International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 10, 2020
ISSN: 1475-7192

Video Watermarking Techniques-Classifications And Applications

[1]Swaraja.K, [2]Meenakshi.K, [3]Padmavathi.K, [4]Ch.Ushakumari, [5]G.Karuna

Abstract--- *Digital watermarking is a scheme that involves in concealing the information within the signal which is translucent to the user. Video Watermarking is one among the inspiring fields to ensure the improvement of the system by facilitating the authentication of data, advertisement surveillance, safety, tracing of piracy and copyright protection procedures for digital media, concealed within dynamic video codec. Digital watermarking technology is being adopted to ensure and facilitate data authentication, safety and copyright protection of digital media. It is contemplated as the most significant technology in the modernized world, to avert illegal replication of data. Digital watermarking can be practiced on multimedia data. In this work, we emphasized particularly on the overview of different domains in video watermarking schemes, along with its definitions, properties, applications and evaluation constraints utilized to expand the security of data.*

Keywords--- *Imperceptibility, Payload, Robustness, Compressed domain, Frequency domain.*

I INTRODUCTION

The evolution of the Internet and the augmentation of the digital multimedia technology have not only permitted the people to practice, dispense and accumulate digital content effortlessly, but also have endowed the ability of replicating it swiftly and absolutely without loss of quality, with no restriction on the number of copies, avoiding and hacking without authorization. Service providers are unwilling to extend services in digital form, even though digital data comprise various advantages in contrast to analog data, as they panic unimpeded replication and spreading of copyrighted material. The intellectual property ought to be guarded [1]-[2]. The consequences of illegal replication on a huge scale made the content creators and owners more anxious. This issue is not just theoretical. The financial damage due to illicit replication of copyrighted materials [3] runs into billions of dollars. Hence, there is an enormous requirement for the methods which can safeguard the financial value of digital video, image as well as medical image [4],and preserve the rights of content owners.

Illicit duplication, circulation and amendment of digitized works are infringe upon intellectual property rights. Hence authenticity and integrity with regard to digital video has become an important research area nowadays. Thus digital watermarking has come into existence for copyright protection, ownership and authentication to avert illegal copying. In addition, other methods that can ensure security to the digital content are cryptography and Steganography. Steganography and watermarking mutually appear under data-hiding techniques, i.e., they are used to hide covert information within the cover. Yet, there is a difference between Steganography and watermarking. Steganography masks the existence of covert information. Steganography arrests the continued existence of covert information while in watermarking the use of covert information can be identified. Thus watermarking makes the

1,2,3,4,5, Professor, ECEGRIET, Hyderabad

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

covert information unfeasible. Digital watermark is normally used to spot the ownership or verify the authenticity of any digital data or multimedia. As the digital copy of data is identical to the original, the digital watermarking is a security means and marks the data, but does not control the right to use it.

Earlier digital video watermarking procedures utilizing frequency domain approaches were explored, but nowadays the focus is laid on concealing the watermark in compressed format along with hybrid domain through certain amendments. The compressed and hybrid video watermarking were drawing much concentration from the period when video signals were stored and conveyed in format of packed. As the digital video carries a large quantity of details, in real period it is tough to hide the watermark into raw video.

The rest of the paper is setin the following manner.Section 2 describes the fundamentals of video and video formats. Section 3illustrates the overview of video watermarking.Section 4 specifies different video watermarking approaches.Eventually Section 5 determines evaluation constraints and requisites of watermarking methods. Section 6 describes dissimilar applications of video watermarking. Section 7 concludes this proposal.

II FUNDAMENTALS OF VIDEO

II.I. Digital Images and Video

An image I (x, y) is a signal which corresponds to the amount of light emanated to a spectator at the entire spatial coordinates (x, y). An analog image is a signal with continuous values, obtaining a real value at each coordinate. A digital image maintains values simply at discrete coordinates, recognized as pixels. A digital image is attained in two steps from an analog image: initially the analog image is sampled to appear as a discrete-signal; next, consequent to sampling, each and every sampled value is quantized to a particular value amongst countable group of values. All pixel values of several images are indicated by 8 bits which allocate up to 256 discrete intensity levels. Digital video [5]-[6] is viewed as a prearranged series of digital images to facilitate the display in sequence, in addition to the subsequent audio and synchronization signals. All images of the video are recognized as a frame. Frame rate is the number of displayed frames for each unit time. Each frame is signified as two detached fields in several videos that are put on show in an interlaced or interleaved manner. Analog television makes use of the fields more intently, analogous to the interlaced scanning. In the course of presentation of the video, the synchronization signal is utilized to persist reliability, assuring that the visual and audio signals are put on view simultaneously at the accurate time.

II.II. Analog Video

A video signal can be delineated as a series of two-dimensional (2-D) images, projected from a threedimensional (3-D) object against the image surface of a video camera. The signal of analog video with continuous space and amplitude. Usually video is captured frame-by-frame by an analog camera. It also attains a frame by scanning successive lines through assured line spacing. These scanned lines in all frames are renewed into an electrical signal corresponding to the analog video signal.

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

II.III. Digital Video

Through sampling and quantization, or by employing a digital video camera directly, a digital video can be attained from an analog video signal. The imaged scene is sampled by a digital video camera as discrete frames. Every frame is composed of a few lines and every line is sampled to build a numeral of pixels (samples) for each line. A pixel is provided as a rectangular region through constant color. The intensity of each pixel is indicated by 8 bits (monochrome video) or 24 bits (color video). The data rate and the resolution of a digital video are determined as follows:

Data rate = (number of frames/second) × (number of lines/frame) × (number of pixels/line) × (number of bits/pixel).

Resolution = (number of pixels/line) × (number of lines/frame)

II.IV. Color Spaces

The emitted or reflected light at a specific 3-D point is recorded by the color value at every part of a video frame in the observed scene. The intensity or luminance of all pixels of a monochrome video frame is specified by just a single number; but, color video frames need atleast three numbers to indicate a color value at all pixels correctly. The coordinate system that corresponds to color is signified as color space. The color value at all pixels in the RGB color space, is denoted by three foremost colors of light, Red (R), Green (G) and Blue (B)). The unlikely colors can be formed by integrating red, green and blue in proper proportions. The RGB color space is a familiar method in favor of monitor displays. The HVS does not recognize certain pictures exclusively. Consequently, a color is expressed in terms of its luminance and chrominance autonomously to make feasible more competent processing along with broadcasting of color signals. A variety of 3-component color spaces are presently available. Of these, one component corresponds to the luminance and the other two, jointly stand for hue and saturation. Y: Cr: Cb color space is admired amongst them. It is usually brought into play to specify a digital video. The YCrCb color space is the scaled and altered version of the analog YUV color space. The luminance component 'Y' is designed as a weighted average of the 3 color components R, G and B. The chrominance or color difference (Cr and Cb) components indicate the variation among the color intensity and the luminance component. Cr point to red chrominance component (Cr = R - Y) as well as Cb point to blue chrominance component (Cb = B - Y).

II.V. YCrCb Sampling Formats

When compared to RGB an imperative benefit of the YCrCb color space is that the Cr and Cb components possibly will be denoted through an inferior resolution than that of Y component since the Human Visual System (HVS) is not as much of sensitive to color than luminance. This lessens the quantity of data essential to signify the chrominance components lacking a foremost outcome on visual quality. There are a mixture of YCrCb formats, wherein the chrominance components are sub-sampled with unusual sub-sampling factors. Fig.1 illustrates three YCrCb formats that are sustained by H.264/AVC.

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

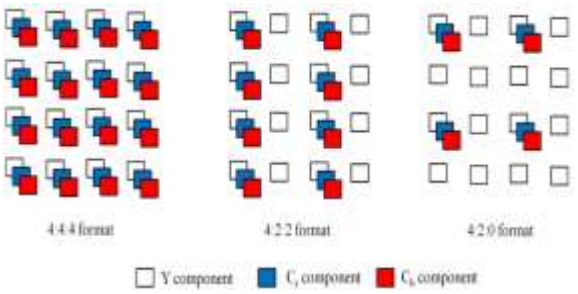

Fig.1. Sub-sampling patterns for chrominance components.

The video applications to facilitate extremely high resolutions employ 4:4:4 format. In this format, the chrominance components are sampled in precisely the equivalent resolution as the luminance components. Explicitly, every pixel location has mutually chrominance and luminance samples at full resolution. To lessen the essential data rate, BT.601 delineated 4:2:2 format, wherein the chrominance components are sub-sampled beside every line by a factor of 2, implying that there are 2 Cb samples and 2 Cr samples for every 4 Y samples. To further lessen the essential data rate, BT.601 also identifies an additional format, which subsamples the Cr and Cb components by half mutually in the vertical and horizontal directions. This is recognized as the 4:2:0 format and is exercised in video circulation, such as, movies on Digital Versatile Disc (DVD) and Video-OnDemand (VOD). The 4:2:0 format, encloses 1 Cb sample and 1 Cr sample for every 4 Y samples. 2.6 Video Formats The Common Intermediate Format (CIF), given by the International Telecommunications Union Telecommunications sector (ITU-T), has the luminance resolution of 352 × 288. This design was extended in favor of video conferencing applications. The quarter CIF (QCIF), with half the resolution of CIF in mutually vertical as well as horizontal dimensions, is employed for mobile multimedia applications. The Source Intermediate Format (SIF) is extended for video applications entailing standard quality, such as, CD movies and video games. This format is regarded the same as CIF i.e. (352 × 288/240). There are two SIF formats: one, with the luminance resolution of 352 × 288 plus a frame rate of 25Hz, and the other, with a luminance resolution of 352 × 240 plus a frame rate of 30Hz. The Society of Motion Pictures and Television Engineers (SMPTE) has identified quite a few High Definition (HD) formats which entail huge uncompressed data. 720p HD video format has the luminance resolution of 1280 × 720. Further, 1080p HD has the luminance resolution of 1920 × 1080. Hardly any standard (pixel) dimensions on behalf of digital video frames are described in Table 1.

Table 1. General dimensions of digital video frames

Name	Luminance Pixels per Line	Luminance Number of Lines
Sub-QCIF	128	96
QCIF	176	144
CIF*	352	288
4CIF	704	576
16CIF	1408	1152
CCIR601 [145]	720	480
SMPTE 274M [146]	1920	1080
SMPTE 296M [147]	1280	720

*Common Intermediate Format

Data rate of the video is a challenge for storing or processing a digital video. An uncompressed 4:2:2 YCBCR CCIR601 video delineated by means of 8 bits/pixel and 30 frames/s, has a data rate of: [(720 Y pixels/line) × (480 Y lines/frame) +(360 CB pixels/line) × (480 CB lines/frame) +(360 CR pixels/line) × (480 CR lines/frame)]× (30 frames/s) × (8 bits/pixel) = (691 200 pixels/frame) × (30 frames/s) × (8 bits/pixel) = 165 888 000 bits/s = 20 736 000 bytes/s ≈ 70 Gbytes/hour An eminent compact disc (with more or less 650 Mbytes of storage) probably will accumulate very soon in 30 seconds of this video regardless of the detail that a DVD (with almost 17 Gbytes capacity) can save in about 15 minutes. The data rate of nearly 160 Mbits per second goes beyond the capacity in support of a range of low cost, local-area networks, such as, 10 Mbits/s or 100 Mbits/s Ethernet. Evidently dealing with uncompressed video is either expensive or unrealistic. The inspiration of digital video compression is on account of the prerequisite for meting out uncompressed video at high data rates.

III WATERMARKING OVERVIEW

III.I. Phases in Digital Watermarking

Digital watermarking has been presented as a key to the problem of copyright protection of multimedia data in the next generation networks [7]. Essentially, nowadays with a broad range of video applications, Multimedia transmissions over wireless channels and the Internet requires that multimedia resources must be protected. Thus, video coding integrated with digital watermarking techniques can be efficiently employed to achieve this goal. However, digital video watermarking has many aspects that must be considered during the design of any digital video watermark schemes such as imperceptibility, robustness, capacity, complexity, synchronization, bit-rate control and error drift [8] [9] [10] [11]. A watermarking system consists of two main components: a watermark embedding unit and a watermark extracting unit as shown in Figure 2 The embedding unit adds the watermark component to the host data. The output of the embedding unit is the watermarked data. Attackers intend to do one of the following illegal actions such as modifying, copying, destroying or removing the watermark from the host data.

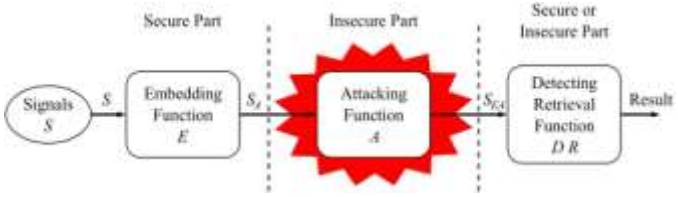

Fig.2 Digital watermarking life cycle phases

After embedding watermark, the watermarked media are sent over Internet or some other transmission channels. Whenever the copyright of the digital media is under question, the embedded information is decoded to identify copyright owner. The decoding process can extract the watermark from the watermarked media (watermark extraction) or can detect the existence of watermark in it (watermark detection). The embedding or encoding process can be viewed as a function or mapping that maps the input X (original media), W (watermark) and/or K (key) to output X ″ (watermarked media). Mathematically it can be expressed as

$$X' = E(X,W,[K]) \quad (1)$$

where E(·) denotes the embedding process and [·] represents optional argument. Similarly the decoding or extraction process D(·) can be expressed formally as

$$W' = D(X'',[X],[K]) \quad (2)$$

and the detection process d(·) can be expressed as

$$\{\text{Yes or No}\} = d(X'',[X],W,[K]) \quad (3)$$

III.II. Watermark Theory

The watermark contains information of the origin, ownership, destination, copy control and transaction. A watermark is inserted into a cover content like a digital code into a video sequence. A watermark can hold any information but the quantity of information is restricted. The information gets affected if the watermark holds more information. Moreover, the capacity of watermark is limited by the size of a particular video sequence. There are primarily three assessment constraints in video watermarking and at the same time there is an intricate trade-off among these constraints which are imperceptibility, robustness and payload. Simultaneously, security (authoritative persons only can spot the watermark) and complexity (number of computations incorporated while embedding and extracting the watermark) are the two requirements for the efficient and robust watermarking techniques.

Besides the essential obligations, a watermarking technique to succeed as a real-time method, ought to gather the following additional requisites for compressed image and video data valid to recording device:

Oblivious: Even after lacking the original unwatermarked data, it must be viable to extort the watermark information, as a recorder and a set-top box at their disposal lack the original data.

Low complexity: The watermarking techniques cannot be too intricate since they are to be practiced in real time and also utilized in customer products, so they have to be economical. This means that entirely decompressing the data, inserting a watermark and compressing the data, do not constitute a choice for inserting a watermark.

Preserve host data size: The dimension of the compressed host data must not be augmented with the watermark. Sending the data over a preset bit-rate channel can create problems like the one in hardware decoders where the buffers rush out of space; otherwise there will be a problem in the synchronization of audio and video incase the dimension of a compressed MPEG-video stream enhances. Security systems that exploit watermarking methods have in common a sequence of cryptographic methods. Primarily the watermark information has to be encrypted.

Consequently, the processed watermark information is appended to the host data in the course of inserting methods. The encryption and inserting methods exercise keys; these keys may differ in time. Cryptography protocols have to look after the key-management intricacy. The center of attention is on extending, analyzing and verifying the inserting methods for watermarks.

III.III. Oblivious vs. non-oblivious watermarking

In non-oblivious watermarking (private, non-blind), watermark extraction algorithms can utilize the original unwatermarked data to place the watermark in a few applications like copyright protection and data monitoring, whereas the blind techniques can extort a watermark without any reference to the original content. The detection is in general made complicated and the data capacity is also limited by the blind watermarking scheme. A huge database of original content is required by the non-blind watermark extraction though it is more robust, representing the technique which is impracticable for several applications. In the majority of applications like copyprotection and indexing, the watermark extraction algorithms have no contact with the original unwatermarked data, which make the watermark extraction more intricate. Watermarking algorithms of this kind are known as public, blind or oblivious. By making amendments for every bit of the watermark to the host data, a robust watermark can be accomplished. In spite of large scale amendments in the host data and a lot of variations for each watermark bit, a maximum quantity of watermark bits can be stored in a data object. Consequently, a trade-off is supposed to be established concerning the diverse requirements, with the intention that a pre-eminent watermark can be developed for each application. The mutual dependence among the essential prerequisites is revealed in Fig.3.The security of a watermark ensures its robustness, but the watermark cannot be robust if it is not protected.

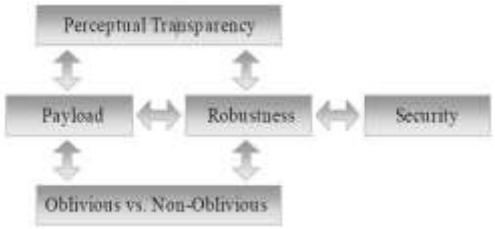

Fig. 3. Mutual dependence among the basic necessities.

III.IV. Watermark Attacks

This section offers a study of possible attacks on watermarks. Watermark attacks can be organized into four major groups [12]:

Simple attacks are theoretically simple. They endeavor to destroy the inserted watermark by amendments to the entire image without any attempt to identify and segregate the watermark. Examples comprisefrequency reliant compression, noise addition, cropping and adjustment. **Detection-disabling attacks** strive to shatter correlation and to make identification of the watermark unattainable. Typically, they make a few geometric alterations akin to zooming, transfer in spatial or temporal direction, rotation, cropping or pixel transformation, deletion or inclusion. The watermark in the cover content can be retrieved with enhanced intelligence by the watermark detector.

Ambiguity attacks try to confound the detector by generating forged watermarked data to lessen the influence of the watermark by inserting numerous extra watermarks so that it becomes obscure.

Removal attacks assess or guess the watermark from a number of unusual watermarked copies, detach it and dispose of the watermark. Collusion attack, denoising and utilizing theoretical cryptographic fault of the watermark method are a few examples. A few attacks do not obviously fit into a solitary group.

III.V. Classifications of Watermarking Techniques

In the process of embedding the watermark, video watermarking schemes are segregated into three major groups such as spatial domain, frequency domain and compressed domain. Dissimilar methods are applied in each domain. In this sector, a concise analysis is elucidated with the present video watermarking schemes based on the domain in which watermarking is carried out.

III.VI. Spatial domain watermarking

The schemes employed while inserting the watermark in the spatial domain involves in amending the pixel locations or pixel values of the original video or the watermark bits to be inserted are normally added to the luminance part or to the color components without exploiting the mathematical transforms on the original content. The watermarks are generally encoded as a noise-like progression and then appended to the original content, whereas with a correlationbased receiver the extraction is typically achieved. As mathematical transforms are not entailed, these schemes are reasonably efficient in terms of computations entailed. In real-time applications this is benefited where accessible of resources is narrow for inserting the watermark. Thus the chief benefits achieved with this scheme are the low time complexity in addition to simplicity of execution. Conversely, these schemes provide several difficulties in meeting robustness and imperceptibility constraints [13]. Countless methods have been anticipated for extending watermark schemes in the spatial domain, some of them are the Least Significant Bit (LSB) and Spread Spectrum Signal Correlation (SSSC) schemes, etc. In the LSB method, the original frame is utilized to insert the watermark. The places of the pixels are customized based on a secret key by engendering a pseudo-random number. Another scheme termed as SSSC involves in adding a pattern of noise which is pseudo-random towards the luminance value frames in the spatial domain, besides the likeness amongst the pattern of noise and probably watermarked video for each frame is also calculated. When the likeness surpasses a particular threshold then, the watermark is noticed [14].

III.VII. Frequency domain watermarking

To surmount the major drawbacks in the spatial domain most of the video watermarking schemes have been utilized in the domain of frequency transform. Moreover, to augment watermark robustness and imperceptibility in the frequency domain, analysis of the bands is a prerequisite. Conversely, these schemes have a few shortcomings in terms of complexity. While switching from the spatial to a frequency domain numerous of transforms are entailed. For instance, some transforms such as the discrete Fourier transform, discrete cosine transform, discrete wavelet transform, and hybrid transforms are discussed in this section. In addition, a review is given of some proposed methods that have been applied to developing watermark techniques in the frequency domain. The spatial-domain watermarking methods are on average uncomplicated but not much robust. When weighed against methods sustained on frequency domain, for instance, the discrete Fourier transform (DFT) [15],[16], discrete cosine transform (DCT) [17]-[18], discrete wavelet transform (DWT) [19],[20], along with singular value decomposition (SVD) [21],[22], slant transform [23] permit the deployment of signal characteristics and human visualization properties to conquer

enhanced robustness and invisibility. In the earlier period, quite a few watermarking algorithms have been built-up based on assorted incorporation of the above mentioned transforms [24],[25]. Due to multiresolution capability of DWT in time and frequency, it turns into an eminent transform for image processing . For extremely allied image data, the DCT grasps outstanding energy compaction. Watermarking by means of DWT and DCT typically reveal high-quality recital in terms of robustness and invisibility. Besides these two transforms, SVD is a dominant numeric tool cooperative for applications akin to data hiding and image compression. A matrix is factorized into three component matrices in the SVD, which correspondingly enclose left singular vectors, singular values in diagonal, and right singular vectors. Either by modifying the singular values [25] or the singular vectors associated with the largest singular value, a watermark bit can be inserted into an image block. Indeed, quite a lot of endeavors [25]-[26] have been made on the escalation of robust watermarking techniques in an amalgam domain relating the DCT, DWT and SVD. Quite a few existing watermarking techniques are identified by the typical compression process and matrix decomposition. These encompass unsighted SVD techniques that are placed in the bits of the mark within the singular values matrix. Schur transform also decomposes the image, video or mark into unitary transform U and upper triangle matrix T. The diagonal access are eigen values of all blocks in which the most of the energy is potted. A blend of DCT and SVD [28], DWT and SCHUR [29], DCT-DWT-SVD [27] methods seeks to erect watermarking techniques robust in conflict with the majority of attacks. The refined properties of SVD technique are utilized in image watermarking, [30]. This technique is endowed with a proficient means to extort algebraic features like a 2-D matrix. The foremost properties of the matrix of the SVs can be extended in video watermarking. A Little deviation arises in the matrix of the SVs, when a slight amendment is made to the original video. This makes the scheme robust against attacks [30]. By means of this property, the watermark can be inserted into this matrix without discrepancy in the acquired video.

III.VIII. Compressed and Bit-Stream domain watermarking

In this domain of watermarking the watermark is inserted into the bit stream of compressed video. The benefit of this scheme is that the computational cost is low compared to the earlier domains. As the digital video carries a large quantity of data, it is complicated, and so it is realistic to insert watermarks merely in raw video in real time. Usually, before watermarking compression has to be performed on a raw video prior to transmission through the network. Thus the chief concern is how to design a practical compressed video watermarking scheme such that the concealed watermarks probably will be perceived in real time. Consequently the watermark can be inserted in a video in three ways: raw-video, bit-stream and encoding process. The raw video watermarking algorithm inserts the watermark in the frames of video sequences and it is not strong to video compression. Bit-Stream watermarking technique inserts a watermark into the compressed video stream which requires fewer calculations. The third way of inserting the watermark in the encoding process is tough against MPEG compression and there is no bit rate rise of the video stream. Now a days embedding is done in compressed domain since video signals are always stored and transmitted in the compressed format and also as compression is one type of attack, there will be no need to assess it separately against the compression attack. Chiefly there are two approaches for inserting the watermark in compressed video. In this approach, the watermarking process and compression are mutually performed; the error induced by watermark does not extend as the watermarked data are used for subsequent predictions. But there is a rise in bit-rate which must be restricted in this category. In the subsequent approach the compressed video need not

be entirely decoded, which reduces the critical computations during assessment progression and recompression. As the inaccuracy persists, maintaining excellence is the chief trouble in this approach and also cannot be approved in real-time encoder system. As most of the digital video is transmitted in the compressed form, many compressed methods [35-37] have been proposed. M. Kutter et. al [31] proposes an algorithm to place in the watermark by varying the motion vectors. J. Zhang et. al [32] alters kutters algorithm by inserting the watermark into the motion vector of macro blocks that have large amplitude and little phase change. Zina Liu et. al [33] proposes an algorithm to embed a watermark in the motion vectors. Initially the Y component of P frame is separated into high and low texture areas. The motion vectors are modified based on the texture of the area. Then the prediction errors of the matched blocks are calculated at another time according to the distorted motion vectors. At last the new motion vectors collectively with new prediction errors, are encoded into compressed bit streams and thus reducing the flaws and block effects of watermarked video. I. Setyalwan et. al [34] have urbanized an algorithm called extended differential energy watermarking (XDEW) in which the watermark was inserted together into I frames and P frames. Although DEW and XDEW have little difficulty they are not strong enough against attacks which involve frame operators.

IV EVALUATION CONSTRAINTS AND REQUISITES OF WATERMARKING

The performance criteria while watermarking at any rate must include perceptual transparency, robustness, capacity as well as security. The complete simulation outcomes are assessed by analyzing the Imperceptibility, Robustness along with Data payload. Imperceptibility:- Imperceptibility is a feature of the watermarked video which facilitates in maintaining the quality of the video. The watermark should be perceptually unobvious and must not amend even after inserting the watermark into the image, video or text. The visual feature of the watermarked video is approximated by the PSNR (peak signal-to-noise ratio). PSNR is a regularly exercised objective perceptual quality assessment. The divergence of the watermarked and attacked frames on or after the original video frames, is verified by analyzing the PSNR and is given in Eq(4).

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad (4)$$

To assess the PSNR, the Mean Square Error (MSE) linking the original and watermarked frame is worked out, since MSE is the mean square error relating the original video and the watermarked video which is specified in Eq (5).

$$MSE = \frac{1}{R \times C}\sum_{i}^{R}\sum_{j}^{C}[V(\mathrm{i},\mathrm{j}) - \mathrm{V}'(\mathrm{i},\mathrm{j})]^2 \qquad (5)$$

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. 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. (6)

$$NC(V,V') = \frac{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j),V'(i,j)]}{\sum_{i=1}^{R}\sum_{j=1}^{C}[V(i,j)]^{2}} \qquad (6)$$

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. 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 (7).

$$\delta = \frac{TB_{watermarked} - TB_{original}}{\sum_{f=1}^{L_f} N_w(f)} \qquad (7)$$

Where TBoriginal is the number of bits utilized to code the original video sequence, TBwatermarked is the number of bits exploited to code the watermarked video sequence and Nw(f) is the overall number of watermarked coefficients in that video sequence.

V WATERMARKING APPLICATIONS

Content protection along with content tracking has frequently been proclaimed as the inspiration for digital watermarking. Watermarking can be exploited in other applications and potential applications which encompass the following.

- • **Content Tracking:** Through inserting a watermark into all copies of the content the proprietor personalizes. The inserted watermark recognizes the customer who has supervision of that copy. If an incredulous copy of the content is revealed, identifying the watermark relates the origin of the expected copy. These watermarks are seldom termed as fingerprints. Content tracking is not in actual fact intended for individual customers. For instance, assume that the video owner deals with the services of disparate mastering and allocation companies to build and issue the video on media. Conversely, the owner is anxious that several companies possibly will have deficient protection actions to conserve the video. Deceitful corporations or employees possibly will conspire to provide illegitimate copies to pirates. To map out protection contravenes, the owner inserts an unrelated watermark into the copies he offers to the mastering corporation. The video owner recognizes the watermark, if prohibited copies are generated prior to the authorized emancipation of the video to spot the company, whose protection is required. Then the content owner might prefer disagreement with that corporation. A related application arises where the movie owner is anxious regarding collusion, connecting various theater owners and pirates in digital cinema.
- • **Property owner or Copyright recognition:** In copyright watermarking, the implanted watermark encompasses the information regarding ownership, such as, the uniqueness of the proprietor and the copyright date. Identifying the watermark gives the content owner a reason to argue for ownership. The inserted information possibly will also be supportive in identifying plagiarism. The watermark is noticed in the original content.
- • **Copy Protection:** The watermarked content is categorized as a copy protected with the existence of the watermark. An appliance that complies with the copy protection procedure discerns the watermark and subsequently rejects the making of copies. A few copy protection systems restrict the customer from making supplementary copies from a copy, but permit the customer to build a solitary generational copy. In such methods, the inserted watermark encloses information, such as, "forever allocate supplementary copies", "merely single extra copy acceptable" and "refusal of further copies permitted". Exploiting watermarks in this style entail assistance from recording devices to identify the watermark and evade illicit repetition. The inserted watermark will not avert the video from being hackneyed if the recording device overlooks the watermark. Consequently a compromise amongst the inconsistent requirements of the service providers along with the customers would be the inserting of a Serial Copy Management System (SCMS), like copy protection system in all digital recorders. By the SCMS, customers can create replica of several digital sources. But they cannot create copies of copies. This copy protection system verifies the video streams on behalf of a predefined copy forbid watermark. If such a watermark is identified, the arriving video should have been copied earlier and is then rejected by the recorder. The watermark is inserted, if the copy-forbid watermark is not identified, and the watermarked video is preserved. Thus the video data preserved on this recorder forever includes a watermark and cannot be replaced if a recorder is outfitted with such a copy protection system.
- • **Broadcast Monitoring :** An inserted watermark might be utilized to discern or spot a signal of curiosity, chiefly after the signal has been merged with supplementary signals. Identification arises the instant the watermark is noticed. For instance, an advertiser desires to confirm that a precise advertisement is being relayed

as contracted. Validation and inspection are vital concerns as the making and allocation of telecast video content, accompanied by advertisements, amusement content, and news, comprises vast economic value.

- • **Authentication:** The aptitude to discern distorted or fake video is crucial in applications, such as, video surveillance. To validate the reliability of the watermarked signal, inserted watermark should encode information which is essential. If amendments are perceived, the watermark permits the recognition of the imprecise regions. Authentication furthermore incorporate anti-forgery, where a watermark is inserted to boost the intricacy in generating illicit content. For instance, watermarks are projected to look after documents, such as, passports and identification cards.
- • **Robust data hiding:** The inserted watermark may be utilized as a concealed channel to communicate messages from one customer to another. For instance, the dispatcher inserts the watermark within a video, encoding the covert message inside the watermark. The watermarked video is afterwards offered to the beneficiary, probably by means of an unconfident channel or by making the video openly accessible. As the watermarked video and original video are perceptually alike, the communication of the covert message is concealed by means of the original video signal as an inoffensive envelop. The anticipated beneficiary discerns and deciphers the watermark to attain the covert information. These watermarking techniques can further be exploited in fingerprinting and many other applications, some of which are explained below.

Fingerprinting: A customer can accept digital services, similar to pay TV or video on order, through cable or satellite dish by means of a set-top box along with a smart card, which he has to purchase and can as a result be allied to his uniqueness. To prevent other non-paying customers to take advantage of the equivalent services, the service contributor encrypts the data, in support of which he utilizes single or additional keys. This defends the services all through the broadcast. The set-top box in the residence of the customer decrypts the data if a legitimate smart card is utilized, and appends a watermark, in lieu of the uniqueness of the customer, to the data compressed obviously. The fingerprinted data can currently be contributed to the in-house video decoder to inspect the data or the data can be preserved in compressed form.The service contributor can presently recognize customers who convey the data to third parties, flouting their license deal.

Indexing: Guiding of video mail, where annotations can be inserted within the video content; indexing of motion pictures and news items, where markers and annotations can be interleaved, can be utilized by search engines. Medical security: placing the date and the patient's name in medical images may possibly be a supportive protection measure.

VI CONCLUSION

In this paper fundamentals of video and various video formats are specified. Further, dissimilar classifications of video watermarking schemes were illustratedalong with the theory of watermark and various watermark attacks.Additionally the evaluation constraints and requisites of various watermarking methods were mentioned. Finally various disparate applications of video watermarking are enlightened.

Received: 27 Feb 2019 | Revised: 20 Mar 2019 | Accepted: 30 Apr 2020

REFERENCES

[1] Manoharan, Rajesh, et al. "Selection of Intermediate Routes for Secure Data Communication Systems using Graph Theory Application and Grey Wolf Optimization Algorithm in MANETs." IET Networks (2020).
[2] Rajesh, M., Gnanasekar, J.M. Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks. Wireless Pers Commun 97, 1267–1289 (2017). https://doi.org/10.1007/s11277-017-4565-9
[3] Rajesh, M. Streamlining Radio Network Organizing Enlargement Towards Microcellular Frameworks. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07336-9
[4] P. Samuelson, "Legally Speaking: Digital Media and the Law", Communications of ACM, vol. 34, no. 10, pp. 23-28, October 1991.
[5] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," Proceedings of the IEEE: Special Issue on Advances in Video Coding and Delivery, vol. 93, no. 1, pp. 171–183, Jan. 2005.
[6] J. Litman, Digital Copyright. Amherst, NY: Prometheus Books, 2001.
[7] K.Swaraja, Protection of Medical Image Watermarking, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), Special Issue 11, July 2017, ISSN: 1943
[8] C. A. Poynton, A Technical Introduction to Digital Video. New York, NY: John Wiley & Sons, Inc., 1996.
[9] K. Jack, Video Demystified. San Diego, CA: HighText Publications, 1996.
[10] Shi, F., S. Liu, H. Yao, Y. Liu, and S. Zhang, Scalable and credible video watermarking towards scalable video coding, in Advances in Multimedia Information Processing-PCM 2010, Springer, 2010.
[11] Hsu, C.-T. and J.-L. Wu, "DCT-based watermarking for video. Consumer Electronics, IEEE Transactions on", 44(1): p. 206216,1998.
[12] Langelaar, G.C., I. Setyawan, and R.L. Lagendijk, "A State-of-the-Art Overview. IEEE Signal processing magazine",2000.
[13] Kyung-Su, K., L. Hae-Yeoun, and L.Heung-Kyu, "Practical, real-time, and robust watermarking on the spatial domain for high-definition video contents. IEICE transactions on information and systems", 91(5): p.1359-1368,2008.
[14] Xue, J. and J. Tian, Compressed Domain Watermarking with Reduced Error Propagation, Google Patents. 2013.
[15] Frank Hartung, Jonathan K. Su and Bernd Girod: Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. Security and Watermarking of Multimedia Contents, 1999.
[16] Paul, R.T., "Review of robust video watermarking techniques. IJCA Special Issue on Computational Science", 3: p. 9095,2011.
[17] Hartung, F. and B. Girod, "Watermarking of uncompressed and compressed video. Signal processing", 66(3): p. 283- 301,1998.
[18] Tao P, Eskicioglu AM, " An adaptive method for image recovery in the DFT domain", J Multimedia 2006:36–45.
[19] Tsui TK, Zhang X-P, Androutsos D, "Color image watermarking using multidimensional Fourier transforms", IEEE Trans Inform Forensics Sec 2008;3:16–28.
[20] Lin SD, Chen C-F,"A robust DCT-based watermarking for copyright protection", IEEE Trans Consumer Electron 2000;46:415–21.
[21] Patra JC, Phua JE, Bornand C, " A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression", Digital Signal Process 2010;20:1597–611.
[22] Chamlawi R, Khan A, Usman I, " Authentication and recovery of images using multiple watermarks", ComputElectrEng 2010;36:578–84.
[23] Shen H, Chen B, "From single watermark to dual watermark: a new approach for image watermarking", ComputElectrEng 2012;38:1310–24. [21] Su Q, Niu Y, Zhao Y, Pang S, Liu X, "A dual color images watermarking scheme based on the optimized compensation of singular value decomposition", AEU – Int J Electron Commun 2013;67:652–64.
[24] Lai C-C," A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", Digital Signal Process 2011;21:522–7.
[25] Meenakshi, K., Srinivasa Rao, C. and Satya Prasad, K., 2014. A scene based video watermarking using slant transform. IETE Journal of Research, 60(4), pp.276-287.
[26] Meenakshi, K., Prasad, K. S., & Rao, C. S. (2017). Development of Low-Complexity Video Watermarking With Conjugate Symmetric Sequency–Complex Hadamard Transform. IEEE Communications Letters, 21(8), 1779-1782. 14.
[27] Meenakshi, K., Ch Srinivasa Rao, and K. Satya Prasad. "A robust watermarking scheme based Walsh-Hadamard transform and SVD using ZIG ZAG scanning." In Information Technology (ICIT), 2014 International Conference on, pp. 167-172. IEEE, 2014.

[28] Murty S, Kumar PR,"A robust digital image watermarking scheme using hybrid DWT–DCT–SVD technique", Int J Comput Sci Netw Sec 2010;10:185–92.
[29] Bedi SS, Kumar A, Kapoor P, "Robust secure SVD base DCT–DWT oriented watermarking technique for image authentication", In: Proc Int Conf on IT to Celebrate S Charmonman's 72nd Birthday; 2009, pp. 461–7.
[30] A. Sverdlov, S. Dexter, A. M. Eskicioglu," Robust DCT-SVD domain image watermarking for copyright protection : embedding data in all frequencies", 13th European Signal Processing Conference (EUSIPCO 2005), Antalya, Turkey, September 2005, pp. 4-8.
[31] Swaraja K (2018), Medical image region based watermarking for secured telemedicine, Multimed Tools Appl, https://doi.org/10.1007/s11042-0186020-7.
[32] Dixit M, Kulkarni P, Somasagar P, Angadi V, "Variable scaling factor based invisible image watermarking using hybrid DWT–SVD compression–decompression technique", In: IEEE students' conference on electrical, electronics and computer science (SCEECS). 2012. pp. 978–81.
[33] Kutter M, Jordan F and Ebrahimi T, proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video, Technical report M2281, ISO/IEC document, JTC1/SC 29/ WG11, 1997.
[34] Zhang Jun, Li Jiegu and Zhang Ling, "video watermark technique in motion vector", proceedings of XIV Brazilian Symposium on Computer graphics and Image Processing, pp. 179-182, 2001.
[35] Zina Liu, Hunqing Liang, XinxinNiu, Yixian Yang "A Robust Video Watermarking in motion vectors", ICSP'04 Proceedings.
[36] I.Setyawan and R.L.Lagendijk., "Low bit rate video watermarking using temporally extended differential energy watermarking algorithm", Proc. Security and watermarking of multimedia contents III, 2001. 4314: 73- 84.
[37] Swaraja, K., Latha, Y.M., Reddy, V.S.K. and Paramkusam, A.V., 2011, December. Video watermarking based on motion vectors of H. 264. In India Conference (INDICON), 2011 Annual IEEE (pp. 1-4).
[38] Swaraja, K., Madhaveelatha, Y. and Reddy, V.S.K., 2014, December. A pristine digital video watermarking in H. 264 compressed domain. In Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on (pp. 1-4).
[39] .K.Swaraja, Y.Madhaveelatha, V.S.K.Reddy, A secure method of optimized low complexity video watermarking", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 4, MARCH 2015, ISSN 1819-6608, pp.1822-1827.