Survey on Classification of Different Video Watermarking Techniques

K.Swaraja
ECE, GRIET, Bachupally, Hyderabad, JNTU, India

Abstract— **The progression of Internet services and a variety of storage technologies made video piracy as a rising difficulty principally with the promulgation of media distribution through the internet. Essentially digital watermarking entails in inserting secret signs recognized as watermarks inside video data which can be utilized later for copyright recognition as well as authentication confirmation purposes. This paper basically illustrates the classification of watermarking algorithms based on the domain in which the watermark has to be inserted. These algorithms exploits the spatial, frequency and compressed domain properties and characteristics while embedding the watermark with the objective of maintaining the better Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) values along with Payload even after withstanding to numerous attacks. Major assessment entailed in watermarking approach is its design considerations, selection of apt watermarking methodology along with robustness.**

Keyword - Spatial domain, Transform domain, Imperceptibility, Robustness, Payload.

I. INTRODUCTION

Digital Watermarking is a method used to protect multimedia data that spread over the internet. Digital watermarking is a procedure of hiding a message related to a digital signals in varied types such as image, audio and video inside the signal itself. Digital watermark is a category of marker covertly inserted in a noise lenient signal such as audio, image or video data. It is generally used to recognize ownership of the copyright of such signal. "Watermarking" is the practice of concealing digital information in a carrier signal. Inserting a multimedia signal with information which cannot be detached effortlessly is called digital watermarking. The purpose is not to guard the contents from being copied or stolen, but is to offer a method to authenticate the image and guarantee the reliability of the image. Watermarking methods are reviewed on the basis of their performance on a small set of parameters. These parameters comprise robustness, transparency, payload, blind detection and security.

Mounting attractiveness of video based applications such as Internet multimedia, individual video recorders, wireless video, set-top box, video-on-demand, video phone and video conferencing have a requirement for much higher compression to congregate bandwidth criteria and finest video quality as feasible. Dissimilar video Encoder Decoders (CODECs) have progressed to convene the recent requisites of video application based products. There are numerous of algorithms in the video watermarking field while inserting the watermark. They can be divided mainly into two categories: inserting the watermark in the host video and inserting the watermark in the compressed video stream which is depicted in the figure 1.

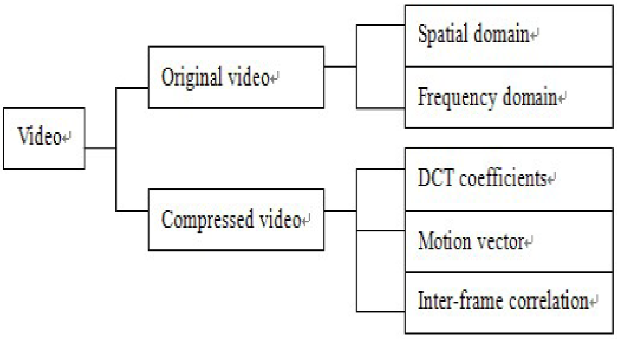

Figure 1. Categories while insertion of watermark

As shown in Figure 2, there are number of embedding strategies other than that shown in Figure 1. Video watermarking algorithms can be segregated into three types of solutions: the original uncompressed video, video codec and the compressed video stream. The watermark can be inserted at three different domains as show in the figure 2. Non-compressed domain video watermarking is utilized at Embed 1. in which Watermark is straightforwardly inserted into the original encoded video sequences [1], afterward the video including the watermark image is encoded [2]. At Embed 2 the watermark is inserted in the video encoding phase. Watermark insertion and retrieval module are established in the encoder [3-6]. Today's video compression standards comprise ISO / IEC of MPEG-1, MPEG-2, MPEG-4 and ITU-T of H.261, H.263, etc. Their basic thoughts are motion compensation prediction coding as well as block-based transforms coding. We can employ the attributes of encoded data and the standard of video data compression (such as transformation to the spatial redundancy, quantization and entropy coding, the motion compensation, motion estimation, etc). At Embed 3 watermark is openly inserted into the compressed encoded bit stream.In this paper a survey on classification of digital video Watermarking techniques is presented for enhanced performance, robustness and conversed a range of significant aspects exercised in watermarking, characteristics and application region where watermarking schemes need to be exercised.

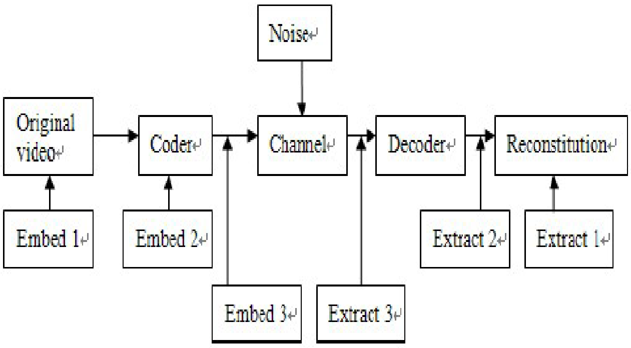

Figure 2.Different ways of embedding the watermark

This paper is organized into four sections. The next section describes the main classification of watermarking techniques especially based on the domain in which the watermark is to be inserted. Section 3 illustrates the different evaluation parameters of video watermarking schemes. The conclusion and the future work are confirmed in section 4.

II. CLASSIFICATIONS OF WATERMARKING TECHNIQUES

Watermarking techniques can be categorized as fragile, semi-fragile and robust. Lossy transformations applied on the original host signal cannot stay alive by the fragile watermarks; their role is to tamper recognition of the original signal. Imperceptibility is caused by inserting the watermark information into the perceptually trivial parts of the data. Robust watermarks are applied for the sake of copyright safety along with security applications. Thus the challenge is to offer both transparency and robustness, which are technically contradictory parameters. A robust watermark has to be inserted into the different parts of the data. Semi-fragile watermarks are supposed to be insensate to various familiar transformations like compression, but are ought to be susceptible to image transformations that change the information, such as, restoring a part of the image. From a signal processing approach the challenge in favor of semi-fragile watermarking is to present a watermark that can differentiate information varying as well as uncomplicated signal processing alterations. The techniques of watermarking are categorized as public and private. The original image is not required by the public or blind watermarking techniques to extract the watermark. Public watermarks are usually used for applications involving a robust watermark, similar to identifying the consumer to avert illegal replication and circulation. The original image is required by the private or non-blind watermarking techniques to confirm the watermark. Private watermarks are required for a few fragile watermarking applications, which involve authentication along with tamper recognition. Watermarking algorithms can be categorized as spatial-domain, transform-domain or compressed-domain based on the domain in which the watermark is embedded. These algorithms are expanded below. A summary of a huge number of watermarking algorithms in the dissimilar domains can be learned in [7,8].

A. Spatial Domain Watermarking

The watermark is inserted directly into pixels in the spatial domain watermarking schemes. Numerous spatial watermarking techniques present easy and efficient methods for inserting a watermark into an image. But they are not robust enough to regular attacks. In the spatial domain, watermarking schemes are not robust enough to attacks like noise, such as, JPEG lossy compression. But, the watermark can be recovered effortlessly despite the fact that the image is cropped or deciphered. We present here some of the methods in spatial domain. Hartung et. al [8] have given some spatial domain techniques. Tanaka et. al [9]-[10] established the notion of tagging images to conceal information and guarantee ownership privileges earliest in 1990. Next, in 1993 Caronni et. al [11] explained the unofficial image circulation. They projected marking images by means of spatial signal modulation and entitled the process as tagging. A squared tag consisted of a stable value relative to the utmost image intensity inside the square and decomposed the exterior border. An elected image region is tagged by accumulating or deducting the tag along with a random, zero mean, noise model. In the same year, Tirkel et. al accepted the significance of digital watermarking and probable applications in favor of image tagging, copyright enforcement, forged security, and restricted entry to image data [12]. In their method, the resultant m-sequence PN code is inserted as watermark in the least significant bit (LSB) plane of the image data. This method is, in fact, an addition to basic LSB coding methods wherein the LSBs are substituted by the coding information. The proposal of applying m-sequences along with LSB accumulation was extended and enhanced by the authors as a result of utilizing 2-D m-sequences, with the outcome of more robust watermarks [13]. Matsui et. al as well as Tanaka et. al projected quite a lot of watermarking algorithms [14]. Their initial scheme depending on predictive coding method was applied on gray scale images; their subsequent scheme adapts the ordered dithering method in favor of binary pictures. Moreover, in their final method the watermark is inserted within the facsimile documents. From the time when the above schemes were originated, investigations and awareness in watermarking have augmented extensively. Bender et. al projected two schemes for hiding the data [15]. In the primary method entitled, Patchwork, arbitrarily preferred pixel pairs are employed to conceal one bit, by escalating individual pixel by one and declining the further pixel by one. In the subsequent method, entitled, Texture Block Coding, the watermark is inserted by replicating one image texture block into a different region in the image through a related texture. The watermark can be extracted by computing the autocorrelation function. To raise the effort of spread-spectrum watermarking in the spatial domain, Kutter et. al projected a scheme which entirely works by means of the blue image component (in the RGB color model) to enhance the strength of watermark, while sustaining negligible visual artifacts [16]. Macq et. al initiated watermarking, customized to the human visual system (HVS) by means of masking and modulation [17]-[18]. In their method, the watermark which is a spatially restricted binary pattern, is low-pass filtered, frequency transformed, masked plus subsequently added to the host image.

B. Transform Domain Watermarking

Watermark is inserted by transforming the image into the frequency domain by utilizing Discrete Fourier transform (DFT), full-image DCT, block-wise DCT, DWT, Schur, SVD, Hadamard, Fourier-Mellin or supplementary transforms in transform domain watermarking schemes. It is frequently asserted that inserting the watermark in the transform domain is beneficial with regard to perceptibility as well as safety. Designing watermarking techniques in the transform domain is complicated compared with designing spatial domain watermarking techniques. Yet, there are various block DCT-domain techniques, as this transform is applied by several compression standards which include JPEG, MPEG2, H.263, etc. Well-organized watermarking in the DCT domain was initially established by Koch et. al [19]-[21]. In the JPEG coding method, the image is primarily alienated into square blocks of 8×8 size. Afterwards the DCT is calculated for these square blocks. Amongst the pseudo randomly preferred blocks, a couple of mid-frequency coefficients are chosen from among 12 prearranged pairs. To insert a bit, the coefficients are next adapted depending on the bit value such that the variation among them is either positive or negative. Podilchuk et. al [22]-[23] established perceptual watermarking exploiting the noticeable difference (JND) to ascertain an image-reliant watermark modulation mask. The watermark is inserted into preferred coefficients in both the DCT and wavelet transform domain. In support of DCT coefficients, the perceptual model delineated by Watson et. al exploited frequency and intensity sensitivity in addition to the local contrast masking. This method presents an image-reliant masking thresholds for all the DCT blocks of size 8 × 8. Boland et. al [24] initiated the frequency-domain watermarking for the first time and Cox et. al [25], expanded perceptually adaptive techniques based on modulation. Cox et. al sketched correspondence among their technique and spread-spectrum communication, as the watermark is stretched over a group of visually significant frequency components. Ruanaidh et. al projected watermarking in the frequency domain [26] through the amendment of the phase. The phase of a preferred coefficient of an N1×N2, DFT is adopted to insert a bit by adding a small 'δ'. A discrepancy of their scheme based on the Radon transform was projected by Wu et. al [27]. For methods functioning in other transform domains, the watermark is typically specified by a pseudo-random 2-D model. 2-D wavelet transform decomposes the image and the watermark. A weighted version of the watermark is also added to all sub-bands of the image. As usual the decoding of watermark is based on the NC, connecting the approximate of the inserted watermark and the watermark itself. The dissimilarity among the schemes stretches out in the manner the watermark is weighted consecutively to lessen visual artifacts.

C. Compressed-Domain Video Watermarking

From the time the video signals are stored and disseminated in the compressed format, it is unfeasible initially to decipher the video sequence, insert the watermark, and subsequently re-program it. Consequently, designing low-complexity video watermarking technique to insert the watermark in the compressed domain, is appealing. The most of the earlier work in compressed-domain video watermarking showed interest in inserting the watermark into the MPEG2 bit stream. In the MPEG2 standard, the residual blocks are coded first by the DCT transform, then quantized and reorganized, followed by run-level coding in addition to the variable length coding. Langelaar et. al projected two real-time watermarking schemes [28]. Either of the methods inserted the watermark instantly into the MPEG compressed bit stream. The initial method inserted the watermark by varying the variable length codes (VLCs). By choosing appropriate VLCs and compelling their least significant bits (LSB), the watermark is inserted to match the subsequent watermark bits. The next scheme eliminated a few of the high-frequency DCT coefficients of the bit stream to insert the watermark. Wolfgang et. al [29] proposed an image adaptive DCT-based (IA-DCT) method that employed the visual model depicted in [30]. This method comprises an image-independent part related to frequency sensitivity as well as an image-dependent part related to luminance sensitivity, along with contrast masking. IA-DCT techniques have been developed to video by them. Employing the IA-DCT watermarking technique to all the I-frames and relating the linear interpolation of the watermarks to the frames among two successive I-frames made it possible to acquire the preeminent visual quality. Only some of the newly- published papers have concerted on inserting a watermark in the sequence of H.264 bit-stream. Qiu et. al proposed a hybrid watermarking scheme that inserted in the DCT domain a robust watermark. A fragile watermark was also inserted in the motion vectors [31]. Their method inserts the watermark inside the compressed H.264 video; however, it is not robust against familiar watermarking attacks. Wu et. al proposed a private watermarking technique of inserting the watermark in I-frames of H.264 [32] that tolerates H.264 compression attacks in I-frames.

III.EVALUATION PARAMETERS AND REQUIREMENTS OF WATERMARKING

The performance criteria for watermarking in any case must comprise perceptual transparency, robustness, capacity, and security. The entire simulation results are evaluated by finding the Imperceptibility, Robustness and Data payload.

A. Imperceptibility

Imperceptibility is a quality of the watermarked video. It must not change even after inserting the watermark into the image, video or text, and the watermark ought to be perceptually indiscernible. The visual quality of the watermarked video is estimated by the PSNR (peak signal-to-noise ratio). PSNR is a commonly used objective perceptual quality measure. The discrepancy of the watermarked and attacked frames from the original video frames, is determined by calculating the PSNR and is delineated by Eq (1).

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (1)$$

To evaluate the PSNR, the earliest Mean Square Error (MSE) between the original and watermarked frame is computed, as MSE is the mean square error connecting the original video and the watermarked video which is given by Eq (2).

$$MSE = \frac{1}{R\times C}\sum_{i}^{R}\sum_{j}^{C}[V(\mathrm{i,j}) - \mathrm{V'(i,j)}]^2 \qquad (2)$$

At this moment, the notations R and C correspond to the width and height of a frame, V(i, j) is the pixel value of coordinate (i, j) in original video, and V'(i, j) is the pixel value of the watermarked video. Thus the invisibility is measured by calculating the average mean square error (MSE) and the average PSNR. The higher the PSNR, the better is the quality of the video. In general, for digital images, noise with PSNR is higher than 30 dB which is hardly noticeable.

B. Robustness

It is the capability of a detector to extort the unseen watermark from some distorted watermarked data. It is frequently assessed through the endurance of a watermark after attacks, such as, compression, re-sampling, cropping, geometric distortions, frame swapping, frame dropping, frame averaging and scaling. Robustness is the resistivity of the watermark in opposition to common signal processing and malicious attacks. It is supposed to be skilled in extorting the watermark from the watermarked video. Even if the algorithmic principle of the watermarking method is public, the watermark should not be viable to be taken away. In particular, the watermark must be robust to the following:

Common signal processing: The watermark should be retrievable although common signal processing operations (such as, analog-to-digital conversion and digital-to-analog, re-sampling, re-compression and common signal enhancements to image contrast and color) are affected on the video sequence.

Common geometric distortions: The watermark should be resistant to geometric image operations, such as, cropping, rotation and scaling.

Subterfuge attacks: Collusion and Forgery: The watermark should be robust to collusion by several individuals even though all hold a differently watermarked copy of the identical content merging their copies to demolish the watermark. Likewise, it should be unfeasible to merge the copies to generate a latest valid watermark.

For comparing the similarities between the original and extracted watermarks, the two-dimensional normalized correlation (NC) value was employed. The NC value can be between '0' and '1'. In principle, if the NC value is closer to '1', the extracted watermark is getting more similar to the embedded one. In order to evaluate the performance of watermarking algorithm objectively, NC (normalized correlation) function is evaluated and computed by using Eq. (3)

$$NC(V,V') = \frac{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j).V'(i,j)]}{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j)]^{2}} \qquad (3)$$

Where, V' is the extracted watermark and V is the original watermark. V(i,j) represents original watermark image and $V^{'}(i,j)$ represents the extracted watermark image.

C. Payload

It is the quantity of information which is interleaved into original video (i.e. mark size). We delineate the watermark cost 'δ' as the augment in number of bits utilized to encode the watermarked video for every watermark bit and is given by Eq (4). Where $TB_{original}$ is the number of bits utilized to code the original video sequence, $TB_{watermarked}$ is the number of bits exploited to code the watermarked video sequence and $N_w(f)$ is the overall number of watermarked coefficients in that video sequence.

$$\delta = \frac{TB_{watermarked} - TB_{original}}{\sum_{f=1}^{L_f} N_w(f)} \qquad (4)$$

IV. CONCLUSION & FUTURE SCOPE

As the volume of literature available in the field is vast, the focus is on review of Classification techniques for video watermarking and also regarding the requirements of the evaluation parameters. The entire simulation results are to be evaluated by finding the Imperceptibility, Robustness and Data payload. The robustness is measured through NC by evaluating against attacks, such as, frame dropping, frame averaging, frame swapping, compression, add noise and statistical analysis. The imperceptibility is measured by evaluating the PSNR. Thus in future embedding the watermark in compressed domain as well as exploiting the hybridization of different transforms along with the optimization techniques, can further improve the efficiency of results in terms of PSNR, NC and payload.

REFERENCES

[1] Hui Zhou, Tao Xu, Xiaochuan Wu. Resist the collusion attack of a digital video watermarking algorithm. Computer Applications 2006; 26 (04):812-814.

[2] Hefei Ling, Zhengding Lu, Fuhao Zou. New real-time watermarking algorithm for compressed video in VLC domain. International Conference on Image Processing 2004; 24: 2171–2174.

[3] Hua Cao, Jing-li Zhou, Sheng-sheng Yu, Shuguang Su. Based on H.264 Low bit rate video stream 264 semi-fragile watermarking algorithms. Electronics 2006; 34 (01):40-44.

[4] Desheng Fu, Jianrong Wang. Based on H. 264 of the video watermarking technology. Computer Applications 2009; 29 (04):1174-1176.

[5] Lihe Zhang, Hongtao Wu, Changli Hu. A Gabor transform based video watermarking algorithm . Software 2004; 15 (08):1252-1258.

[6] Yafei Shao, Guowei Wu, Li Zhang, Xinggang Lin. Digital Video Broadcasting in the compressed domain watermarking algorithm. Electronics 2003; 31 (10):1562 -1565.

[7] Frank Hartung, Jonathan K. Su and Bernd Girod: Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. Security and Watermarking of Multimedia Contents, 1999.

[8] Hartung, F. and Kutter, M., "Multimedia watermarking techniques", Proceedings of the IEEE, vol. 87, pp. 1079–1107, July 1999.

[9] Tanaka, K., Nakamura, Y., and Matsui, K., "Embedding secret information into a dithered multi-level image", in Proceedings of IEEE Military Communications Conference, vol. 1, (Monterey, CA, USA), pp. 216–220, 1990.

[10] Tanaka, K., Nakamura, Y., and Matsui, K., "Embedding the attribute information into a dithered image", in Systems and Computers in Japan, vol. 21,pp. 43–50, 1990.

[11] Caronni, G., "Assuring ownership rights for digital images", in Proceedings of Reliable IT Systems (VIS), (Germany), 1995.

[12] Tirkel, A. Z., Rankin, G. A., van Schyndel, R. M., Ho, W. J., Mee, N. R. A., and Osborne, C. F., "Electronic watermark", in Conference Proceedings of Digital Image Computing: Techniques and Applications (DICTA), vol. 2, (Sydney, NSW, Australia), pp. 666–673, December 1993.

[13] Tirkel, A. Z., van Schyndel, R. G., and Osborne, C. F., "A two dimensional digital watermark", in Conference Proceedings Digital Image Computing: Techniques and Applications (DICTA), (Brisbane, Qld., Australia), pp. 378–383, December 1995.

[14] Matsui, K. and Tanaka, K., "Video-steganography", Journal of the Interactive Multimedia Association Intellectual Property Project, vol. 1, no. 1, pp. 187– 205, 1994.

[15] Bender, W., Gruhl, D., and Morimoto, N., "Techniques for data hiding", in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 2420, (San Jose, CA, USA), pp. 164–173, February 1995.

[16] Kutter, M., Jordan, F., and Bossen, F., "Digital signature of color images using amplitude modulation", in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 3022, (San Jose, CA, USA), pp. 518–526, February 1997.

[17] Delaigle, J.F., Vleeschouwer, C. D., Goffin, F., Macq, B., and Quisquater, J.J., "Low cost watermarking based on a human visual model", in Multimedia Applications, Services and Techniques- ECMAST'97. Second European Conference Proceedings, (Milan, Italy), pp. 153–167, May 1997.

[18] Delaigle, J.F., Vleeschouwer, C. D., and Macq, B., "Digital watermarking", in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 2659, (San Jose, CA, USA), pp. 99–110, February 1996.

[19] Burgett, S., Koch, E., and Zhao, J., "Copyright labeling of digitized image data", IEEE Communications Magazine, vol. 36, pp. 94–100, March 1998.

[20] Koch, E., Rindfrey, J., and Zhao, J., "Copyright protection for multimedia data", in Proceedings of the International Conference on Digital Media and Electronic Publishing, (Leeds, UK), May 1994.

[21] Koch, E., Rindfrey, J., and Zhao, J., "Towards robust and hidden image copyright labeling," in Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing, pp. 452–455, 1995.

[22] Podilchuk, C. I. and Zeng, W., "Perceptual watermarking of still images", in Proceedings of Signal Processing Society Workshop on Multimedia Signal Processing, pp. 363–368, 1997.

[23] Podilchuk, C. I. and Zeng, W., "Digital image watermarking using visual models", in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 3016, (San Jose, CA, USA), pp. 100–111, February 1997.

[24] Boland, F. M., O'Ruanaidh, J. J. K., and Dautzenberg, C., "Watermarking digital images for copyright protection", in Proceedings of International Conference on Image Processing and its Applications, vol. 410, (Edinburgh, UK), pp. 326–330, July 1995.

[25] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T., "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, pp. 1673–1687, December 1997.

[26] O.Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M., "Phase watermarking of digital images", in Proceedings of IEEE International Conference on Image Processing (ICIP), vol. 3, (Lausanne, Switzerland), pp. 239–242, September 1996.

[27] Wu, M., Miller, M. L., Bloom, J. A., and Cox, I. J., "A rotation, scale and translation resilient public watermark," in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), vol. 4, (Phoenix, AZ, USA), pp. 2065, March 1999.

[28] Langelaar, G. C., Lagendijk, R. L., and Biemond, J., "Real-time labeling of MPEG2 compressed video," Journal of Visual Communication and Image Representation, vol. 9, pp. 256–270, December 1998.

[29] Wolfgang, R. B., Podilchuk, C. I., and Delp, E. J., "Perceptual watermarks for digital images and video," in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 3567, (San Jose, CA, USA), pp. 40–51, January 1999.

[30] Watson, A. B., "DCT quantization matrices visually optimized for individual images," in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 1913, (San Jose, CA, USA), pp. 202–216, February 1993.

[31] Qiu, G., Marziliano, P., Ho, A. T. S., He, D., and Sun, Q., "A hybrid watermarking scheme for H.264/AVC video," in Proceedings of the 17th International Conference on Pattern Recognition, vol. 4, (Cambridge, UK), pp. 865–868, August 2004.

[32] Wu, G.-Z., Wang, Y.-J., and Hsu, W.-H., "Robust watermark embedding/ detection algorithm for H.264," Journal of Electronic Imaging, vol. 14, pp. 13013–1–9, January 2005.

AUTHOR PROFILE

Dr. K. Swaraja is currently working as Professor at Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telengana, India and has obtained her Ph.D. in the area of Digital Image Processing from the auspices JNTU, Hyderabad, Telengana, India. She received M. Tech degree in Digital Electronics & Communication systems from the prestigious JNTU, Anantapur, A.P, India and B.Tech degree from JNTU, Anantapur, AP, India in Electronics and Communication Engineering. She has more than 25 publications on an assortment of topics in reputed national & international journals and conferences. Her areas of interest are digital image processing and Communication systems.