International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-7 Issue-5, June 2018

A Review of DWT and PCA based Digital Watermarking Schemes

Nidhi Chawla, Vikram Singh

Abstract: ***Video watermarking is an important issue to encrypt intellectual property information for the data creators. Increasing data exchange over the internet also enhancing the probability of piracy and attacks on the encrypted/watermarked video. This problem is encouraging the research community to work over the robust watermarking algorithm which provides ideally attack free watermarked video with the quality maintenance of the video. The Video watermarking techniques using Discrete Wavelet Transform (DWT) or Principal Component Analysis (PCA) played a vital role to develop enhanced algorithm to develop the digital watermarking techniques since the last decade. In this paper, a rigorous literature survey has been done to understand the new possible trends in digital watermarking. An investigation of DWT, PCA, and other possible techniques has been done. The possible attacks also discussed along with a survey to understand the robustness of the proposed algorithm of watermarking. This study and survey provide a better way to understand the new areas and scope of research to the researchers.***

Keywords: DWT, PCA, DCT, Watermarking, Attacks

I. INTRODUCTION

Electronics media is getting popular over the non-electronics media since the last decade. This helps to send data in digital form over the internet which is much faster and easier and can be accessed by anyone. That's why the protection of digital media content and ownership of the document has become an important issue. The fact or process of embedding a piece of code in a digital image, video, or audio file in order to provide copyright information is termed as watermarking. In last decades researchers have introduced new techniques and methods to protect the owner's intellectual property using the digital watermarking. Digital Water Marking (DWM) is a powerful tool for the defining the ownership of the creator of data (audio, video, image etc.). Simultaneous improvement of robustness and impalpable of watermarking in digital video is the major issue encountered by the research community. This motivates to find the comparison over last decade techniques used for the watermarking and review the literature to find new research gaps in the current scenario used by the research community. Current scenario of watermarking techniques includes protection from different types of attacks like jpg compression, salt, and pepper noise attack etc. In this paper, different digital video watermarking techniques have been analyzed and investigated.

Manuscript published on 30 June 2018.
***** Correspondence Author (s)
Nidhi Chawla, M.Tech. Scholar, Department of Computer Science and Engineering, Chaudhary Devi Lal University, Sirsa (Haryana)-125055, India.
Vikram Singh, Professor, Department of Computer Science and Engineering, Chaudhary Devi Lal University, Sirsa (Haryana)-125055, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

This survey and study help the research community to find the new area of research in the domain of digital video watermarking. The efficient way of digital watermarking was introduced by Alfred Haar, in 1909, who gave first wavelet theory and then many researchers utilize this theory to evolve new techniques for digital watermarking for different types of data (audio, video, image etc.).

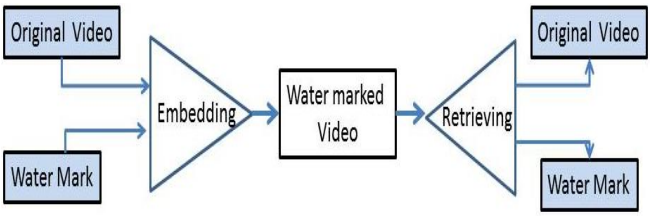

Figure 1 Concept of Digital Water Marking

Figure 1 depicts that Digital watermarking contains an encoder and a decoder. Encoder requires an original image e.g. image "AO" and a watermark (Wm) which belongs to the owner of the data which can be a fingerprint, trademark or logo. Further, an encoding algorithm (E) which contain a security key(S) is required at encoder which embeds the watermark into a digital signal in binary form and replaces the binary values of the original image to make a watermarked image (AW) which can be described in function:

$$AW = E(AO, Wm, S) \quad (1)$$

The decoder is just vice versa of the encoder. It uses reverse(detection) algorithm (e) to separate the watermark from the original image which could be corrupted due to attacks, noises etc.to prove the ownership of the data which can be described if function:

$$Wm' = e(AW, S, \ldots) \quad (2)$$

The algorithm may include the key to encrypt or decrypt the information. The output of the decoder is embedded watermark and original video. In Figure 2, watermarking can be classified in many ways depending upon its domain used for watermark encryption. Type of data used like audio, video, text, and application of a watermark. Watermarking can be understood with help of figure 2. The watermarking is divided into 4 categories. First is domain wise watermarking there is a spatial domain which is a direct implementation of a simple algorithm which is vulnerable to attacks like cropping to the image to tamper the watermark. Another is frequency the domain in which watermark is modified to transform domain which provided tamper resistance to the watermarked image than spatial domain. [6]

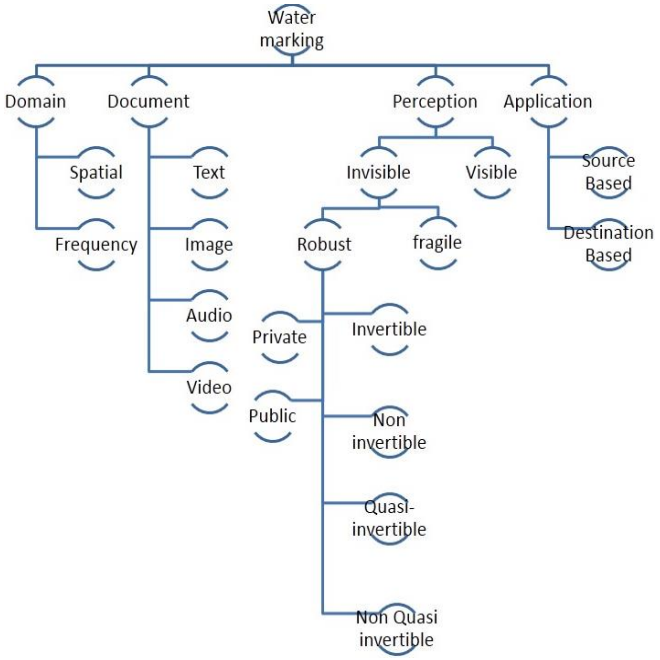

Figure 2: Classification of Video Watermarking

According to the type of document we can classify watermarking as text like books, bills etc. or type of text files like txt, docx, pdf etc. according to images like jpeg, jpg, png etc. Audio can be a recording of the owner or created audio like music. Video can be like flv, mkv, mp4, 3gp etc. Human perception can be considered to classify the watermarking because some are visible to human eyes directly which is visible watermark where which is not visible directly to human eyes are an invisible watermark. Invisible watermark is embedded in the pixels of the original image to provide temper resistance from unauthorized access. Watermark can be tamper easily are fragile watermark where if it is resistive to tampering then they are a robust watermark.

II. SECTION II. CHARACTERISTIC OF DIGITAL WATER MARKING

Every watermarking technique has its own property and advantages against attacks and noises. There are some parameters that need to be considered while selecting any watermarking technique for better results and to satisfy needs of data providers. So they can feel safe to provide data without getting thoughts of piracy, duplication, or unauthorized access to the content of data providers which can cause any economical or loss of intellectual property of them. These characteristics of the watermarking are as follows:

1. Robustness: This is one of the main and common properties of the watermarked image to withstand from different kind of attacks, distortion, and compression etc. [8][9] Rapid growth of the internet has given access to data and receiving and sending which can cause damage to the data and embedded watermark.[11] At the end when the data is decoded to retrieve the watermark from the image then clear the watermark is received from the encoded data describe the robustness of the data.[6] The encoded data should be robust so it can provide high temper resistance to discourage the unauthorized access to data.
2. Imperceptibility: Data of the owner or provider can be in any form e.g. image, video etc. To secure the data, watermark binary value has been fixed to original image pixels.[16] After replacing the pixels, the image quality should not be changed much or can be detected by human eyes.[6][12][46]. If the quality of the watermarked image is detectable then it will be easy to tamper, damage or removal of the watermark in the image so it should be invisible and quality of the watermarked image should be constant.[36]
3. Payload: This is also known as “capacity” of the image to hold the amount of information in the watermark which disturbing the quality or appearance of the data. So we can say that payload can affect imperceptibly of the watermarked image[16]. Increasing the amount of data in the watermark will increase the demand of area and pixels replacement on the image which will affect the image quality after watermarking so there the should be a limited or required amount of data in the watermark which can be held by the original image or video[19]. Watermark to be implemented in the image or video so we can get good quality of the watermarked image.[41] Data in the watermark can be information of owner or logo etc. which can be higher bit then the required size and decrease the imperceptibility of the image which is not favourable. So we have trade-off very carefully between stability and payload.
4. Blind detection: This is the system which is used to decode the watermark from images[16]; if the decoder is using original data to decode the image with the key then it is non-blind detection where if we didn’t use original data then it is blind detection[4]. Blind detection is more favourable because original data can be a video file that is bigger than images so it extracts the watermark without original video which saves computational time and makes the process easy to perform.[47][48]
5. Security: This is one of the main properties of a watermarked image. Every technique has its own advantages and disadvantages but we used those techniques which can provide robustness and quality image with better security[5][10][16]. Watermark should be easy to detect but hard to remove from the image to provide security to the image.[8]Security is our main concern in watermarking [11]. It should encourage the data provider to share his data over the internet or anywhere without any hesitation and fear of piracy, delicacy and unauthorised access.

Currently, still, images have been used for watermarking for copyright and access to the unauthorised person. Watermarking should be easy to detect but hard to remove. There is one special domain, which is very easy to perform and another one is transformed domain which is quite complex but useful than the special domain. This process gives an image in which a watermark is embedded to an original image which is invisible and inaudible to others because we put digital watermarks in the pixel of the host image.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

It is inseparable because the only owner has a compression technique and decompression which can accurately separate the watermark from the host image. Recently we are using frequency domain which gives a robust image which has no effect on compression, cropping, and rotating etc. which help to protect the watermark for decompression.

This has a scope in research in this because of many of our images use a technique which cannot withstand with the attacks from the unauthorized 3rd party who wants claim the intellectual property of owner [24]. So they compression the image again which damage the watermark sometimes so it can't be decompression to abstract the water image from the image or put his watermark with owners watermark which makes hard to find which one is the rightful owner of the property. Spatial domain is easy to use and perform which makes it makes it easy to remove by cropping the image. Transform domain is complex but gives a robust image which is hard to manipulate but still it can be damaged so we need a single solution to protect our digital data from attacks.

III. SECTION III. DIGITAL WATERMARKING TECHNIQUES

A. PCA (Principle Component Analysis)

This type of technique is used as a step-down method to decor relate image pixels and watermarks added [24]. In another way, it can also be used to retrieve the ownership. It is also used to remove liner dependency of the data. It used an orthogonal transformation to convert the dependency of variables into an independent variable called principle component.[9]

a. Embedding Procedure using PCA:-

First, the video which has to be watermark is taken by the owner to hide its ownership mark in that video then 2 levels

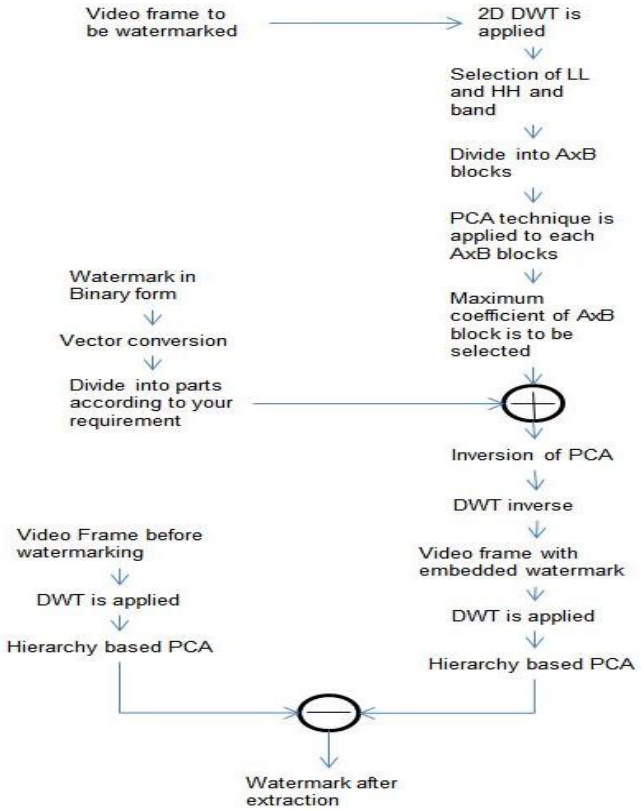

Figure 3: PCA Watermarking Process [27]

DWT is applied to a picture in any video frame then the selection of band is done as in PCA technique higher level band is selected then the area for watermarking is taken in matrix form or in block form after selecting area PCA technique is applied after that maximum coefficient in the matrix is selected [28-29]. Then the watermark which is to be added in image is converted in binary form then there is conversion of that binary watermark into vector form then it is divided into the required parts which are set earlier after that the maximum coefficient and that divided parts are added in this way watermark is added into that particular video frame.

b. Extraction Procedure using PCA:-

The watermarked video is taken then first PCA inversion is done after that DWT inversion is done then the video frames which are watermarked are extracted and then the DWT is applied again after that Block based or hierarchy based PCA is done [28,38]. Then the original video is taken which is not watermarked and in that video DWT is applied and the hierarchy based PCA is applied after that then the watermarked video frames and the unwatermarked video frames are compared, after comparing the watermark is extracted as there is difference in a particular area in non-watermarked video frame and the watermarked video frame.

In [9] the insertion of data in DWT is LL sub-band coefficients and the decorrelation is done with hierarchy among the elements of PCA. The data is inserted in higher frequency level in an adaptive manner due to which it offers high robustness. The results in this are the outcome of the various test which is performed on this that is spatial attacks, compression attacks etc. In [21], the author has analyzed the performance of digital watermark and generalized robustness criteria of the watermark. This helps to measure the capacity of the watermark and attack distortion. Watermark can be viewed on communication channel where most attacks happen on the hostile channel. These attacks are mostly Gaussian noise of additive color and LSI filtering. In most of the conventional channel, communication was hard to perform with watermark especially with white Gaussian Noise. We need a communication system with minimum losses which is the scope of future research. Our main purpose is to transmit the data as it is without any loss in quality. In [32] authors have discussed different kinds of techniques used for watermarking in 2D and 3D images. Attacks are used to tamper the watermark which leads to an undetectable watermark in the extraction process. Researchers have given his or her dedication to this field because of these reasons. Firstly we can get test images very easily and secondly its algorithm is easy to implement in the image. Lastly, we can change algorithm of image watermarking into video watermarking very easily. They discussed two techniques which are mostly used one is a spatial domain in which watermark is represented in the pixels of the original image. In transform domain, they represent it in frequency bands in segments of images. This gives robustness to the image more than spatial domain.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

In [33] author proposed a technique for watermarking in videos which are based on visual cryptography. In this technique, they use an original video and watermark which can be any visible logo of the owner. The original video is split into different frames and then put the logo in the frames of the video using the spatial domain. This approach has stalking frames which contain logo information which has a correlation with the frames of the video. This gives robustness than the non-correlative frames. This technique is resistive to geometric attacks. This has a scope of research to counter the collusion attacks.

In [34] author has discussed the protection of intellectual property of the owner like copyrights, fingerprint etc. watermarking has been growing and developing solutions to provide robust images but they are no focusing on protection of Intellectual Property (IP). They are feeling insecure in this environment due to lack of proper solution. This paper has focused on the collusion attacks to test the image and provide necessary data to protect from collusion attacks. This paper discussed two main pitfalls in the video watermarking, first is the eavesdropping in which users detect every frame of the video to detect the watermark and another is the jamming in which watermark jammed by the user to make it undetectable. This requires a new technique which should be resilient to these attacks which the research gap in this paper to be explored by the research community.

In [27] a new scheme is proposed using 2 level DWT an algorithm is implemented in conjunction with PCA transform this technique is successfully tested and with the help of experimental results it is very clear that the efficiency is very good i.e. 44.097db (PSNRR). In this technique, the watermark is embedded in the higher coefficient of the PCA block. The proposed new technique is very prone to attacks.

In [28] a method of watermarking is introduced by the combination of low-frequency band DCT coefficient and PCA. This method is simulated in MATLAB. The specific feature introduced helps in increasing the capacity of watermark and robustness of the watermark after several attacks like jpeg compression, loss pass filter etc.

In [29] a new technique is introduced by using the combination of DWT-PCA non-blind digital image watermarking. The watermark so inserted is of four different bands of DWT. According to experimental results, PSNR and NC are very good at a range of 0.3 to 0.7 at this range the robustness of image is very good.

In [31] the analysis of different attacks and schemes of watermarking is done and to make the watermark more robust and imperceptible. After analyzing it is found that DCT technique makes the watermark more robust and by using multiple techniques of watermarking in video frames the ownership will be secured somehow as one of the technique will protect from attack.

In [35] a new algorithm is introduced by combining the DWT-PCA technique which makes the watermark more robust and imperceptive. After testing it is found the inserting the watermark in LL sub-band makes the watermark more robust and also the quality of the video will not be degraded. Doing experiments with different types of attacks it is found that normalized correlation (NC) is 1 and the PSNR is 44.097 which is very good and makes the watermark resistive from attacks.

In [38] PCA watermarking technique is used in a block by block basis to decompose the image pixels as the watermarks are added into its principal component. This paper provides a new technique for watermarking which is robust and very imperceptible to attacks. Different attacks are performed to get the robustness of the watermark which is shown via simulation.

B. DWT(Discrete Wavelet Transform)

It is used to add watermarks in video and images. Non-stationary signals are processed by discrete wavelet transform so in the video the watermarks are added in the video frames in sub-images as LL, HL, LH, HH detailed component [39]. This technique captures both frequency and location information [29]. The decoding is done in low resolution to high-resolution manner. After Cube Selection 2-D DWT has been done. The wavelet transforms breaks down an image or video frame into a set of band fixed components which can be put together to rebuild the master copy [23,24]. 2-d DWT is good for any decomposition and recombination of the video and pictures so the DWT techniques are used to decompose the video into the 2-dimensional multi-resolution filtering process. We can also use the DCT but one advantage of the DWT over DCT is that it can more accurately model the aspects of Human vision System as compared in [25-26]. Fig. 4 shows the LL and HH component resulting from 2D DWT.

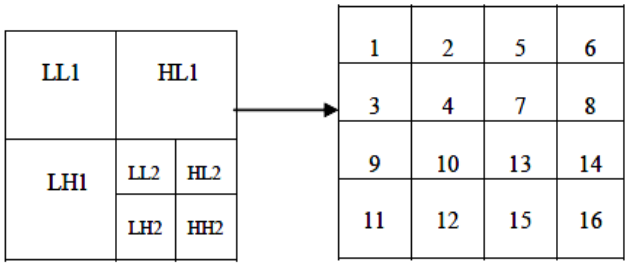

Fig 4. Two-Level DWT and Sub-Band Numbering [22]

An investigation over the literature has been done in DWT techniques over the watermarking embedding and extraction in Video files. In [2] the proposed method inserts many binary images decorrelate from a single watermark, into different frames of a video. The Discrete cosine transform coefficients are modified to form compressed bit stream which is embedded from spatial spread spectrum. For less loss in image precision, a visual mask technique on local image features is absorbed. The simulation experiments show that the introduced watermarking technique is robust and effective which help from spatial attacks like filtering, rotation, scaling, frame averaging etc. The technique introduced in this paper can be further expanded with some minor modification. In [3] an overview of the process used for inserting watermark in I-frames is also used in P-frames for inserting watermark in the video. In P-frame by limiting the watermark the video bit rate increases and therefore the motion's,

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Texture masking, temporal's nonflat areas are utilized in that same time. In I-frames, the spatial mask capacity is used for inserting the watermark. After decoding a new watermark extraction algorithm is introduced which has a controllable performance after experiments with different attacks like filtering, 50% of cropping, 0.001 white noise is added and make it more robust.

IN [4] author has discussed watermark technique in which the quality of the video sequence reduces with the Increase in the robustness of the image. they have proposed an algorithm to enhance the robustness and quality.

In this method, they put a visible watermark in the scene of the video by getting it in segments and use Discrete Wavelet (DWT) to select the block in the segment of video for watermarking. These techniques increase the security of the image.

In [5] author has discussed a video watermarking method based on Discrete Cosine Transform (DCT) by Pseudo 3-D and Quantization Index Modulation (QIM) which can bear several attacks very effectively. In this process, they have used uncompressed video for watermarking by adjusting the correlation between the several blocks of the image and DCT. In this method, the authors have used blind detection for extraction of the watermark and Pseudo 3-D DCT for the insertion of the watermark in the image. This method performs DCT twice in which once is used to measure and calculate the embedding factor of the image and hidden message or useful information in the image. QIM used for embedding the message in the uncompressed domain, then record the user data to generate the secret key. This key is used for embedding the watermark and extraction of the watermark from the video. This proposed method can survive noise attacks, filtering, video compression but it can't withstand geometric attacks. Protection from these attacks will be the major work in the future.

DWT is applied in [7] and the three different coding methods have been used depending on the band coefficient characteristics. These characteristics are lattice code, insignificant coefficient modification depends on human visual model and SVD's quantization index modulation. The proposed model robust against time domain geometrics and frequency based attacks.

In [8] dynamic blocking technique is introduced for selecting the position of inserted watermarks which uses three sub-bands of DWT. This technique is applied to higher edges of the pixels in the image at HL and LH sub-band. This system is better for maps and natural images which has good edges as by using binary algorithm the edges are identified and these edges are backup for each other due to which it becomes more robust.

In [12] author gave a brief introduction to watermarking, its uses and threats. Our technology is improving day by day which allows us to share our digital data to everyone which can be text, image, video etc. and video piracy has become a major issue. So to reduce the piracy we use video watermarking which can be any secret data like a fingerprint, the logo of the owner of the digital data by putting a watermark in the bit stream of video. Watermarks are embedded in the segment of the video and then reconstruct the video. We use DWT of frequency domain to put the copyright information in the form of a watermark in the video frames. This technique gives robustness to the image without disturbing the quality of the image. In future for further improvement 3-D, DWT can be designed to increase the robustness.

In [18] they have proposed a watermarking system which can resist the attacks of geometric distortion which is also known as Rotation, Scaling and translation (RST). This can be achieved by using Discrete Wavelet Transform and their properties. This method embedded the DWT with Spread Spectrum watermark which is presented in the watermark.

In [19], two designs for watermarking have been proposed. These methods provide security for geometric distortion. Image normalization has been used in the first approach. The embedding and extraction of the watermark are done to meet predefined criteria obtained from a normalized image. The author also proposed a normalization procedure which provides robustness to affine attacks. In the second method, the resynchronization of watermark is used to minimize random bending attacks effect. The author used a deformable mesh to redraw the distortion due to attack. The author also used a watermarking algorithm which is robust to affine geometric transformation attacks.

In [36] a new technique is implemented which is the blind extraction of the watermark based on DWT in this no information is needed for original video, owner etc. is not required. According to the proposed algorithm 2D, binary patterns are inserted which makes the watermark more robust and imperceptible. This technique is also prone to combine attacks like MPEG-2 compression and common video attacks. This proposed scheme makes the video watermarking useful for playback control as the original content is unavailable at the decoder side.

C. SVD (Singular Value Decomposition)

Jordan and Beltrami [18] in 1870 proposed method of analysis for square matrices and Young and Eckart in 1936 explored this method for rectangular matrix analysis. The SVD used to extract the algebraic parameters from a matrix of the image [22]. Due to this a good stability of an image can be achieved. If any component is added to the matrix of the image then singular value does not alter much. This technique can be used to embed the watermark in a still image [6]. For the case of the video watermarking, the video is decomposed into a number of frames of images and all the images are embedded by a watermark using SVD process and later all the framed are again combined in the same sequence as before to constitute the watermarked video. Let us consider a video frame image A in the form of a matrix $(m \times n)$. If u *and* v are the orthogonal matrices of size $(m \times n)$ and d is diagonal matrix then applying SVD $'A'$ can be decomposed as follows:

$$A = ud\,v^T \quad (1)$$

$$u = [u1, u2, u3, \ldots, un] \quad (2)$$

$$v = [v1, v2, v3, \ldots, vn] \quad (3)$$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

$$d = \begin{bmatrix} d1 & . & . \\ . & d2 & . \\ . & . & d3 \end{bmatrix} \quad 4$$

Where components of *u* are called left singular vector of 'A' and components of *v* is called right singular vector of 'A'. The singular values of the watermark are introduced in the original images. The SVD important characteristics are that it does not affect the quality of the image. It also maintains the non-symmetric properties of the image. Algebraic properties of images are extracted using the SVD. SVD is more robust to rotation, compression, scaling, noise addition and cropping attacks and so this more popular in the research community.

It can be applied to any kind of images as all kinds of images can be considered as a square matrix so SVD technique can be applied there. The two main properties [20] of SVD are as follows:-

1. If a change is added to an image then there is no such large variation in singular values of the image.
2. Singular values represent independent algebraic image properties.

Further, some of the surveys regarding SVD is as follows. Multiresolution SVD has been discussed in [22].

SVD and DWT based hybrid techniques have been used in [6]. The watermark components are embedded over the singular values of video frames. Due to SVD process, the quality of the videos has been maintained while by using the SVD parameter for the purpose of watermarking the robustness of watermarked video has been enhanced. The author shows that the proposed watermarking technique is robust to many image processing techniques used for attacks. There is still scope of research for combining the characters of the human visual system and proposed watermarking technique.

In the proposed method in [11], the watermark is termed as frame indices and macro block's and inserted over the non-zero quantized DCT blocks. This method is used to detect the tampering and to detect that whether the video has been undergone with some attacks like noise recompression and brightness increase. This is done to check the real-time authentication of the video. The proposed method can be configured to define the robustness, transparency and system capacity for the application-specific area. The method is good for spatiotemporal, temporal and spatial tampering. There is still scope of research in the domain of cryptography and to enhance the system security.

In [13] author has used the different watermarking technique to enhance the robustness and imperceptibility of the image and video. Two methods are Discrete Wavelet transform (DWT) and Singular Value Decomposition (SVD). Both the techniques have its own unique properties and characteristic which gave a rapid growth in authentication of watermarked data. SVD works on selection formula of the subband. We need an original watermark the fingerprint of the owner to fix it in the original image. This method gives more robustness to the image than any other technique and resists most of the attacks very efficiently. In future, we can combine different techniques of watermarking at the different frame of data like images, a video which can increase the capability of the watermark.

In [14] author has proposed a new watermarking technique. In this technique they use two techniques, first is Singular Value Decomposition (SVD) and another is Discrete Wavelet Transform (DWT) sub-band of high frequency. This method has been checked by applying different kinds of attacks. These test will help us to check the imperceptibility of the image and robustness to resist the attacks.

In [20] author has proposed a procedure for compressed video. This developed method put some binary images, disintegrated from single water image, which is put in the different sequence of the image. In this proposed method we use a Discrete Cosine Transform (DCT) coefficient to modify the spatial spread spectrum watermark which is directly put in the compressed bit stream of the video. This process produces fewer losses to fidelity. According to result, watermarked data is less vulnerable to spatial attacks like temporal shifting, scaling, averaging, rotation, filtering etc. and furthermore robustness can be achieved by combining watermarked video and audio together. In case of more security is required and safety become our first priority than all P-frames, b frames, and even I-frames can be watermarked.

In [37] author has discussed a technique which is the combination of DWT-DCT-SVD. The original image is separated into segments of frames which are decomposed by using DWT and HH of High frequency, middle frequency bands LH, and DCT transformed the HL. Watermark coefficient is first to transform using DWT and then SVD to transform and then put the coefficient to the required position in the image. These coefficients are put in the video frames so they can produce less distortion to the original image. This is controlled by Peak Signal to Noise Ratio to attain good imperceptibility. This technique can have non-blind detection of the watermark.

In [22] a new technique is introduced by the combination of SVD with its multiresolution variants (MR-SVD). This scheme is also equated with the previous 3 different schemes for coefficient values of detected watermarks. After experimenting it is found that this scheme gives better imperceptibility and robustness with a PSNR of 79.2363db. Implementation of the algorithm of this scheme is easy on FPGA as compared with DWT. In [38] PCA watermarking technique is used in a block by block basis to decompose the image pixels as the watermarks are added into its principal component. This paper provides a new technique for watermarking which is robust and very imperceptible to attacks. Different attacks are performed to get the robustness of the watermark which is shown via simulation. In [40] the watermarking is done by the PCA and Block-PCA method is proposed by using the principle vectors for reconstruction. According to the analysis the PCA watermarking technique is mostly used in Eigen images. According to the results, the PCA is used for reduction in dimensionality for huge datasets. It is also used for retrieving cover image's reference by compression property of PCA. In [44] PCA technique is used for digital video watermarking.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The introduced algorithm allows inserting the watermark in the three color channels of an input file. The main reason for inserting the watermark in each color channel is to increase the robustness, imperceptibility and data hiding as multiple watermarks are inserted in the three channels. The results show that PSNR is 113.3467db for 40 numbers of frames in the video.

IV. SECTION IV. THREATS AND ATTACKS

To provide high temper resistance we put a watermark in the image or video according to per requirement. This has helped to discourage the unauthorized access by digital watermarking. After adding the watermark in the image only a define algorithm with the key can detect the watermark so to damage and tamper to the image. Unauthorized users use certain techniques and attacks to damage the watermark for image, video etc. they should be robust and imperceptible to reduce the effect of attacks and give a good quality image at the same time.

Geometrical attacks: these are the attacks in which are transformed to damage the watermark in the image by Rotating, Translation, and scaling so this attack is also known as RST attack. After adding the water make in the spatial domain by changing the magnitude of the image in a defined circle. Frequency domain can't change the portion of watermark in the image. But if we rotate the image then the position of the spectrum change which leads to false detection of the watermark of no detection depending upon the damage to the image. [18] This attacks can damage the synchronization between watermarked bit streams which is essential to many techniques which create a problem in detection process where the original image is not available. [19]

Collusion attack: this is one of the simplest attacks to remove the watermark in a video or image. They can damage the watermark by estimation the average number of frames in the video by "n" and then change the value of "n" according to our requirement where "n" is no of frames. [20] Additive noise attack: In [21] author gives a theoretical approach which is based on a random variable. As we have studied in Information theory that the watermark performance depends upon the linear shift-invariant filtering and Gaussian noise. In this approach, the watermark is transmitted through a channel which is known as a hostile channel and has to bear attacks in the communication system. Attack signal in the channel reduces the channel capacity where the use increases the capacity due to the distortion in the watermarked signal. [21]

V. CONCLUSION

This paper has discussed the digital watermarking. Digital watermarking is one of the major concerns because of rapid development in the information technology. Data can be accessed by anyone from anywhere which leads to data sharing and unauthorized uses of the data. So we need a digital watermarking technique to protect the intellectual property like fingerprint, copyrights etc. digital watermarking is used for tamper-resistance to protect the data. There is a need of secure environment to share data with please without any fear of piracy, unauthorised access, and losses to the ownership etc. digital watermarking is process a process in which we use data like image, audio, video etc. and use any technique to transform the watermark and put it in the data. The spatial domain was used for transformation for direct implementation which makes him vulnerable to attacks so we frequency domain like DWT, DCT, SVD in which we transform the coefficient of the watermark in frequency to enhance the robustness to the image as well as imperceptibility. Watermarking technique should fulfill the following characteristic of the watermarking; Robustness is the capability of the watermark image to resist the attack with less damage to the watermark. Imperceptibly is the quality of the image after adding the watermark to the image and security etc. In this paper, different techniques have been discussed and their combination which enhances the security of the watermarked data to prevent attacks. There are many attacks which tamper with the watermark or damage so there should be no detection. These attacks have been discussed in this paper like collusion attack, additive noise attack, Gaussian noise, and many others.

REFERENCES

1. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images" IEEE Transactions on image processing, vol. 8, no. 1, January 1999.
2. S. Biswas, S.R. Das, and E.M. Petriu, "An Adaptive Compressed MPEG-2 Video Watermarking Scheme" IEEE Transactions on Instrumentation and Measurement, vol. 54, no. 5, October 2005.
3. M.Noorkami and R.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.
4. R. Reyes, C. Cruz, M. N. Miyatake and H. P. Meana, "Digital Video Watermarking in DWT Domain using Chaotic Mixtures" IEEE Latin America Transactions, vol. 8, no. 3, June 2010.
5. 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 Transactions on Information Forensics and Security, vol. 5, no. 4, December 2010.
6. C.C. Lai and C.C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition" IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, November 2010.
7. W.T. Huang, S.Y. Tan, Y.J. Chang, C.H. Chen, "A Robust Watermarking Technique for Copyright Protection Using Discrete Wavelet Transform" WSEAS Transactions on Computers, vol 5 Iss 9, 2010, pp:485-495
8. M.R. Keyvanpour, F.M. Bayat, "Robust Dynamic Block-Based Image Watermarking in DWT Domain" Procedia Computer Science 3 (2011) 238–242.
9. H. Khalilian and I.V. Bajic, "Video Watermarking with Empirical PCA Based Decoding" 2013 IEEE.
10. M. Sharma and A. Tiwari, "A Hybrid technique of Video Watermarking in Wavelet domain and Scan based Encryption Method" 2014 IJEDR | Volume 2, Issue 3 | ISSN: 2321-9939.
11. M. Fallahpour, S. Shirmohammad, M.Semsarzadeh, and J. Zhao, "Tampering Detection in Compressed Digital Video Using Watermarking" IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 5, May 2014.
12. Chitrasen and T. Kashyap, "Digital Video Watermarking using DWT for Data Security" International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 1, January 2015.
13. Rajendhiran, J. Elavanthan, M. Vengadapathiraj, R. Vinothkumar and Dr. M. Saravanan, "Video watermarking algorithm for content authorization" International Journal of Science, Engineering and Technology Research (IJSETR) Volume 4, Issue 3, March 2015.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

14. K. Thind and S. Jindal, "A Semi-Blind DWT-SVD Video Watermarking" International Conference on Information and Communication Technologies (ICICT 2014).
15. Md. Asikuzzaman, Md. J. Alam, A.J. Lambert, and Mark R. Pickering, "Robust DT CWT Based DIBR 3D Video Watermarking using Chrominance Embedding" Transactions on Multimedia 2016, pp:1-16, 2016.
16. Md. Asikuzzaman and M. R. Pickering, "An Overview of Digital Video Watermarking" IEEE Transactions on Circuits and Systems for Video Technology 1051-8215 (c) 2016 IEEE.
17. P. Kaur and A. K Gupta, "A Survey on Different Video Watermarking Techniques" International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 4 Issue 4 November 2014.
18. V.Licks, R. Jordan "ON DIGITAL IMAGE WATERMARKING ROBUST TO GEOMETRIC TRANSFORMATIONS" IEEE, 0-7803-6297-7
19. P. Dong, J.G. Brankov, N.P. Galatsanos, Y.Yang, and F.Davoine, "Digital Watermarking Robust to Geometric Distortions" IEEE Transaction on image processing, vol 14 no 12, 2005 pp:2140-2150.
20. S. Biswas, S. R. Das, and E.M. Petriu, "An Adaptive Compressed MPEG-2 Video Watermarking Scheme", IEEE transactions on instrumentation and measurement, vol. 54, no. 5, October 2005
21. J. K. Su, J.J. Eggers, B. Girod," Analysis of digital watermarks subjected to optimum linear filtering and additive noise" Elsevier, signal processing 81 (2001) pp: 1141-1175
22. S. Majumder, S. Swarnalipi, S. Sarkar and S.Kumar Sarkar. A Novel Watermarking using Multiresolution SVD matrix. International Journal of Electrical, Electronics vol.1, Iss 2, 2012 pp.35-39.
23. S.K. Amirgholipour, A. R. Naghsh-Nilchi: Robust Digital Image Watermarking Based on Joint DWT-DCT, International Journal of Digital Content Technology and its Applications Volume 3, Number 2, pp. 42-54, June 2009.
24. M. Chandra, S. Pandey: A DWT Domain Visible Watermarking Techniques for Digital Images, International Conference on Electronics and Information Engineering, pp. V2-421 - V2-427, 2010.
25. Salwa A.K Mostafa, A. S. Tolba, F.M. Abdelkader, Hisham M. Elhindy, Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
26. Sanjana Sinha, PrajnatBardhan, SwarnaliPramanick, AnkulJagatramka, Dipak K. Kole, Arun Chakraborty,Department of Computer Science & Engineering, St Thomas' College of Engineering and Technology, Kolkata, India, Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis, International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011.
27. Nisreen I. Yassin, Nancy M. Salem, and Mohamed I. El Adawy, "Block-Based Video Watermarking Scheme Using Wavelet Transform and Principal Component Analysis", International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012, pp: 296-301
28. ArashSaboori, S.AbolfazlHosseini, "A New Method For Digital Watermarking Based on Combination of DCT and PCA", TELFOR 2014, pp: 521-524
29. Anandkumar, Mukesh Gupta, "Semi visible Watermarking Scheme Based on DWTandPCA" International Conference on Green Computing and Internet of Things (ICGCloT), 2015, pp: 986-990.
30. Dejey, R.S. Rajesh; "Robust Color Image Watermarking Schemes In the Wavelet Domain"; ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, Iss 01, 2010
31. Varsha Gaikwad, RehanaShikalgar, ShubhangiSagare, ShitalShendage, "Analysis of Attacks on Video Watermarking", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 6, Issue 4, April 2017
32. Dr. S. Agarwal, Priyanka, Usha Pal, " Different Types of Attack in Image Watermarking including 2D, 3D Images", International Journal of Scientific & Engineering Research, Volume 6, Issue 1, January-2015
33. Amir Houmansadr Shahrokh Ghaemmaghami, "A Novel Video Watermarking Method Using Visual Cryptography", Engineering of an intelligent system, 2006 IEEE International Conference on 22-23 April 2006
34. Gwena¨elDo¨err and Jean-Luc Dugelay, "Collusion Issue in Video Watermarking," Download Link: https://pdfs.semanticscholar.org
35. M. A Chimanna, S.R.Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery", International Journal of Engineering Research andApplications, Vol. 3, Issue 2, March - April 2013, pp.839-844.
36. C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, H. Perez-Meana, "A Blind Video Watermarking Scheme Robust To Frame Attacks Combined With MPEG2 Compression", Journal of Applied Research and Technology, Vol.8 No.3 December 2010, pp: 323-339
37. C. N. Sujatha, P. Satyanarayana, "Analysis of Robustness of Hybrid Video Watermarking against Multiple Attacks", International Journal of Computer Applications, Volume 118 – No.22, May 2015
38. R. C. Gonzalez, R. E. Woods, and S. L. Eddins, "Digital image processing Using Matlab", Pearson Prentice Hall, New Jersey, 2004.
39. P.W. Chan and M. R. Lyu, "A DWT-based digital video watermarking scheme with error correcting code" Proceedings of the 5Th International Conference on Information and Communications Security, 2003, pp. 202-213.
40. ErkanYavuz and ZiyaTelatar, "Digital Watermarking with PCA Based Reference Images", ACIVS 2007, pp. 1014–1023.
41. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 6, NO. 12, DECEMBER 1997, pp: 1673-1687
42. S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers and J.K. Su, "Attacks on Digital Watermarks: Classification, Estimation-based Attacks, and Benchmarks,"
43. ShouyuanYanga, Zhanjiang, Zhijun Fang, Jucheng Yang, "A Novel Affine Attack Robust Blind Watermarking Algorithm", Symposium on Security Detection and Information Processing, Procedia Engineering 7 (2010) 239–246
44. KunalAhire, Gajendra Singh Chandel, "Digital Video Watermarking Using Principal Component Analysis", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 4, April 2014, pp: 1171-1174
45. P. Singh, A. Agarwal, J. Gupta, "Image Watermark Attacks: Classification & Implementation", IJECT Vol. 4, Issue 2, April - June 2013, pp: 95-100
46. Zaidi, R. Boyer, and P. Duhamel, "Audio Watermarking Under Desynchronization and Additive Noise Attacks", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 54, NO. 2, FEBRUARY 2006, pp: 570-584.
47. Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for authentication and Compression of Cultural Heritage Images", in IEEE transactions on linage Processing, vol. 13, no. 3, pp. 430-448, March 2004.
48. V, M. Potdar, S.Han, Elizabeth Chang"A Survey of Digital Watermarking Techniques " in 3rd IEEE International Conference on Industrial Informatics (INDIN), 10-12 August 2005, Australia

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.