Methodology for Fast and Robust Video Watermarking Technique using DWT, CNN and DCT Techniques

Devendra Singh Patel[1], Akant Kumar Raghuwanshi[2]

[1]M.Tech Scholar, [2]Assistant Professor
Vedica Institute of Technology
RKDF University, Bhopal

Abstract:- In the current scenario, data transmission through digitize way is becoming a fast variant. But security between data transmissions is a measure concern. So digital watermarking technique provides a way to prevent unauthorized access, illegal exploitations and allocations and copyright protection of the digitize data. Discrete Cosine Transform (DCT), Dyadic Wavelet Transform (DWT), and Deep Convolutional Internet backbone techniques are combined to provide a resilient multiple data hiding in this study on a few middle bands of the video frames. Because it efficaciously satisfies the requirement of imperceptibility and offers high soundness against a variety of image-processing attacks, such as Mean filtering, Median filtering, Gaussian noise, salt and pepper noise, poison noise, and rotation attack, this methodology is considered to be robust blind made the process. The resilience of the watermark is defined by the outcome analysis' evaluation of PSNR and MSE, which shows that the record will not be destroyed following voluntary or involuntary attacks and may still be utilized for verification.

Keywords: Blind Watermarking, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Convolution Neural Network (CNN), MATLAB, Robust, PSNR.

I.Introduction

Digital watermarking is the process of permanent incorporation of data (adding a watermark) into digital media content (host data) without degradation, so that the watermark can withstand any external operation. The watermark can be visible or invisible. The basic characteristics of each watermark scheme are its capacity, robustness, security and imperceptibility.

More details about the host image are provided by the watermarking process. As depicted in Fig. 1.1, watermarking essentially consists of four steps: synthesis, encapsulation, dissemination, and attacks and extraction [1].

The process of creating a watermark creates a logo in the form of audio, video, or text that is unique to the information and must be designed so that it is challenging to remove or distort from various attacks. In the process of embedding, a logo or other mark image is added to the host image. The act of distribution can be compared to the transfer of watermarked data. And attempts to alter the content are referred to as assaults [2]. Extraction is that the method that permits owner to be known and provides data to the meant recipients. Extraction uses the same technique as embedding but works in the opposite direction. For implantation and extraction of watermarks, many techniques are employed.

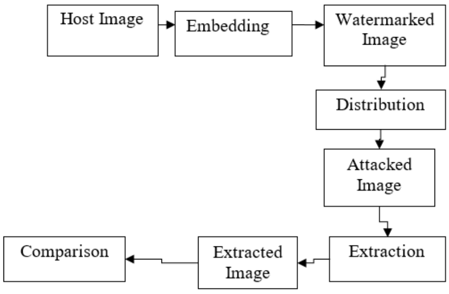

Figure 1: General Image watermarking Procedure

Any process forms has the qualities of watermarked image, robustness, capacity, and security [3]. Each application's requirements are different. Each application doesn't require each of the qualities that are considered while developing watermarking systems.

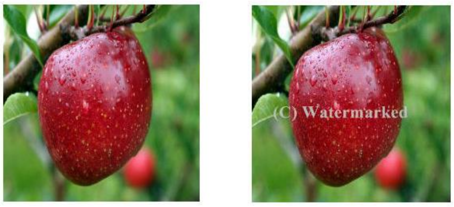

Figure 2: Example of Watermarking

Text Watermarking

Secret agencies have historically utilized techniques for inserting information into text documents. We must distinguish between text watermarking techniques that conceal information in the format (i.e., the layout and appearance) and techniques that conceal content in the semantics (i.e., the meaning and sequence of the words) [4].

The first class designs a text around the message to be hidden. In that sense, the information is not really embedded in existing information, but rather covered by misleading information.

If the watermark is in the format, then it can obviously be removed by “retyping” the whole text using a new character font and a new format where “retyping” can be either manual or automated using optical character recognition (OCR). OCR systems are still not perfect for many applications today and often need human supervision. Thus, removal of watermarks either yields bad results (single characters are wrong, due to OCR) or is expensive.

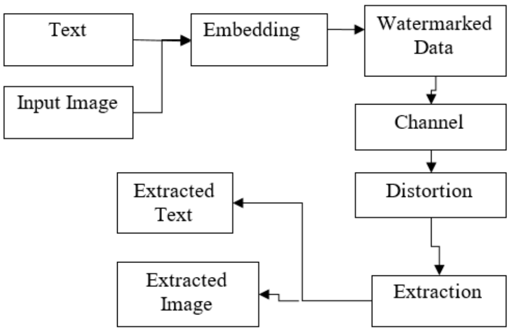

Figure 3: Text Watermarking Technique

The copyright owner has the right to copy, the watermark is more expensive. The text watermarking has copyrighted electronic document which is to be distributed, though it can be defeated in virtual digital libraries. Where users may download copies of documents and books but they are not allowed to further distribute and cannot be store for longer time than certain predefine period. In this type of application, a requested document is watermarked with a requester specific watermark before releasing it for download. If later on illegal copies are discovered, the embedded watermark can be used to determine the source [5].

The Information- and Communication-based Society (ICS) has undergone a paradigm transition from the analog to the digital world in recent years, facilitated by the astounding evolution of the relevant technologies, altering the way the information is accessed, shared, and processed. In this situation, the industrial and research communities are paying more and more attention to security issues in order to deal with the new security difficulties including the defense of digital contents against established threats as well as fresh, more subtle problems [1].

Although digital media has several benefits over analog media [2], the risk of unlicensed replication and distribution of protected content threatens established business structures. Therefore, it is crucial to use a proper and appropriate application to secure the necessary data. Recently, watermarking has attracted a lot of attention. It is primarily driven by the necessity to give digital content, such as audio, video, and still photos, copyright protection.

Encryption and watermarking are two complementing technologies. Data is shielded during transport from the sender to the receiver through encryption. But after delivery and subsequent decryption, the data can produce an inaccurate picture.

Encryption is complemented by watermarking, which incorporates data into the image itself. As a result, the watermark is always present in the data. The authenticity and security issues are investigated in the current study by developing an optimization-based methodology. The watermarking of photographs is of great importance. Application-based watermarking techniques have been created, researched, and authenticated for use with diverse sets of photos. Various resource limits are taken into account while determining the level of authenticity needed to combat the attacks. Digital watermarking can often be divided into two categories: fragile and robust. A weak watermark will suffice if the desired behavior is integrity proof (tamper detection); but, if a watermark is used to convey copyright notices and prohibit illegal copies, it is crucial that it be strong and resistant to several attacks.

The bit stream watermarking techniques utilized in prior studies are less reliable. An efficient, reliable, and undetectable video watermark technique was suggested in this work. The fourier transform (DWT), discrete cosine transform (DCT), and convolution neural network were the foundations on which this algorithm was built (CNN). Two distinct transformation domain strategies have demonstrated high degrees of complimentary robustness.

II.Related Work

Panyavaraporanet al. [1] On the domains of the wavelet decomposition (DWT) and discrete cosine transform (DCT), a proposed invisible digital watermarking procedure is provided. In this case, a video stream's middle sub-band coefficients contained a binary watermark image. The PSNR values of the watermarked videos were as high as virtually up to 37 dB with the ideal watermarking strength, according to testing results of the suggested technique.

Ali et al. [2]proposed a novel robust image watermarking scheme developed in the wavelet domain based on the singular value decomposition (SVD) and artificial bee colony (ABC) algorithm. The watermark bits are embedded into the target blocks by modifying the first column coefficients of the left singular vector matrix of SVD decomposition with the help of a threshold and the visible distortion caused by the embedding is compensated by modifying the coefficients of the right singular vector matrix employing compensation parameters.

Makbol et al. [3] introduced a reliable discrete wavelet transform (DWT) domain singular value breakdown (SVD) and human visual system-based block-based image watermarking scheme. The suggested technique is thought to be a block-based strategy that uses edge entropy and entropy as HVS features to choose important blocks to place the watermark in.

FindIk et al. [4] artificial immune identification system (AIRS) has suggested embedding a binary image of size 32 x 32 to the blue component of a color image of size 510 x 510. This method has good watermark performance.

Vahedi et al. [5] developed a new wavelet-based steganography technique employing bio-inspired optimisation principles for color images, and a binary logo with a size of 64 by 64 was inserted into a 512 by 512 color image.

Chou and Wu [6] proposed to embed the colour image watermarks into the colour host image, in which the computational complexity was very low but its robustness needs to be improved. Moreover, some watermarking methods based on matrix decomposition have been proposed [6-8].

Among them, Lai [7] designed a novel watermarking method based on HVS and singular value decomposition (SVD), in which the binary watermark was embedded into greyscale image of size 512 × 512 by modifying the certain elements of the unitary matrix U. This method has better performance of resisting adding noise, cropping and median filtering, but is worse in the aspect of resisting the rotation and scaling.

Golea et al. [8] proposed an SVD-based colour image watermarking scheme to embed colour watermark image into colour host image, but its invisibility is bad because one or more singular values of embedding block must be modified to keep the order of singular values. Bhatnagar and Raman [8] embedded the greyscale watermark of size 256 × 256 into the greyscale image of size 512 × 512. This method is non-blind watermarking method and has the false-positive detection problem.

Charles Way Hun Fung et al. [9]proposed a way to embedded the watermark in videos that insert data within the side view. once this method the DWT-SVD watermarking is employed to insert a grayscale image on the luminance(Y) of YUV regenerate video. High performance once the PSNR metric is measured. because of the utilization of a non-blind watermark the necessities for the extraction method are the first watermark and video. This work was solely appropriate for tamper detection and authentication.

DivjotKaurThind [10] proposed a digital video watermarking scheme which combines Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD). The simulation result provide robustness against attacks such as frame dropping, frame averaging and lossy compression. The main drawback of this scheme was that its complexity translates in this case into more resources required to perform the computation - more memory and/or processor cycles and/or time.

III.Proposed Methodology

This work suggests a video watermark method that is effective, reliable, and undetectable. The Deep Convolutional Network (CNN), Discrete Wavelet Transform (DWT), and Discrete Cosine Transform served as the foundation for this technique (DCT). Three independent transformation domain techniques have demonstrated that their combination results in a high level of complimentary and diverse levels of robustness against the same assault. choosing the intermediate band's coefficient in a zigzag pattern. The water mark consists of several photos.The wavelet domain transformation of the various pictures is used to perform watermark embedding. The relevant coefficients of wavelet features are supplemented by watermark bits. Fully convolutional networks have the ability to learn and adapt, therefore the trained network can precisely retrieve the watermark from the watermarked image.

Embedding Algorithm

In an image, it is well known that the high-frequency information reflects the local features and the low-frequency information the global details. It is standard procedure to separate the image's high-frequency and low-frequency components and process them separately. It is suggested that an image be divided into high and low frequency components in order to preserve image details and colors in the brightest and darkest areas. It's crucial for the network to strike the right balance between high and low frequency component in order to train a CNN that can both increase the brightness range of a low-contrast image and expose some missing information. The digital image and cover frame's low frequency and high frequency features are first separated out of this work's Y component. L(x, y) is a low-frequency component, whereas R is a high-frequency component (x, y).

$$I(x,y)= L(x,y)+R(x,y)$$

Each channel is subjected to the weighted least squares (WLS) algorithm for the deconstruction. We decide to incorporate watermark data in the host image's wavelet transform domain in accordance with the visual features of the human eye. A 2-DWT transform of the host image is carried out to obtain sixteen strips4 sub-bands of LL, 4 sub-bands of LH, 4 sub-bands of HL, 4 sub-bands of HH i.e. LH21, HH21, LH22, HH22, LL23, HL23, LL24, HL24.The high frequency CNN features of the watermark are then embedded into the 4 sub-bands HH21, HH22, HL23, HL24strip and low frequency CNN features of the watermark are then embedded into the 4 sub-bands LH21, LH22, LL23, LL24. Figure 3.1 illustratesthe watermarking and training procedure of the proposed method.

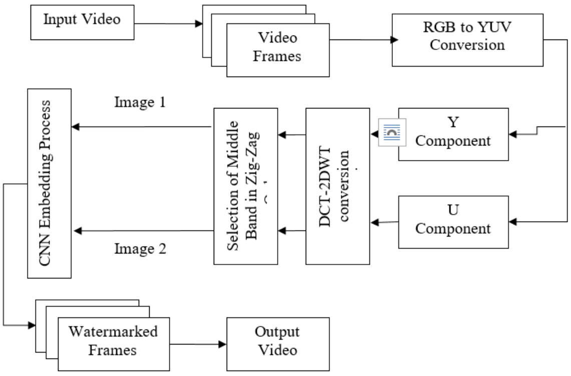

Figure 4: Watermark Embedding Process

CNN Network Architecture

Convolutions (CNNs) were developed in order to address the drawbacks of fully connected neural networks and will serve as the basis for this dissertation. These are a particular kind of neural network that deviates slightly from the structure of conventional neural networks since they are intended to be utilized with images. The fact that CNNs are not fully linked, where every node in a layer is connected to every node in the preceding layer, is another important characteristic of CNNs. A CNN has three main components:

- Convolutional layer
- Rectified Linear Unit
- Pooling layer
- Fully connected layer

The proposed CNN contains three fully connected layers and five fully connected layers, as shown in Figure 4.

i. To create 96 feature maps, a convolution with 96 filters of size 11*11 with strides 4 is utilized.

ii. The Batch Normalization Unit (ReLU) is used to address network nonlinearity.

iii. Max Pooling with 3*3 with stride 2

iv. Conv with 256 filters of size 5*5, 1 stride, and 256 processing elements.

v. Rectified Linear Units, or ReLU, are used to account for network inhomogeneity.

vi. Max Pooling with 3*3 with stride 2

vii. Using a convolution with 384 filters of size 3*3 and one stride, 384 feature maps are produced.

viii. ReLU (Rectified Linear Unit) is utilized to account for network inhomogeneity.

ix. Max Pooling with 3*3 with stride 2

x. Conv produces 384 extracted features with 384 filters of size 3*3 with 1 stride.

xi. ReLU (Rectified Linear Unit) is utilized to address variation in networks..

xii. 256 filters of size 3*3 with a stride of 1 are combined in a convolution to produce 256 feature maps.

xiii. ReLU (Rectified Linear Unit) is used to address variability in networks.

xiv. Max Pooling with 3*3 with stride 2

xv. Fully linked layer for the procedure used to attach the saliency map, having 4096 neurons per layer.

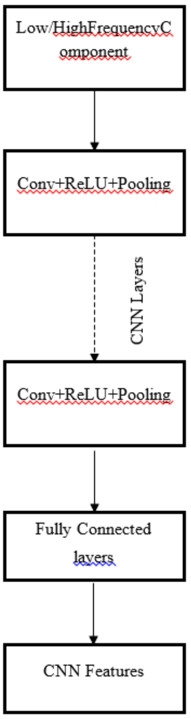

Figure 5: Proposed CNN Architecture

IV.Conclusion

For the protection of the copyright and the identification of the property, algorithms of incorporation and extraction in watermark are necessary. This research provides a comprehensive overview of the various watermarking techniques for digital images in various fields and their needs. It has been discovered that, to minimize distortion and increase capacity, frequency domain techniques must be combined with other techniques that have high abilities and robustness against various types of attacks. In this research watermarking is done by the combining the features of Convolution Neural Network (CNN), Discrete Wavelet Transformation (DWT) and Discrete Cosine Transformation (DCT). The RGB color image is converted to a combination of YUV colors. The Y and U color component of the image is used to reduce computational complexity by including multiple watermarks.CNN-DCT-2DWT embedding and extraction technique is performed on the low frequency and high frequency DWT sub-band of video frames. The analysis of the results was made with different types of attacks and concluded that the proposed technique is quite effective compared to existing watermarking technique.

Following conclusions are derived from this research work as:

i. This algorithm is robust.

ii. This algorithm provides a blind watermark with watermark detection and extraction and is effective against the most common attacks.

iii. PSNR value obtained is 48.29.

iv. The result analysis shows about 14% efficient as compared to existing work.

This research work is focused on digital watermarking. Some of the objectives are fulfilled in this research work but there are also some imitations that can be clearly focused in future. Some of the future work are discussed below:

1. The future works will be focused on improving the performance of proposed technique against more attacks and further research work will be enhanced for medical applications and biometrics applications.

2. This research can be considered as an extension of research as the video consists of a stream of frames and the hacker may delete the frame(s) consisting of authentication information without quality degradation.

3. In future, work will be focused on reducing the time complexity of the methodology as well as to enhance the performance parameters such as PSNR under attack situations.

References

[1] Jantana Panyavaraporn, Paramate Horkaew, “DWT/DCT-based Invisible Digital Watermarking Scheme for Video Stream”, IEEE, 2018, pp. 154-157.

[2] Ali, M., Ahn, C.W., Pant, M., “An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony”, Information Sciences., Vol. 301, pp. 44–60, 2015.

[3] Makbol,Khoo, Rassem, “Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics”, IET Image Processing, vol. 10, pp. 34–52, 2016.

[4] O. FindIk, I.Babaoglu, E.Ülker, “A color image watermarking scheme based on artificial immune recognition system”, Expert System Application, vol. 38, pp. 1942–1946, 2011.

[5] E. Vahedi, R.A. Zoroofi, M. Shiva, “Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles’, Digital Signal Processing, Vol. 22, pp. 153–162, 2012.

[6] Chou, C.H., Wu, “‘Embedding color watermarks in color images”, EURASIP journal on Advances in Signal Processing., pp. 32–40, 2003.

[7] Lai, C.C., “An improved SVD-based watermarking scheme using human visual characteristics”, Optic Communication., Vol. 284, pp. 938–944, 2011.

[8] Golea, N.E.H., Seghir, R., Benzid, R., “A blind RGB color image watermarking based on singular value decomposition”, IEEE, pp. 1–5, 2010.

[9] Charles Way Hun Fung, Walter Godoy jr., “A New Approach of DWT-SVD Video Watermarking”, IEEE, 2011.

[10] Divjot Kaur Thind, Sonikajindal, “A Semi Blind DWT-SVD Video Watermarking”, Procedia Computer Science, Vol. 46, pp. 1661-1667, 2015.