential requirements of watermarking techniques -robustness, fidelity, capacity, so that they can handle several types of image artefacts. This paper gives review on different watermarking techniques for protecting the digital contents.

**KEYWORDS:** DCT, Watermark, hash value, QIM, Tamper Detection, DWT, RSA, PSNR.

## **I. INTRODUCTION**

In today's world digital multimedia are transmitted more easily and rapidly. Due to increased popularity of internet, As there are inexpensive and reliable storage devices are present and also editing software's which leads to unauthorized sharing of these multi-media for example video, audio and image. Video broadcast, DVDs, video conferencing, video surveillance, video on-demand, which takes into account the two main factors of video data that is authenticity and integrity. However, due to use of currently available low-cost video editing software's, it is now easy to eavesdroppers, who can make changes in the video content to harm the interests of the owner or the consumer. After Tampering with videos, which makes them unreliable and defeats the purpose of all these applications at its first place. Without authentication a video viewer or a consumer is not able to verify that the video which we are viewing is actually the original one that was really transmitted by a produce at the other end. And if the video is tampered, then there we have to detect tampering in videos and also we have to locate the areas where the tampering is done by intruder.

Encryption and digital watermarking are the techniques available for the authentication and of the digital multi-media such as digital watermarking and encryption. Encryption prevents the unauthorized access to the digital media. But Encryption has limitations in protecting the intellectual property rights, after the digital content gets decrypted, then there is there is nothing to prevent the illegal user from making changes into it. A new technology is needed to prove the ownership rights. This need attracted attention from the researcher community and industry leading to make better use of information hiding technique, called as digital Watermarking.

## **II. RELATED WORK**

Mehdi Fallahpour, proposed approach in paper, "Tampering Detection in Compressed Digital Video Using Watermarking", [1] that is based on the semi-fragile video watermarking technique to detect the tampering in compressed videos. Bhaskaran et al. proposed approach in patent, "Fragile Watermark for Detecting Tampering in images", [2] that is related to the fragile watermarks for tamper detection in images. H.-Y. Huang, proposed approach in paper, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," [3] that is an effective watermarking scheme using pseudo-3-D DCT and quantization index modulation (QIM). Maneli

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Noorkami, and Russell M. Mersereau, proposed approach in paper “ Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase.” [5] states a common approach for embedding the watermark in I-frames.

In this paper we have developed an algorithm for tamper detection and localization using fragile digital video watermarking. The digital signature of the hash value of the frame along with the micro-block numbers and frame number within the frame are inserted into the frame as a watermark in frequency domain. This method is very sensitive to modifications, maintains good capacity and transparency, also we can locate the region of tampering.

## III. PROPOSED ALGORITHM

In this paper we have proposed a watermarking scheme based on DCT domain. The raw input video frames are extracted from the video sequence. The watermark is generated by computing the bits of digital signature of the hash value of frame in DCT domain and the bits of the block numbers and frame numbers and are inserted in highest non zero frequency coefficient in DCT domain. The embedded watermark is extracted and verified using public key. The details of the proposed technique are described in Fig. 1.

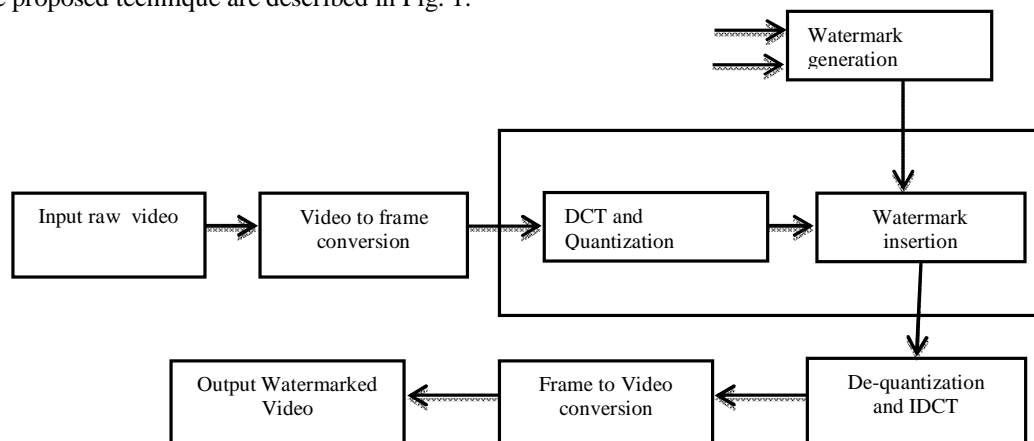


Fig. 1. Overview of watermarking process

The overview of watermark embedding process is shown in Fig. 1. The frames are extracted from raw input video sequences. The watermark generation process is explained in detail in Fig. 2. The frames are transformed into frequency domain by Discrete Cosine Transform (DCT). The watermark is embedded in Quantized DCT (QDCT) domain, the details of watermark insertion technique is shown in Fig. 3. Inverse Discrete Cosine Transform (IDCT) is applied to get back the watermarked frames. The frames are assembled into watermarked video.

### A. Watermark Generation:

To generate the watermark an input frame is scanned to compute the H, which represents the 128-bit hash value MD5 cryptographic function. The watermark is nothing but the bits of digital signature of hash value H and secret key Ks. Extract the frames from the videos. Initialize the hash value to some fix value. Each frame will be divided into a number of blocks which is then transformed into DCT domain by 2D DCT transform. The position of the highest non-zero DCT coefficient is stored so that it can be used while watermark extraction. The value of the JPEG quantization matrix corresponding to the highest non-zero coefficient is set to 1 so that after embedding the watermark bit the pixel value vary by plus or minus 1 instead of plus or minus q, which is corresponding quantizer value leads to less video distortion. Set LSB of the highest frequency component to zero and update the hash value. The watermark is nothing but the digital signature of the hash value H and secretes key Ks. At the time of watermark extraction again hash value is computed as it is updated iteratively block by block smallest alteration in watermarked media may destroy or completely modify the watermark. Along with this binary sequence of frame and block number is embedded into the DCT domain for tamper localization. We are using QCIF video having frame size of 176x144. Each frame is divided into micro-blocks of size 16x16, so we get such 99 blocks. To represent this in binary minimum 7 bits are required.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

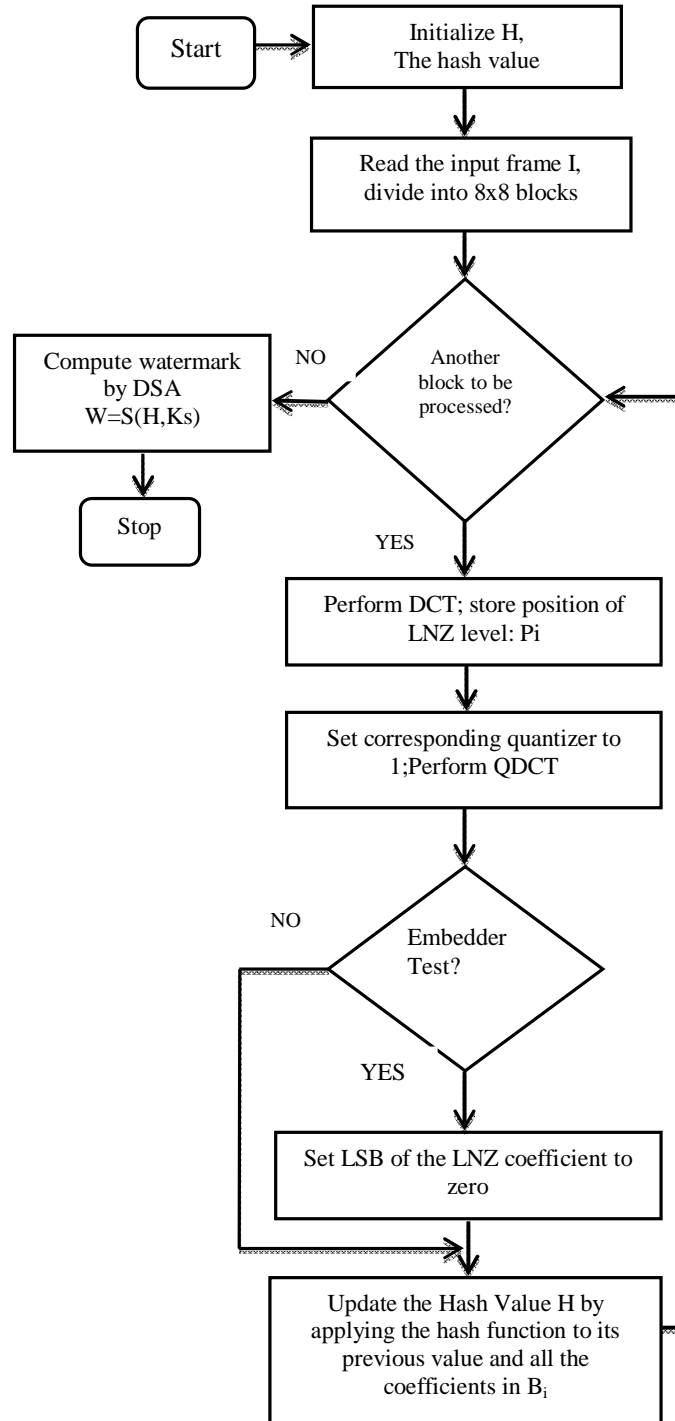


Fig. 2 Watermark Generation

## B. Watermark Embedding:

While embedding the watermark same steps are followed which used in watermark generation. The embedder test is performed to select the block for embedding. The block with all zero coefficients is not used in embedding processes. The LSB of the highest non zero DCT coefficient is replaced with corresponding watermark bit generated from hash

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

value. After embedding the first watermark the second watermark is embedded in QDCT matrix. The QDCT matrix is divided into micro-blocks of the size 16x16. Each MB is divided into 4x4 blocks so we get 16 such blocks. Out of these 16 only 7 blocks are chosen for watermark embedding and each block 4x4 must contain a single watermark bit. We cannot embed inside the block having all zero levels as this block does not contain any non-zero frequency coefficient. Embedding the block numbers and frame numbers in the video helps in tamper localization.

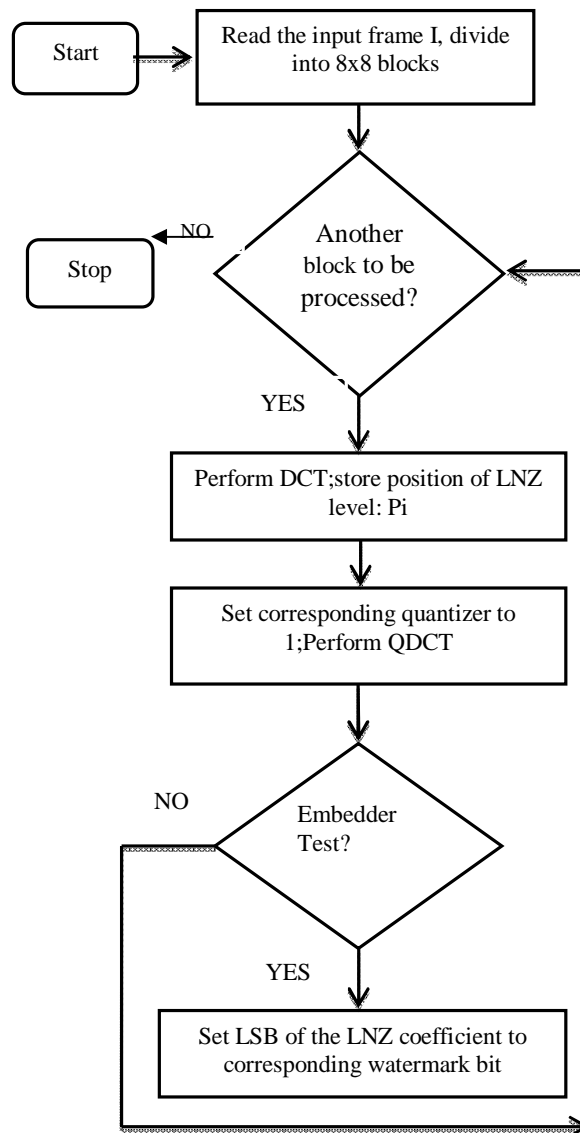


Fig. 3. Watermark Embedding.

Tampering can be of two type's intraframe and interframe tampering. The intraframe tampering refers to addition or removal of content within the frame. Interframe tampering refers to adding extra frames, dropping the frames, reordering the frame sequence, frame replacing. Temporal tampering can be done without imposing the visual distortion so there is need of tamper detection by authentication.

### C. Watermark Extraction

In watermark extraction process input frame is transformed in DCT domain. Quantization is performed at required quality as used in embedding process. Each frame is divided into the micro-blocks which further divided into the

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

blocks of size 4x4. The watermark is extracted from blocks based on the sum of the levels within block. The modified level  $L_i'$  is changed to its original value  $L_i$ .

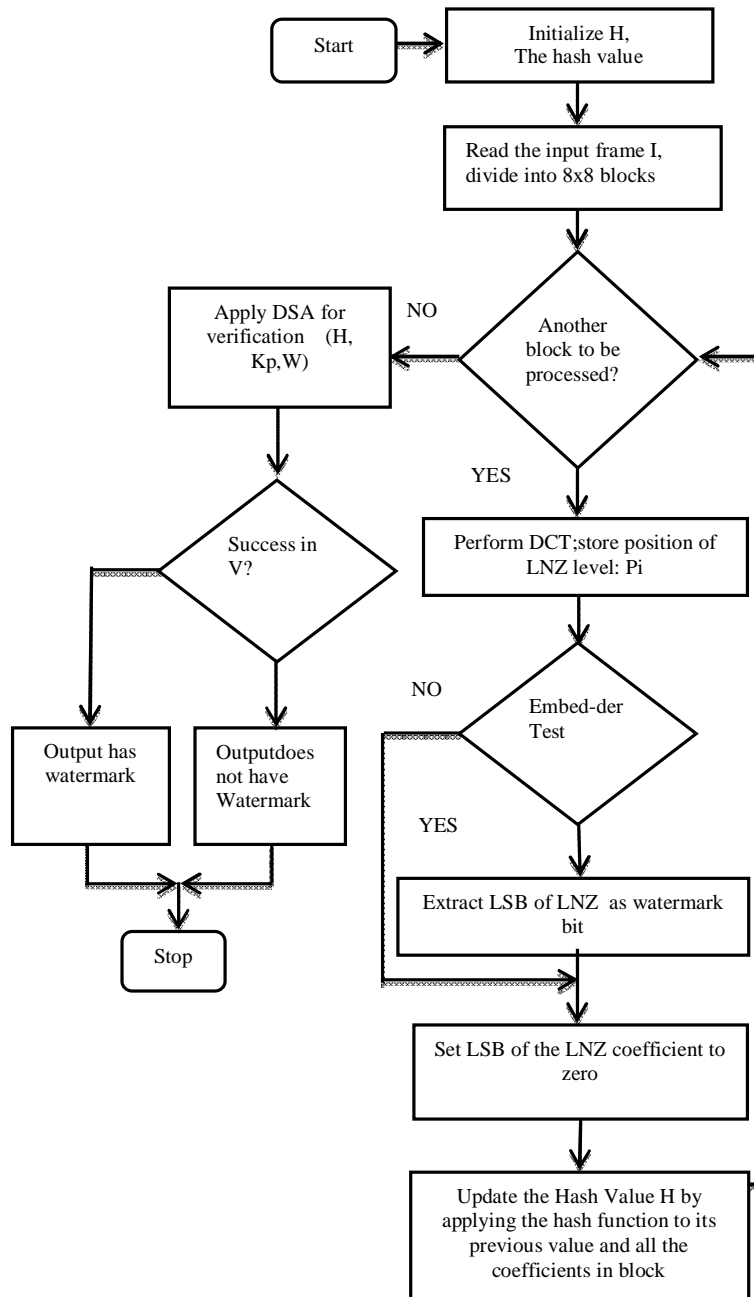


Fig. 4. Watermark Extraction

Another watermark computed from the hash value is extracted subsequently. Again the same procedure is followed as in watermark generation. Watermarked LNZ of QDCT is found by referring the stored indices of the embedded level. The LSB of the LNZ is extracted which is the watermark bit of corresponding block. The previous hash value  $H$ , is updated by applying the hash function to its previous value and all the coefficients in block. After computing the hash of the whole frame the digital signature verification algorithm  $V$ , is applied to the hash value, extracted watermark and public key  $K_p$  to verify whether or not extracted watermark same as the computed.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

## III. EXPERIMENTAL RESULTS AND CONCLUSION

Five standard video sequences we have (*Carphone*, *Foreman*, *News*, *Container*, and *Tennis*) in QCIF format are used for experimentation. The QCIF video frames are of size  $176 \times 144$ .

### A. Transparency

Transparency refers to visual perceptibility i.e. watermarked and original media should be visually equivalent. The transparency of the proposed system is measured by taking the difference between the original and watermarked frames. We have shown original, watermarked and difference frame of *Carphone* and *Foreman* video sequence for quality factor 90 in Fig. 5.

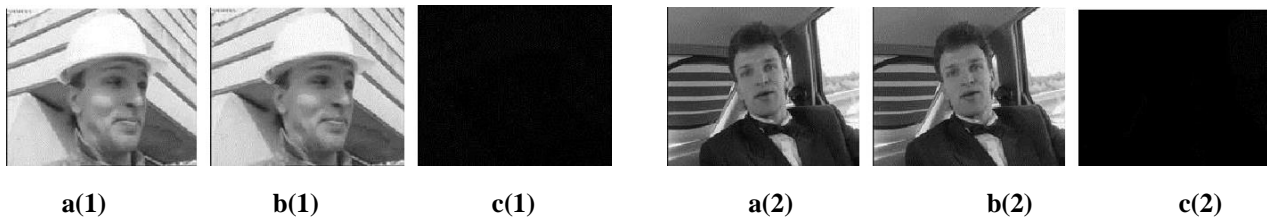


Fig. 5 Original frame, watermarked frame and their difference

It is observed from these figures that no significant visible distortion can be observed in any sequences, hence it meets the transparency requirement.

Peak Signal to Noise Ratio (PSNR), Normalized correlation (NC), and Structural Similarity Index (SSIM) are the parameters used to check the subjective quality of the original and watermarked frames, which are given in following Tables. The table I shows the average PSNR, NC and SSIM of first 100 frames of *Foreman* video sequence and their difference for different quality factors

Table I Average PSNR, SSIM and NC of 100 original and watermarked frames in **Foreman** video sequence.

Frames	Quality	SSIM	NC	PSNR (dB)	SSIM difference	NC difference	PSNR difference (dB)
Original	90	0.9993	0.9999	39.4379	0.0003	0.0001	1.1661
Watermarked		0.9990	0.9998	38.2718			
Original	60	0.9895	0.9994	28.7178	0.0120	0.0033	3.1209
Watermarked		0.9775	0.9961	25.5969			
Original	30	0.9852	0.9956	27.2852	0.0467	0.0114	5.5201
Watermarked		0.9385	0.9842	21.7651			

### B. Spatial Domain Tamper Detection





The tampering detection is shown in Table II. The first watermark is destroyed by changing the even single value of the pixel while in second watermark the block number corresponding to that pixel value is altered. Hence proposed method detects the intraframe tampering frame numbers of *Foreman* sequences.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Table II. Fragility Test by changing single pixel value

Watermarked frame	Pixel changed	Watermark 1	Changed block number in watermark 2	Tampered frame
	(1,1)	Destroyed	1	
	(35,35)	Destroyed	25	

## IV. CONCLUSION AND FUTURE WORK

The proposed fragile watermarking method meets the requirements of watermarking i.e. transparency and capacity. That is less perceptual difference between original and watermarked video. The difference of average PSNR, average SSIM and average correlation is minimum between original and watermarked image and increases with decrease in quality factor. The both the watermarks are successfully extracted from the watermarked video frame without any attacks. By changing the single pixel of the frame the first watermark gets destroyed completely as it is computed using the hash function while in second watermark which is generated from the MB number changes block number corresponding to that pixel. So the first watermark is used for checking authentication and integrity of the video sequence while the second watermark is used for tamper detection and localization. If the watermark corresponding to that particular block is not extracted correctly then the block it tampered.

The proposed method of video watermarking is not robust against compression. Compression discards the perceptually insignificant information i.e. the high frequency coefficients in frequency domain. As proposed method uses the high frequency components for watermark embedding watermark is not extracted from the compressed watermarked video. To overcome this one can choose embedding the watermark in low frequency components but it affects the visual quality of video. So the challenge is to develop the algorithm which is robust against the known method of compression by maintaining good perceptual quality.

## REFERENCES

1. Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao, "Tampering Detection in Compressed Digital Video Using Watermarking," IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 5, May 2014.
2. Bhaskaran et al., "Fragile Watermark for Detecting Tampering in images", U. S. Patent Number 6064764, may 16,2000.
3. H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," IEEE Trans Inf. Forensics Security, vol. 5, no. 4, pp. 625–637, Dec. 2010.
4. De Oliveira, P. R. ,Andreia Fondazzi Martimiano, L. ; Delisandra Feltrim, V. ; Brasilino Marcal Zanoni, G., " Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems", Latin America Transactions, IEEE (Revista IEEE America Latina) Volume:12 , Issue: 6 , Pages: 1141-1148, sept 2014.



ISSN(Online): 2320-9801  
ISSN (Print) : 2320-9798

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

5. Maneli Noorkami, and Russell M. Mersereau, "Digital Video Watermarking in P-Frames with Controlled Video Bit-Rate Increase", IEEE Transactions on Information Forensics and Security, VOL. 3, NO. 3, SEPTEMBER 2008.
6. Jordi Serra-Ruiz and David Megias, "DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," 2010 Fourth Pacific-Rim Symposium on Image and Video Technology.
7. J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Robust video watermarking of H.264/AVC," IEEE Trans. Circuits Syst., vol. 54, no. 2, pp. 205–209, Feb. 2007.
8. Y. Wang and A. Pearmain, "Blind MPEG-2 video watermarking in DCT domain robust against scaling," IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 5, October 2006.
9. Putri Ratna, A.A., Dewi Purnamasari, P., Shaugi, A., Salman, M., "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system", QiR (Quality in Research), 2013 conference, pages 99-104, June 013.
10. Riaz, S., Javed, M.Y., Anjum, M.A., "Invisible watermarking schemes in spatial and frequency domains" Emerging Technologies, 2008. ICET 2008. 4th International Conference, Pages: 211 – 216, Year: 2008.
11. Q. B. Sun, D. J. He, Z. S. Zhang, and Q. Tian, "A secure and robust approach to scalable video authentication," in Proc. Int. Conf. Multimedia Expo, vol. 2, Jul. 2003, pp. 209–212.
12. B. G. Mobasser and M. J. Sieffert, "Content authentication and tamper detection in digital video," in Proc. IEEE Int. Conf. Image Process. Vancouver, BC, Canada, 2000, pp. 458–461.

## BIOGRAPHY

**Shital Balaso Divekar** is a Student of ME Electronics and Telecommunication, D. Y. Patil School of Engg, Ambi, Pune, India also Working as Assistant professor at HSBPVT'S COE, Kashti, Ahmednagar, India.

**Prof. Nitin Dawande** is working as Assistant Professor in Electronics and Telecommunication Department at D. Y. Patil College of Engg, Ambi, Pune, India.

**Prof. Suresh Rode** is working as Assistant Professor in Electronics and Telecommunication Department at, D. Y. Patil School of Engg, Ambi, Pune, India