Robust and Blind Multiple Image Watermarking Using CNN and DWT in Video

Farha Khan  
M. Tech. Scholar  
Department of Electronics and Communication  
All Saints College of Technology, Gandhi Nagar  
Bhopal, India  
farhakhan1609@gmail.com

M. Sarwar Raeen  
Professor  
Department of Electronics and Communication  
All Saints College of Technology, Gandhi Nagar  
Bhopal, India

Abstract—Digital watermarking was introduced as a result of rapid advancement of networked multimedia systems. It had been developed to enforce copyright technologies for cover of copyright possession. Due to increase in growth of internet users of networks are increasing rapidly. It has been concluded that to minimize distortions and to increase capacity, techniques in frequency domain must be combined with another technique which has high capacity and strong robustness against different types of attacks. In this paper, a robust multiple watermarking which combine Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Convolution Neural Network techniques on selected middle band of the video frames is used. This methodology is considered to be robust blind watermarking because it successfully fulfills the requirement of imperceptibility and provides high robustness against a number of image-processing attacks such as Mean filtering, Median filtering, Gaussian noise, salt and pepper noise, poison noise and rotation attack. The proposed method embeds watermark by decomposing the host image. Convolution neural network calculates the weight factor for each wavelet coefficient. The watermark bits are added to the selected coefficients without any perceptual degradation for host image. The simulation is performed on MATLAB platform. The result analysis is evaluated on PSNR and MSE which is used to define robustness of the watermark that means that the watermark will not be destroyed after intentional or involuntary attacks and can still be used for certification. The analysis of the results was made with different types of attacks concluded that the proposed technique is approximately 14% efficient as compared to existing work.

Keywords—Digital watermarking, Spatial Domain, Transform Domain, DWT, DCT, CNN.

I. INTRODUCTION

In the recent years, Information and Communication Society (ICS) has experienced a paradigm shift from the analog to the digital world fostered by the astonishing evolution of the involved technologies, changing the way the information is accessed, shared and processed. In this scenario, security issues have gained increasing attention from the industrial and research communities in order to cope with the emerging security challenges involving the protection of digital contents against traditional menaces as well as new, more subtle, vulnerabilities [1].

Digital media has many advantages over analog media [2], however the possibility of unlicensed duplication and dissemination of copyrighted material poses a hazard to traditional business models. Hence, a proper and suitable application is essential to secure the required data. There has been a significant interest recently in watermarking. It is primarily motivated by a need to provide copyright protection to digital content, such as audio, video and still images [3].

Two complementary techniques are - encryption and watermarking. Encryption protects the data during the transmission from the sender to the receiver. However, after receipt and subsequent decryption, the data might present a distorted image [4]-[7].

Watermarking complements encryption by embedding data directly into the image. Thus, the watermark always remains present in the data. In the present research, the authenticity and security problems are studied by establishing a method based on optimization. In particular, the focus is on watermarking of images. Application based watermarking methods have been developed and studied for various sets of images and tested for authenticity [8][9]. The level of authenticity required to tackle the attacks is determined, taking different resource constraints into consideration. In general, the digital watermarking can be classified into two groups namely, fragile and robust. If the desired behavior is the integrity proof (tamper detection), then a fragile watermark is enough; whereas, if a watermark is used to carry copyright notices and prevent unauthorized copies, it is important that it is robust, and can survive the many attacks [10]-[12].

Bit stream watermarking used in earlier research are less robust in nature. In this study, an effective, robust and imperceptible video watermark algorithm was proposed. This algorithm was based on a cascade of three powerful mathematical transformations; Discrete wavelet transform (DWT), discrete cosine transforms (DCT) and Convolution neural network (CNN). Two different techniques of transformation domain have shown a high degree of complementary and different levels of robustness.
II. RELATED WORK

Panyavaraporn et al. [1] proposed an invisible digital watermarking algorithm on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains. Herein, a binary watermark image was embedded in the middle sub-band coefficients of a video stream. The experimental results of proposed algorithm indicate that the PSNR values of the watermarked videos were as high as almost up to 37 dB with the optimal watermarking strength. 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 host image is transformed into an invariant wavelet domain by applying redistributed invariant wavelet transform, subsequently the low frequency sub-band of wavelet transformed image is segmented into non-overlapping blocks. The most suitable embedding blocks are selected using the human visual system for the watermark embedding. 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] presented a robust block-based image watermarking scheme based on the singular value decomposition (SVD) and human visual system in the discrete wavelet transform (DWT) domain. The proposed method is considered to be a block-based scheme that utilizes the entropy and edge entropy as HVS characteristics for the selection of significant blocks to embed the watermark.

Findik et al. [4] proposed to embed the binary image of size 32 × 32 to the blue component of color image with size 510 × 510 by artificial immune recognition system, and this method has good performances of the watermark.

Vahedi et al. [5] proposed a new wavelet-based watermarking approach for color images using bio-inspired optimization principles, and the binary logo of size 64 × 64 was embedded into the color image of size 512 × 512.

III. METHODOLOGY

This paper proposes an efficient, robust and imperceptible video watermarking algorithm. This algorithm was based on a cascade of powerful mathematical transformations; Convolution Neural Network (CNN), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT). Three different transformation domain techniques have shown that a high level of complementary and different levels of robustness against the same attack are achieved by their combination. Selection of the coefficient of the intermediate band as in the zigzag order. Several images are used for the water mark. Watermark embed processing is carried out by transforming the multiple images in wavelet domain. Watermark bits are added to the significant coefficients of wavelet characteristics. Because of the learning and adaptive capabilities of convolution neural networks, the trained network can exactly recover the watermark from the watermarked image. The proposed method embeds watermark by decomposing the host image. Convolution neural network calculates the weight factor for each wavelet coefficient. The watermark bits are added to the selected coefficients without any perceptual degradation for host image.

A. Embedding Algorithm

It is known that in image, the low-frequency information of an image represents the global details, and the high-frequency information represents the local details. It is a common practice that we can separate the image low-frequency component and high-frequency component and process them individually. The methodology is proposed to decompose an image into high and low frequency components to preserve image details and colors in the brightest/darkest regions. In order to train CNN which can not only enhance the luminance range of the low-contrast image but also reveal some missing details, it is important for the network to make an appropriate balance between high and low frequency components. In this work first, the Y component is decomposed into low frequency feature and high frequency feature of watermark image and cover frame. Low frequency component, L(x, y), and a high-frequency component R(x, y).

\[
I(x,y) = L(x,y) + R(x,y)
\]

The decomposition is performed by applying the weighted least squares (WLS) method to each channel. For embedding algorithm, considering the human eye’s visual characteristics, we choose to embed watermark information in the wavelet transform domain of the host image. A 2-DWT transform of the host image is carried out to obtain sixteen strips 4 sub-bands of LL, 4 sub-bands of LH, 4 sub-bands of HL, 4 sub-bands of HH i.e. LH21, LH22, LH23, LH24, HH21, HH22, HH23, HH24, LL21, LL22, LL23, LL24. The high frequency CNN features of the watermark are then embedded into the 4 sub-bands HH21, HH22, HH23, HH24 and low frequency CNN features of the watermark are then embedded into the 4 sub-bands LH21, LH22, LH23, LH24.

Figure 1 illustrates the watermarking and training procedure of the proposed method.
To combat the issues of fully connected neural network, convolutional neural networks (CNNs) were created and will be used as the foundation of this dissertation. These are a type of neural network which is designed specifically to be used with images, and differ slightly from traditional neural network structure. Another key property of CNNs is that they are not fully connected, where every node in a layer is connected to every node in the previous layer. There are three main elements to a CNN:
- Convolutional layer
- Rectified Linear Unit
- Pooling layer
- Fully connected layer

The proposed CNN has 5 convolutional layers and 3 fully connected layer which are shown in Figure 2.

Conv with 96 filters of size 11*11 with strides 4 are used to generate 96 feature maps.
For nonlinearity in network, ReLU (Rectified Linear Unit) is applied.
Max Pooling with 3*3 with stride 2
Conv with 256 filters of size 5*5 with 1 stride that generate 256 feature maps
For nonlinearity in network, ReLU (Rectified Linear Unit) is applied.
Max Pooling with 3*3 with stride 2
Conv with 384 filters of size 3*3 with 1 stride that generate 384 feature maps
For nonlinearity in network, ReLU (Rectified Linear Unit) is applied.
Max Pooling with 3*3 with stride 2
Conv with 384 filters of size 3*3 with 1 stride that generate 384 feature maps
For nonlinearity in network, ReLU (Rectified Linear Unit) is applied.
Max Pooling with 3*3 with stride 2
Conv with 256 filters of size 3*3 with 1 stride that generate 256 feature maps
For nonlinearity in network, ReLU (Rectified Linear Unit) is applied.
Max Pooling with 3*3 with stride 2

Fully connected layer with 4096 neurons each for adding the operation that is used to attach the feature maps.

Stride Convolution: The feature map generated according to the network is reduced by the convolutional operations. Padding is done to the output images before performing convolution, as output image has to be of same size as that of input image [5]. But this padding may cause artifact in the input image. So, this network is designed with deconvolution layer to make the output size be similar to input size. This deconvolution layer not only decreases the artifacts as well as reduces the computational overhead by applying filters.

Rectified Linear Unit: Rectified Linear Unit (ReLU) are used in many CNN architectures as an activation function for the network. In this activation function, the negative coefficient are replaced with zero value which is represented by the local features of the input image. The function is represented as:

\[
f(x) = \begin{cases} 
0 & \text{for } x < 0 \\
x & \text{for } x \geq 0 
\end{cases}
\]  

Some of the neurons dropped because they do not contribute to forward passage and do not participate in back propagation. Every time an input is presented, the neural network analyzes another architecture, but all these architectures share a common weight. This technique reduces the complex adaptations of neurons because a neuron cannot rely on the presence of some other neurons.
The proposed CNN Learner is designed to extract and learn features of watermarked image I(x,y). During training of the network, the weight functions are updated according to loss function. The loss function used here is stated as:

$$L_s = \frac{1}{N} \sum_{i=1}^{N} (y_i - \hat{y}_i)^2$$

Where, $L_s$ = Structural Similarity
The total weight for each pixel is evaluated by multiplication of $W_i(x,y), W_h(x,y)$:

$$W_{CNN} = W_i(x,y) + W_h(x,y)$$

Where, $W_i(x,y)$ = Weight extracted out of low frequency component $W_h(x,y)$ = Weight extracted out of high frequency component $W_{CNN}$ = Weight of CNN features

Pooling Layer: The pooling layer is simply there to reduce the dimensionality of the previous layer so it is a more appropriate size for the next layer of the network. Typically, this is done with max-pooling, which takes the maximum value of the window the filter is looking at, convolved across the image. A CNN can have any number of convolutional and pooling layers, in any order, with the only limitations being computation power and time, and the risk of overfitting.

Fully-Connected Layer: The fully connected layer is a regular neural network and is typically used as the final step in a convolutional neural network being used for image classification, where the desired output is an m element array (with m being the number of categories of images) containing probabilities of the image being of a particular category.

The Watermark embedding process includes the following steps (as in Figure 1):

- The video is divided into image frames. RGB frames are converted to YUV frames.
- For watermarking purpose the 2-level DWT-DCT is applied.
- The RGB watermark image is converted to a YUV image. The pixels of the watermark are nested with the weighted CNN function of x in the middle band of the wavelet transformation. The integration equation is:

$$I_{1i}=I_{1i}+x*W_{image}$$

Where, $x$ = magnitude factor which is used to specify the strength of the embedded data.

$W_{image}$ = CNN feature of watermarked image.
$I_{1i}$ = Video frames Y or U components.

The inverse DWT is used to maintain the watermark component of the frame. Finally, watermarked video is obtained from watermarked frames.

Further CNN is trained/learned

Procedure: Multiple Image Video Watermarking Embedding
Divide the video into RGB frames ($V_{RGB}$)
Input images $image1$ and $image2$ for watermarking
For each frame do $V_{YUV} = \text{Convert RGBYUV}(V_{RGB})$

$$Y = 0.299 * R + 0.587 * G + 0.114 * B;$$
$$U = -0.14713 * R - 0.28886 * G + 0.436 * B;$$
$$V = 0.615 * R - 0.51499 * G - 0.10001 * B;$$

Extract Y and U component from $V_{YUV}$

$V_Y = V_{YUV}(:,:,1);$
$V_U = V_{YUV}(:,:,2);$
Apply the DCT-DWT-DWT transform in $V_Y$ and $V_U$ component of $V_{YUV}$
To embed the watermark select following sub-bands $[LH21, HH21, LH22, HH22, LL23, HL23, LL24, HL24]$ Vectorize the image 1 and image 2
Rebuild the sub-bands using equation

New$V_Y = \text{Old$V_Y + K*CNNfeatureimage1}$
New$V_U = \text{Old$V_U + K*CNNfeatureimage2}$

Where $K$ = Gain Factor

Apply inverse DCT-DWT-DWT transform in New$V_Y$ and New$V_U$
End For

C. Watermark Extraction Algorithm
The steps used to extract the watermark are the same as the embedding steps, but in the opposite direction as follows (as shown in Figure 3):

- Watermarked video is converted into images. Each RGB frame is converted into a YUV representation.
- DCT and 2-level DWT Daubechies are applied to intermediate sub-colors.
- The following equation is used to extract the watermark:

$$W = \frac{I_{ref} - I_i}{x}$$

The extracted watermark is compared to the original watermark as follows:

$$NC = \frac{\sum_i \sum_j (w(i,j) * w'(i,j))}{\sum_i \sum_j w(i,j)^2}$$

Where, NC is the normalized correlation. The NC value is 1 if the watermark and the extracted watermark are identical and not opposite direction as follows (as shown in Figure 3):
For each frame do
Apply the DCT-DWT-DWT on frames Y and U component of the video frame
Image1=(NewV_Y - OldV_Y)/K;
Image2=( NewV_U - OldV_U)/K;
Rebuild Original Image
End for

D. Performance Measures
The robustness of the watermark means that the watermark will not be destroyed after intentional or involuntary attacks and can still be used for certification. Some of the performance parameters are discussed below:

Mean Square Error (MSE)
It is represented as:

\[ MSE = \frac{1}{XY}\sum_{i=1}^{X}\sum_{j=1}^{Y}[(c(i, j) - e(i, j))] \] (8)

Where,
X and Y are the height and width of the image.
C (i, j) is the pixel value of the cover image
x(i, j) is the pixel value of the embedded image.

Peak Signal to Noise Ratio (PSNR)
PSNR represents the degradation of the output image with input images. It is expressed as a decibel scale. Higher the value of PSNR higher the quality of image. PSNR is represented as:

\[ PSNR = 10\log_{10}(\frac{X \times Y}{MSE}) \] (9)

Where,
X and Y are height and width respectively of the image.
MSE= Mean Square Error between enhanced image and reference images

Magnitude Factor (α)
The magnitude factor is used to specify the strength of the embedded data. It is calculated as:

\[ I_i = I_i + x \times W_{image} \] (10)

Where,
x = magnitude factor.
W_{image} = CNN feature of watermarked image.
I_i = Video frames Y or U components.

IV. RESULT ANALYSIS
In this research work following analysis are performed:
i. To analyze the performance of proposed algorithm without attack with different images as well as video.
ii. To analyze on Different Attacks such as Gaussian noise, Poisson Noise, Salt and pepper Noise, etc.
iii. To compare with some existing work.
The table 5.1-5.3 shows the result of proposed algorithm by applying CNN-DCT-2DWT methodology.

| Images       | Videos | MSE      |
|--------------|--------|----------|
| Image 1 (256×198) | video 1 | 0.000039 |

Table 5.1 represents the MSE evaluation of proposed methodology for different images.

| IMAGES | VIDEOS | PSNR  |
|--------|--------|-------|
| Image 1 (256×198) | video 1 | 92.12 |
| Image 2 | (1.5 MB) | 72.9491 |
| Image 3 | video 1 | 93.01 |
| Image 1 | video 1 | 51.13 |

Table II represents PSNR evaluation of proposed methodology for different images.

| Images       | Videos | Embedding Time (in sec) | Extraction Time (in sec) |
|--------------|--------|------------------------|--------------------------|
| Image 1 (256×198) | video 1 | 25.34 | 12.95 |
| Image 2 | (1.5 MB) | 25.312 | 12.947 |
| Image 3 | video 1 | 26.11 | 14.20 |
| Image 4 | video 1 | 25.82 | 14.23 |

Table III represents time evaluation of proposed methodology for different images.

| Images       | Videos | PSNR  |
|--------------|--------|-------|
| Image 1 | video 1 | 45.887 | 28.038 | 13.68 |
| Image 2 | video 1 | 45.887 | 26.011 | 12.80 |

Table IV show the result analysis of proposed algorithm under mean attack.

| Images       | Videos | PSNR  |
|--------------|--------|-------|
| Image 1 | video 1 | 45.887 | 28.038 | 13.68 |
| Image 2 | video 1 | 45.887 | 26.011 | 12.80 |

Table V: Analysis of Proposed Algorithm under Median Attack
Table V shows the result analysis of proposed algorithm under median attack.

Table VI: Analysis of Proposed Algorithm under Rotation Attack

| Images | Videos | PSNR | Embedding Time (in sec) | Extraction Time (in sec) |
|--------|--------|------|-------------------------|--------------------------|
| Image 1 | video 1 | 40.6407 | 21.86 | 12.96 |
| Image 2 | video 1 | 40.6399 | 21.735 | 14.194 |

Table VI shows the result analysis of proposed algorithm under rotation attack.

Table VII: Analysis of Proposed Algorithm under Salt & Pepper Noise Attack

| Images | Videos | PSNR | Embedding Time (in sec) | Extraction Time (in sec) |
|--------|--------|------|-------------------------|--------------------------|
| Image 1 | video 1 | 76.99 | 30.200 | 18.54 |
| Image 2 | video 1 | 75.9912 | 35.615 | 13.487 |

Table VII shows the result analysis of proposed algorithm under salt and pepper noise attack.

Table VIII: Comparative Analysis of Proposed Algorithm under Gaussian Noise Attack

| Images | Videos | PSNR | Embedding Time (in sec) | Extraction Time (in sec) |
|--------|--------|------|-------------------------|--------------------------|
| Image 1 | video 1 | 91.88 | 80.49 | 12.82 |
| Image 2 | video 1 | 91.8848 | 56.35 | 13.58 |

Table VIII shows the result analysis of proposed algorithm under gaussian noise attack.

Table IX: Analysis of Proposed Algorithm under Poisson Noise Attack

| Images | Videos | PSNR | Embedding Time (in sec) | Extraction Time (in sec) |
|--------|--------|------|-------------------------|--------------------------|
| Image 1 | video 1 | 33.827 | 74.25 | 23.62 |
| Image 3 | video 1 | 33.827 | 74.25 | 23.62 |

Table IX shows the result analysis of proposed algorithm under poisson noise attack. After analyzing different attacks it has been concluded that the proposed algorithm is robust in nature.

A. Comparative Analysis

In [1] author proposed an invisible digital watermarking algorithm on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains is presented. Herein, a binary watermark image was embedded in the middle sub-band coefficients of a video stream. The experimental results of proposed algorithm indicate that the PSNR values of the watermarked videos were as high as almost up to 37 dB with the optimal watermarking strength. Magnitude factor is used for evaluation which is used to specify the strength of the embedded data.

Now the comparative analysis is performed with some of the existing work which are shown below in Table 5.10.

Table X: PSNR Analysis of Proposed Algorithm with Existing Work

| Magnitude Factor (α) | PSNR |
|----------------------|------|
| Proposed Work        | Existing Work [1] |
| 12                   | 48.2974 | 40.4370 |
| 14                   | 43.5215 | 39.1008 |
| 16                   | 43.2999 | 37.9538 |
| 18                   | 43.2768 | 36.9352 |
| 20                   | 39.4235 | 36.0270 |

Figure 4 shows the comparative PSNR value of proposed methodology as well as existing methodology. The result shows better PSNR value with magnitude factor (α) =12.
V. 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 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 techniques.

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.

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. 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. 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., Aho, 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, Khow. Rasem., “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, Sonika Jindal, “A Semi Blind DWT-SVD Video Watermarking”, Procedia Computer Science, Vol. 46, pp. 1661-1667, 2015.
[11] Aparna J R, Sonal Ayyappan, “Image Watermarking using Diffie Hellman Key Exchange Algorithm”, International Conference on Information and Communication Technologies, 2014.
[12] Adamu Muhammad Buhari, Huo-Chong Ling, Vishnu Morn Baskaran, KokSheik Wong, “Fast Watermarking Scheme for Real-time Spatial Scalable Video Coding”, Image Communication, 2016.