I.J. Intelligent Systems and Applications, **2025, 2, 31-41**
Published Online on April 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2025.02.03

Copyright Protection and Illegal Distributor Identification for Video-on-demand Applications using Forensic Watermarking

Ayesha Shaik*
Center for Cyber Physical Systems,Vellore Institute of Technology, Chennai, 600127, India
E-mail: ayesha.sk@vit.ac.in
ORCID iD: https://orcid.org/0000-0002-9804-8031
*Corresponding author

Masilamani V.
Computer Science and Engineering, Indian Institute of Information technology, Design and Manufacturing Kancheepuram, Chennai, 600127, India
E-mail: masila@iiitdm.ac.in
ORCIDiD: https://orcid.org/0000-0002-0664-1023

Received: 01 September 2024; Revised: 15 November 2024; Accepted: 20 December 2024; Published: 08 April 2025

Abstract: In the direct-to-home (DTH) environment video-on-demand (VOD) applications are tremendously popular due to its inexpensive and convenient nature. In VOD approach legal customers can connect their set-top boxes (STB) to the Internet and can access or record the available content. Due to the easy transmission of the highest quality digital data to the customers by the pay-per-view approach, the data are highly at risk. The data can be vulnerable for illegal distribution of duplicate copies and they are prone to unnecessary modifications which creates a financial loss to the information creators. So it is necessary to authenticate the owner as well as the illegal distributor to reduce the digital piracy which is the motivation for this work. This paper presents a forensic watermarking scheme for protecting copyrights, and for identifying the illegal distributor who distributes the legal copy in the illegal fashion though it is copyright violation. In this paper, two watermarks are embedded in the video that is on-demand, where one watermark is the owner's information and another watermark is related to the unique information of the STB. This work is also suitable for the biomedical domain, where one watermark can be the patient information and another watermark will be the health center information, in order to secure the patient information and the hospital information.

Index Terms: DWT, DCT, PPLU Decomposition, Forensic, Digital Watermarking.

1. Introduction

In the present decade the VOD applications are becoming extremely popular in the DTH environment with the high speed Internet services and technologies. The videos or movies can be accessed whenever we want and how many times we want. The access to select the videos that want to watch, which is convenient in time and location, and highly inexpensive features [1] are the reasons in increasing popularity of VOD applications. The videos will be transferred to the customers based on the request made by the viewers through the STB (interface between home TV and video subscriber environment) information.

A simplified block diagram of video subscriber network (VSN) to home connection is shown in Fig. 1. The flow diagram of the video on demand access has been shown in Fig. 2. In this figure it has been shown that after accessing content from the server the legal customers (LC) can make illegal copies for redistribution or some attacks can be done in order to defame the information creators (ICR) or owners. According to the survey done by the Asia Pacific Economic Cooperation (APEC) film industry revenues fell enormously [2] due to illegal copies. So we need to protect the copyrights of the IC and also we need to protect the information of LC. Forensic watermarking is one of the solutions to find out the source of illegal distribution [3].

Forensic watermarking is helpful in these criteria to identify the LC or authenticate the ICR. Digital piracy [4-7] is one of the main issues faced by the information creators and it happens due to the LC. The legal users who want to

watch the video has to purchase the video by pay-per-view approach and they have permission to watch the video but not to modify or redistribute it. If the user redistributes or modifies then it is a crime as it will lead to the financial loss of the companies. If we consider the digital pyramid [8], the number of file sharers or downloaders of the content is huge in number compared to the file suppliers as shown in Fig. 3. So, we need to find out the illegal source to prevent financial loss to the data content owners. In this paper, a forensic watermarking technique for VOD applications is proposed. In the existing method, watermarking technique using discrete wavelet transform (DWT), partial pivoting lower and upper triangular (PPLU) decomposition and singular value decomposition (SVD) is presented [9]. The main problem in this technique is it is prone to false positives due to the usage of SVD [10]. So here a forensic watermarking method which is false positive tolerant is proposed for authentication of ICR and illegal sources of distribution.

Fig.1. Home to video subscriber connection

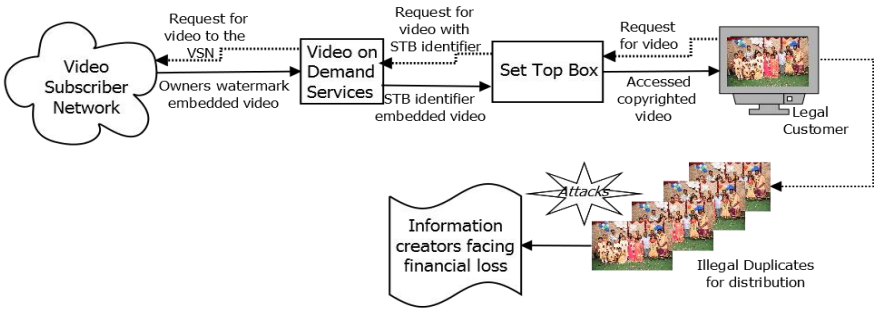


Fig.2. Flow diagram for forensic watermarking in Video-on-demand applications

The existing works focuses either on secure streaming or ownership identification but not on both applications. So, this way the necessity of the proposed technique justifies according to the objective. The problem articulated in the proposed work is that a watermarking scheme which will be helpful to identify the rightful owners and also supports secure video-on-demand applications. The existing works focuses either on secure streaming or ownership identification but not on both applications. So, this way the necessity of the proposed technique justifies according to the objective.

The purpose of the proposed work is to authenticate the set top box owner and to identify the illegal distributor. The novelty is that the set top box information is used in order to identify the illegal distributor. This paper is organized as follows: Section 2 gives a survey of existing watermarking algorithms. Section 3 describes proposed watermarking method. Section 4 presents an experimental analysis of proposed method followed by the conclusion.

2. Related Works

The Nexguard solutions [11] are providing forensic watermarking (FW), for digital cinema initiative specification. FW is provided in 100000 screens, 1M DVD screeners, more than 1000 eScreeners and STBs by Nexguard. In [11], a cost effective watermarking for broadcast environment is provided. In [12], statistical tools for identifying digital forgeries are discussed. A digital forgery identification method based on color filter array is presented [13]. Digital camera identification based on sensor noise patterns are discussed in [14]. The useful traces for digital forensics generated during acquisition are discussed in [15].

The traces will appear on different levels such as scene level, signal level and data structure level, and depending on device characteristics. Watermarking schemes are classified based on (i) embedding domain: spatial and transform, (ii) visibility of watermark: visible and invisible, (iii) embedding method: additive and multiplicative, and (iv)

requirement of original image during watermark extraction: non-blind and blind watermarking. Transform domain watermarking schemes are preferred due to its robust nature against attacks. Invisible watermarking schemes will not have visual disturbance in the watermarked content compared to the visible watermarking schemes. So, with respect to the visibility of the watermark, watermarking schemes are applied depending on the application.

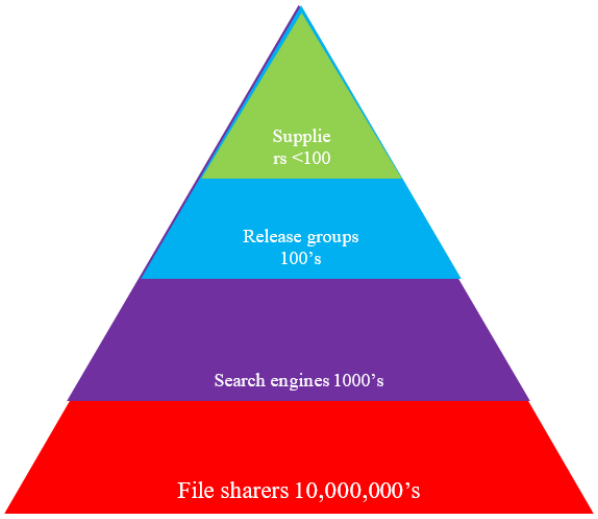


Fig.3. Pyramid of digital piracy [8]

A video watermarking method depending on scene change detection and pixel adjustment is proposed in [4]. A semi-fragile watermarking algorithm using discrete cosine transform and compressive sensing has been proposed in [3].

The sensitivities related to consumer and ethical scenario for digital piracy of MP3 data is discussed in [16]. Here, ethical orientation is mainly depended on expenses, outcomes and ethical opinions of downloading. The assumption for illegal downloading of MP3 files is that the people are not willing to steal CDs from the shops. Because the likelihood of getting caught and punished is high in CDs scenario compared to the illegal downloading of MP3 files.

The people who download the digital content have the mindset that if the people are doing it and not getting punished why they should not participate as there no strict preventive measures and punishments by law. In [16] it is clearly mentioned that the downloading intentions and consequences of getting caught in illegal download are negatively correlated. The study of the several digital watermarking schemes which are robust and secure is discussed in [17].

The analysis of hybrid Singular value decomposition based watermarking schemes is presented in [18]. The survey of robust watermarking methods for depth based images, screen content images, an high dynamic range images are proposed in [19]. The authors used the training in single stage and multiple stages for watermarking based on the utilization of neural networks. The authentication of the intellectual property rights of deep neural networks was proposed in [20] as it is a pressing need in the present scenario.

PPLU Decompostion

PPLU decomposition [9] is a factoring technique to obtain lower triangular and upper triangular matrices of a matrix using partial pivoting (PP) procedure. This factorization outputs three matrices such as lower triangular matrix (*L*), upper triangular matrix (*U*) and a permutation matrix (*P*) which is obtained from row changes of matrix (*C*) during PP procedure. PPLU decomposition of C is defined as follows: *PPLU(C) = (L, U, P)* such that *PC = LU*. An illustrated example for PPLU decomposition of a 3x3 matrix is given below. Let

$$C=\begin{bmatrix}1 & 0 & 4\\ 0 & 0 & 1\\ 3 & 2 & 13\end{bmatrix}$$

Then *C* can be decomposed into

$$P=\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix} \quad L=\begin{bmatrix}1 & 0 & 0\\ 3 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \quad U=\begin{bmatrix}1 & 0 & 4\\ 0 & 2 & 1\\ 0 & 0 & 1\end{bmatrix}$$

$$P\ x\ A=\begin{bmatrix}1 & 0 & 4\\ 3 & 2 & 13\\ 0 & 0 & 1\end{bmatrix} \quad L\ x\ U=\begin{bmatrix}1 & 0 & 4\\ 3 & 2 & 13\\ 0 & 0 & 1\end{bmatrix}$$

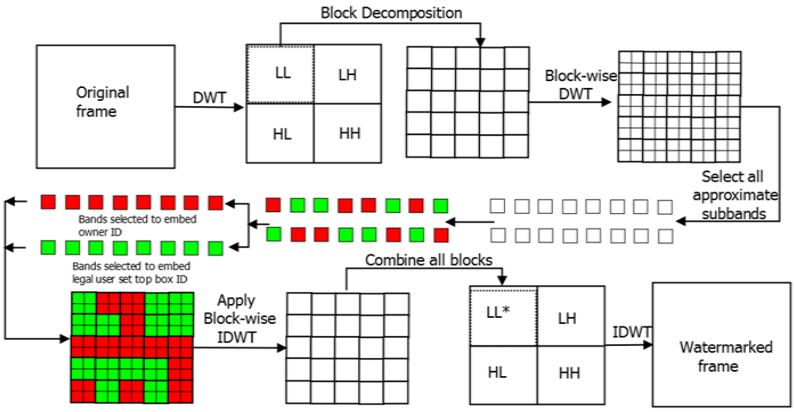


Fig.4. Block diagram for proposed watermarking method

3. Proposed Approach

In this section, a digital video forensic watermarking method for VOD access is presented. The proposed block diagram is shown in Fig. 4. In this approach two WMs are embedded into the video, one for authenticating ICR and other is to identify the illegal distributors (IDBR). For owner authentication, the unique information related to the owner is used and for IDBR identification STB ID is used. For each video before sending to the viewer, initially the significant frames in the video are obtained. On those frames a DWT operation is performed to decompose into 4 sub bands. Then the approximate sub band is divided into 8×8 blocks. On each block DWT is performed and again decomposed into 4 sub bands. Now let us assume the number of 8×8 blocks are N. If we apply DWT on these N blocks, we will get N approximate sub bands of size 4×4. Using a secret key (generated by Gollman cascade feedback carry shift register [21]) known to the owner, select N/2 sub bands randomly for embedding ICR information, and the remaining N/2 sub bands for inserting STB ID. The proposed watermarks embedding algorithm for Video on Demand application is given in Algorithm 1. The secret key is generated using Gollman cascade linear feedback shift register which is a random number generator. The secret key selection is essential in the way watermark is embedded making it secure. If the secret key is emitted, the portions selected for watermarking will vary and vulnerable for third party attacks.

Algorithm 1: Proposed VOD watermark embedding

Input:	Original Video V, Watermarks W_{ICR} and W_{STB}
Output:	Watermarked Video (V_w)
Step 1:	Select significant frames F_i $(1 \le i < S)$, using absolute histogram difference between the consecutive frames, where S is total number of frames in the video
Step 2:	Apply DWT to F_i $\mathrm{DWT}(F_i) = (\mathrm{LL}_{F_i}, \mathrm{LH}_{F_i}, \mathrm{HL}_{F_i}, \mathrm{HH}_{F_i})$
Step 3:	Divide LL_{F_i} into 8×8 blocks
Step 4:	On every block (assume N blocks) perform DWT to obtain sub bands $\mathrm{DWT}(\mathrm{LL}_{F_i}{}^m) = (\ BLL_{F_i}^m,\ BLH_{F_i}^m, BHL_{F_i}^m, BHH_{F_i}^m)$, where $1 \le m \le N$
Step 5:	Use secret key K to randomly select $N/2$ sub bands from $BLL_{F_i}^m$ where $1 \le m \le N$.
Step 6:	Say selected sub bands are $BLL_{F_i}^{m1}$ and remaining are $BLL_{F_i}^{m2}$, $m1 = m2; 1 \le m1, m2 \le N/2$
Step 7:	$BLL_{F_i}^{m1}$ is used to embed W_{ICR} and to obtain $BLL_{F_i}^{m1^{ICR}}$. (*Go to Algorithm 2*)
Step 8:	$BLL_{F_i}^{m2}$ is used to embed W_{STB} and to obtain $BLL_{F_i}^{m2^{STB}}$. (*Go to Algorithm 3*)
Step 9:	Then perform inverse DWT for all these sub bands $BLL_{F_i}^{m1^{ICR}}$ and $BLL_{F_i}^{m2^{STB}}$ to obtain watermarked approximated sub band $LL_{F_i}^{m^W}$
Step 10:	Then perform inverse DWT for the watermarked sub band $LL_{F_i}^{m^W}$, $\mathrm{LH}_{F_i}, \mathrm{HL}_{F_i}, \mathrm{HH}_{F_i}$ to obtain V_W

The proposed ICR watermark embedding algorithm for Video on Demand application is given in Algorithm 2.

Algorithm 2: Proposed ICR watermark embedding	
Input:	Input sub band $BLL_{F_i}^{m1}$, watermark W_{ICR}
Output:	Watermarked Sub band $BLL_{F_i}^{m1^{ICR}}$
Step 1:	$BLL_{F_i}^{m1^{ICR}}(p,q) = BLL_{F_i}^{m1}(p,q)(1+\alpha.W_{ICR}(p,q))$
Step 2:	Return watermarked sub band $BLL_{F_i}^{m1^{ICR}}$

The proposed STB watermark embedding algorithm for Video on Demand application is given in Algorithm 3.

Algorithm 3: Proposed STB watermark embedding	
Input:	Input sub band $BLL_{F_i}^{m2}$, watermark W_{STB}
Output:	Watermarked Sub band $BLL_{F_i}^{m2^{STB}}$
Step 1:	Perform PPLU decomposition on $BLL_{F_i}^{m1}$ to obtain three matrices L, U , P.
Step 2:	Find product of two matrices L and U, say Y
Step 3:	Now watermark first row of Y as shown. $Y_w = Y + W_{STB}$
Step 4:	Now find watermarked sub band as follows. $BLL_{F_i}^{m2^{STB}} = P^{-1} \times Y_w$
Step 5:	Return $BLL_{F_i}^{m2^{STB}}$ to the Algorithm 1.

The proposed watermark extracting algorithm for Video on Demand application is given in Algorithm 4.

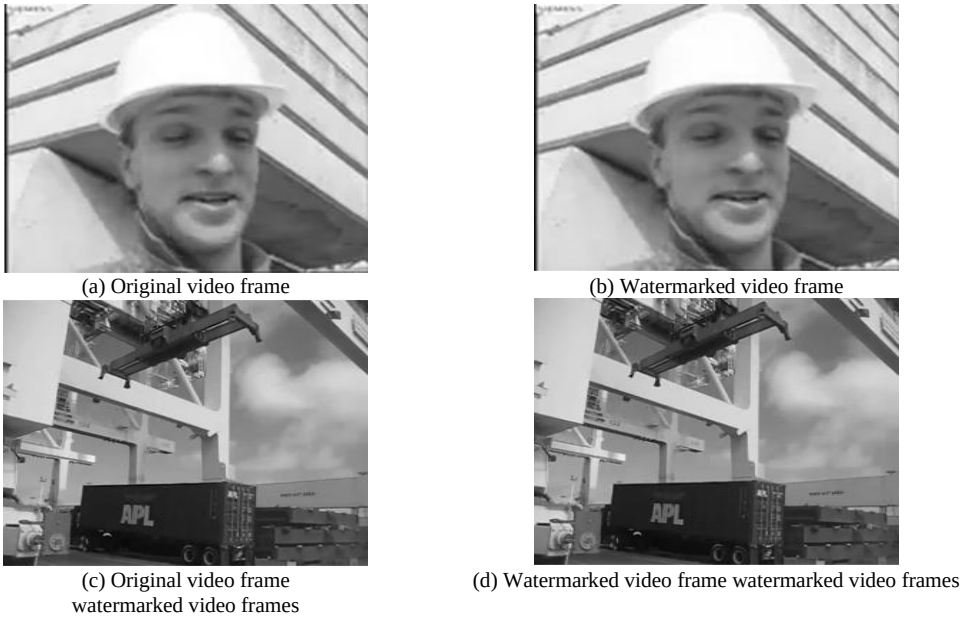
Algorithm 4: Proposed VOD watermark extraction	
Input:	Watermarked Video V_w^*
Output:	Watermarks W_{ICR}^* and W_{STB}^*
Step 1:	Select significant frames F_i^* $(1 \le i < S)$, using absolute histogram difference between the consecutive frames, where S is total number of frames in the video
Step 2:	Apply DWT to F_i^* $\mathrm{DWT}(F_i^*) = (\mathrm{LL}_{F_i}^*, \mathrm{LH}_{F_i}^*, \mathrm{HL}_{F_i}^*, \mathrm{HH}_{F_i}^*)$
Step 3:	Divide $\mathrm{LL}_{F_i}^*$ into 8×8 blocks
Step 4:	On every block (assume N blocks) perform DWT to obtain sub bands $\mathrm{DWT}(\mathrm{LL}_{F_i}^{m^*}) = (\ BLL_{F_i}^{m^*}, BLH_{F_i}^{m^*}, BHL_{F_i}^{m^*}, BHH_{F_i}^{m^*})$, where $1 \le m^* \le N$
Step 5:	Use secret key K to randomly select $N/2$ sub bands from $BLL_{F_i}^{m^*}$ where $1 \le m \le N$.
Step 6:	Say selected sub bands are $BLL_{F_i}^{m1^*}$ and remaining are $BLL_{F_i}^{m2^*}$, $m1^* = m2^*; 1 \le m1^*, m2^* \le N/2$
Step 7:	$BLL_{F_i}^{m1^*}$ is used to extract W_{ICR}^* . (*Goto Algorithm 5*)
Step 8:	$BLL_{F_i}^{m2^*}$ is used to extract W_{STB}^*. (*Goto Algorithm 6*)
Step 9:	Find correlation between W_{ICR} and W_{ICR}^*. If the value is high then owner is authenticated
Step 10:	Find correlation between W_{STB} and W_{STB}^*. If the value is high then legal customer is authenticated

The proposed ICR watermark extracting algorithm for Video on Demand application is given in Algorithm 5.

Algorithm 5: Proposed ICR watermark extraction	
Input:	Watermarked sub band $BLL_{F_i}^{m1^*}$,
Output:	Extracted watermark W_{ICR}^*
Step 1:	$W_{ICR}^*(p,q) = BLL_{F_i}^{m1^*}(p,q) - BLL_{F_i}^{m1}(p,q)/(\alpha.BLL_{F_i}^{m1}(p,q))$
Step 2:	Return watermark W_{ICR}^* to Algorithm 4

The proposed STB watermark extracting algorithm for Video on Demand application is given in Algorithm 6.

Algorithm 6: Proposed STB watermark extraction	
Input:	Watermarked sub band $BLL_{F_i}^{m2^*}$,
Output:	Extracted watermark W_{STB}^*
Step 1:	Perform PPLU decomposition on $BLL_{F_i}^{m2^*}$, to obtain three matrices L^*, U^* , P^*.
Step 2:	Find product of two matrices L^* and U^*, say Y^*
Step 3:	Now extract watermark from first row of Y^* as shown. $W_{STB}^* = Y^* - Y$
Step 4:	Return W_{STB}^* to the Algorithm 4.



(a) Original video frame (b) Watermarked video frame

(c) Original video frame watermarked video frames (d) Watermarked video frame watermarked video frames

Fig.5. Original and watermarked frames for foreman and container dataset videos

4. Results and Analysis

The proposed method has been experimentally tested on the foreman, container, sample, and VIRAT data set videos [22, 23]. The proposed method shows better PSNR and less BER compared to the method given in [9]. In this method, it requires three DWT, three SVD and one PPLU decomposition which will be time consuming. So a watermarking method which consumes lesser time compared to the method in [9] is proposed. Initially the significant frames are detected and then those frames are resized to 512×512. Then 1-level Haar DWT is applied on each detected frame for decomposing into [LLo LHo HLo HHo] sub bands. For embedding watermark LLo approximate sub band is selected because it is highly significant compared to the other three sub bands. The main reason for not selecting these three sub bands is if the attacker removes these three sub bands, then also the PSNR of the watermarked content will not degrade significantly which will be an advantage for the third parties.

The LLo sub band is again decomposed into 8×8 blocks. Then some 8×8 blocks are selected randomly for embedding owner information and remaining 8×8 blocks are selected for embedding set top box ID. The original video frames and watermarked video frames are as shown in Fig. 5.

Table 1. BER obtained for ICR and STB watermarks

Attack	BER between inserted and extracted owner ID	BER between inserted and extracted STB ID
Crop (10%)	0.0012	0.1064
HE	0.1196	0.08
SPN 0.005	0.0153	0.1133
SPN 0.001	0.0029	0.1076
GN(0,1)	0.2232	0.2221
GN(0,2)	0.2251	0.2257

The bit error rate (BER) obtained for proposed method for a list of attacks is tabularized in Table 1. The watermark embedding and extracting time for the existing and proposed methods is shown in Table 2. The PSNR between original video frame and watermarked video frame is listed in Table 3. The watermark embedding time and extracting time for

the proposed method is low as it uses only one DWT operation and one PPLU operation, but the existing method uses three DWT, one SVD and one PPLU decomposition which is time consuming.

Table 2. Watermark embedding and extracting time (in seconds)

Method	Watermark Embedding Time (in seconds)	Watermark extracting Time (in seconds)
DWT-SVD-PPLU [13]	0.93747	0.583262833
Proposed method	0.666501	0.2501415

In Table 3, the PSNR is obtained for dataset videos such as container, foreman and news videos. The proposed method provides high PSNR as the distortion done by the watermark to the original frame is low, compared to the existing technique.

Table 3. Watermark embedding time and extracting time (in secs)

Method	Container	Foreman	News
DWT-SVD-PPLU [13]	32.753	32.4432	33.8359
Proposed method	51.1816	51.2371	51.1819

The BER between inserted and extracted ICR id's for varying intensities of salt and pepper noise is plotted in Fig. 6.

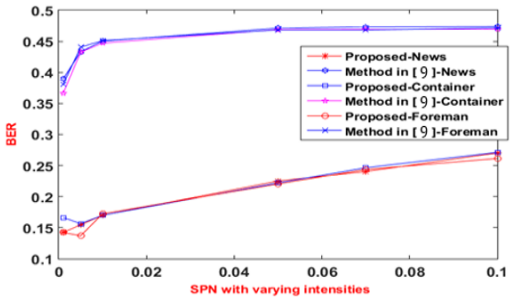


Fig.6. Varying intensities of SPN for for existing and proposed methods for dataset videos

In Fig. 6, the BER between the inserted and extracted owner's ID (B1), obtained for the News, Container and Foreman videos for the method given in [9] and the proposed method is shown. The X-axis presents the density of the salt and pepper noise attack (SPN) with varying intensities and the Y-axis presents the BER obtained for the owner ID (B1). The BER B1 for the proposed method is shown in between 0.13 to 0.285. The BER B1 for the existing method [9] is shown in between 0.36 to 0.45. From this Fig. 6, one can say that the proposed method performs better against SPN attack for ownership authentication as the BER obtained for proposed method is low compared to the existing method. The BER between inserted and extracted STB watermarks for varying intensities of salt and pepper noise is shown in Fig. 7. In Fig. 7, the BER between the inserted and extracted set top box's ID (B2), obtained for the News, Container and Foreman videos for the method given in [9] and the proposed method is shown. The X-axis presents the density of the salt and pepper noise attack (SPN) with varying intensities and the Y-axis presents the BER obtained for the set top box's ID (B2). The BER B2 for the proposed method is shown in between 0.225 to 0.3. The BER B2 for the existing method [9] is shown in between 0.36 to 0.45. From this Fig. 7, one can say that the proposed method performs better against SPN attack for illegal distributor authentication as the BER obtained for proposed method is low compared to the existing method.

The BER between inserted and extracted ICR id's for varying intensities of Gaussian noise is plotted in Fig. 8.

In Fig. 8, the BER between the inserted and extracted owner's ID (B3), obtained for the News, Container and Foreman videos for the method given in [9] and the proposed method is shown. The X-axis presents the density of the Gaussian noise attack (GN) with varying intensities and the Y-axis presents the BER obtained for the owner ID (B3). The BER B3 for the proposed method is shown in between 0.34 to 0.36. The BER B3 for the existing method [9] is shown in between 0.47 to 0.48. From this Fig. 8, one can say that the proposed method performs better against GN attack for ownership authentication as the BER obtained for proposed method is low compared to the existing method.

The BER between inserted and extracted STB watermarks for varying intensities of Gaussian noise is shown in Fig. 9. In Fig. 9, the BER between the inserted and extracted set top box's ID (B4), obtained for the News, Container and Foreman videos for the method given in [9] and the proposed method is shown. The X-axis presents the density of the salt and pepper noise attack (SPN) with varying intensities and the Y-axis presents the BER obtained for the set top box's ID (B4). The BER B4 for the proposed method is shown in between 0.225 to 0.3. The BER B4 for the existing

method [9] is shown in between 0.34 to 0.35. From this Fig. 9, one can say that the proposed method performs better against GN attack for illegal distributor authentication as the BER obtained for proposed method is low compared to the existing method.

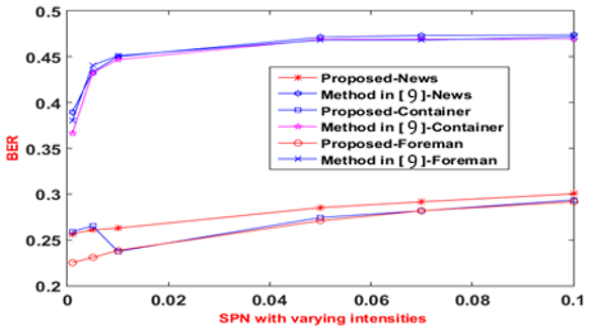


Fig.7. Varying intensities SPN STB ids for existing and proposed methods for dataset videos

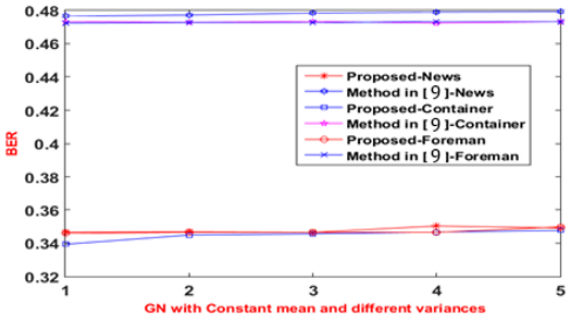


Fig.8. Varying intensities of GN

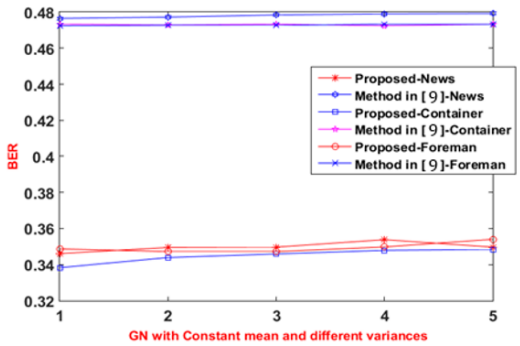


Fig.9. Varying intensities GN STB ids for existing and proposed methods for dataset videos

The paper mainly focuses on the BER and PSNR as both are essential to measure the performance of the watermarking that discloses the quality of watermarked image. Less PSNR value indicates the watermark embedding has degraded the quality of the image which is not suggestible. More PSNR is the indication of less degradation to the watermarked image. Addressing to the Robustness, In Table 2, the authors have listed the robustness of the proposed method against the attacks such as cropping, histogram equalization, salt and pepper noise, and Gaussian noise. The measure listed is BER, which is an indication of low bit error rate, then the authentication is done, otherwise not authenticated. BER is computed between the embedded watermark and the extracted watermark. The PSNR measure is required to obtain the similarity between the original image and watermarked image.

The watermark insertion time watermark extraction time in seconds for each dataset video are tabularized in Table 4 and Table 5. From Tables 4 and 5, we can see that the proposed method consumes lesser time compared to the existing methods.

Table 4. Watermark insertion time (seconds) for existing and proposed methods

Method	Container	Foreman	News
DWT-SVD-PPLU [13]	0.921587	0.9527	1.023605
Proposed method	0.815634	0.83696	0.91303

Table 5. Watermark extraction time (seconds) for existing and proposed methods

Method	Container	Foreman	News
DWT-SVD-PPLU [13]	1.348986	1.23609	1.284519
Proposed method	0.088774	0.08366	0.113006

Table 6. Comparison of proposed method with the existing methods

Images	[16]	[15]	Proposed	[14]
Foreman	32.41	44.39	51.23	32.57
Container	32.37	44.07	51.18	32.032
Sample	32.69	44.04	51.19	31.926

The visual quality of the watermarked image is compared with the existing methods and tabularized in Table 6. One can see that in Table 6, the PSNR of the proposed method is higher than the other existing methods. It is due to that in the proposed method, the amount of degradation done to the data is less.

Datasets [22] and [23] have been used for the implementation. The authors listed the results for average embedding time and extraction of the watermarks for the existing method and the proposed method for critical evaluation and validation.

Table 7. Comparison of the proposed method with other existing methods with the new Image quality measures

Method	Image Quality measure	Obtained value
Proposed method	FFT [17]	0.1084
	DCT	0.9648
	PSNR-HVS	50.23
Existing method [13]	FFT	0.0423
	DCT	0.9549
	PSNR-HVS	45.6688
Existing method [15]	FFT	0.0098
	DCT	0.3097
	PSNR-HVS	40.5233

In order to validate the visual quality of the proposed method, the method was further experimented with the no-reference image quality measures such as fast Fourier transform [24], discrete cosine transform [25] based measures and also with PSNR-HVS [26] image quality measure. The experimental values are listed in Table 7. In Table 7, FFT and DCT quality measures will output a score between 0 and 1. For DCT quality measure, higher the score, the image quality is good. But for FFT quality measure, it will give the score for the distortion measurement, higher the score, lower the distortion. One can see that in Table 7, FFT and DCT scores of the proposed method are higher than the existing methods. These two methods are no-reference quality measures. He PSNR-HVS is a reference quality measure ranging from 0 to 10000. As the technique now discusses on VOD, the results for biomedical domain not included and the work is still going on. The authors theoretically claim the method works for biomedical domain. The implementation for biomedical domain has to be done in the future after availing the datasets. As the technique proposed discusses watermarking technique for video on demand (VOD) applications and copyright protection, the authors have included the results only for VOD. Related to the biomedical domain, the work is yet to progress. Moreover, the biomedical domain is not associated with the VOD applications, the authors have not discussed extensively in the article as it is out of scope.

5. Conclusions

In this paper, a robust forensic watermarking for video on demand applications is proposed. Here two watermarks are embedded into the video that is on demand by the users. One watermark is embedded in order to authenticate the owner of the video and another watermark is embedded to identify the illegal distributor. This technique gives very less BER and high PSNR compared to the existing techniques. This technique can also be applied to the bio-medical domain, where one watermark can be the patient information and other watermark will be the information of the health care center or diagnostic center. The proposed method has been validated with the image quality measures such as PSNR and PSNR HVS measures. The proposed method has also been validated with the no-reference quality measures such as FFT and DCT measures.

References

[1] Amelia Groen. Why i demand more from my video on demand.
[2] APEC. 2011 cti report to ministers:effective practices for addressing unauthorized camcording.

[3] Mediasilo. Secure: Security, check- enterprise-grade security trusted by the biggest names in business and entertainment.
[4] Webroot. The Societal Costs of Digital Piracy.
[5] Shaifali M Arora Et Al. A Dwt-Svd Based Robust Digital Watermarking for Digital Images. Procedia Computer Science,132:1441–1448, 2018.
[6] Simon Stokes. Digital Copyright. 2014.
[7] NIdaa Hasan Abbas, Sharifah Mumtazah Syed Ahmad, Sajida Parveen, Wan Azizun Wan, And Abd Rahman Bin Ramli. Design Of High Performance Copyright Protection Watermarking Based On Lifting Wavelet Transform And Bi Empirical Mode Decomposition. Multimedia Tools and Applications, 77:24593–24614, 2018.
[8] TFE Times. The pyramid of internet piracy.
[9] Nazeer Muhammad and Nargis Bibi. Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. IET Image Processing, 9(9):795–803, 2015.
[10] Xiao-Ping Zhang and Kan Li. Comments on" an svd-based watermarking scheme for protecting rightful ownership". IEEE Transactions on Multimedia, 7(3):593–594, 2005.
[11] Nexguard. Nagra nexguard forensic watermarking.
[12] Alin C Popescu and Hany Farid. Statistical tools for digital forensics. In International workshop on information hiding, pages 128–147. Springer, 2004.
[13] Alin C Popescu and Hany Farid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10):3948–3959, 2005.
[14] Jan Lukas, Jessica Fridrich, and Miroslav Goljan. Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security, 1(2):205–214, 2006.
[15] Rainer B¨ohme, Matthias Kirchner, S Katzenbeisser, and F Petitcolas. Media forensics. In Information Hiding, volume 9, pages 231–259. Artech House, 2016.
[16] Steven Lysonski and Srinivas Durvasula. Digital piracy of mp3s: consumer and ethical predispositions. Journal of Consumer Marketing, 25(3):167–178, 2008.
[17] Mahbuba Begum and Mohammad Shorif Uddin. Digital image watermarking techniques: a review. Information, 11(2):110, 2020.
[18] Zurinahni Zainol, Je Sen Teh, Moatsum Alawida, Abdulatif Alabdulatif, et al. Hybrid svd-based image watermarking schemes: a review. IEEE Access, 9:32931–32968, 2021.
[19] Wenbo Wan, Jun Wang, Yunming Zhang, Jing Li, Hui Yu, and Jiande Sun. A comprehensive survey on robust image watermarking. Neurocomputing, 488:226–247, 2022.
[20] Yue Li, Hongxia Wang, and Mauro Barni. A survey of deep neural network watermarking techniques. Neurocomputing, 461:171–193, 2021.
[21] Xin Li, Yonatan Shoshan, Alexander Fish, and Graham A Jullien. A simplified approach for designing secure random number generators in hw. In 2008 15th IEEE International Conference on Electronics, Circuits and Systems, pages 372–375. IEEE, 2008.
[22] Virat. The virat video dataset.
[23] VIPSL. Database: Images video clips.
[24] Kanjar De and V Masilamani. Image sharpness measure for blurred images in frequency domain. Procedia Engineering, 64:149–158, 2013.
[25] Kanjar De and V Masilamani. Fast no-reference image sharpness measure for blurred images in discrete cosine transform domain. In 2016 IEEE Students' Technology Symposium (TechSym), pages 256–261. IEEE, 2016.
[26] Karen Egiazarian, Jaakko Astola, Nikolay Ponomarenko, Vladimir Lukin, Federica Battisti, and Marco Carli. New full-reference quality metrics based on hvs. In Proceedings of the second international workshop on video processing and quality metrics, volume 4, page 4, 2006.

Authors' Profiles

Dr. Ayesha Shaik received the Doctor of Philosophy (Ph.D.) degree from IIITDM Kancheepuram. She is currently an Associate Professor with the School of Computer Science and Engineering and is also associated with the Research Center for Cyber Physical Systems, Vellore Institute of Technology (VIT), Chennai Campus. Her research interests include image processing, digital image processing, watermarking, and deep learning.

Dr. Masilamani V. completed his Ph.D. in Computer Science and Engineering from Indian Institute of Technology, Madras. He pursued his M.Tech. in Computer Science & Data Processing from Indian Institute of Technology, Kharagpur. He is currently working as a Professor in IIITDM Kancheepuram. His research interests include Image Processing and Computer Vision, Machine Learning, Algorithms and Data Structures, and Theory of Computing. He is having experience of 15 years of teaching and research at IIITDM Kancheepuram.

How to cite this paper: Ayesha Shaik, Masilamani V., "Copyright Protection and Illegal Distributor Identification for Video-on-demand Applications using Forensic Watermarking", International Journal of Intelligent Systems and Applications(IJISA), Vol.17, No.2, pp.31-41, 2025. DOI:10.5815/ijisa.2025.02.03