Video Piracy Detection and Prevention

Sipna Lankepillewar^{#1}, Ankita Patil^{#2}, Shashank Pandey^{#3}, Shubham Patil^{#4}, B. D. Shendkar^{#5}

[#]Department of Computer Engineering, Sinhgad Institute of Technology and Science, Savitribai Phule Pune University, Pune

¹sipnalankepillewar@gmail.com
 ²ankulipatil56@gmail.com
 ³shashankpandey1102@gmail.com
 ⁴sjpatil98@gmail.com
 ⁵bhagyashree.d.shendkar@gmail.com

Abstract

Piracy is an important issue as far as the manufacturers are concerned as it can result in a huge revenue loss. The reason behind the practice of full-scale piracy is mainly due to the difficulty involved in tracking the source responsible for the piracy. The aim of this paper is to use digital watermarking techniques to detect video piracy and avoid those pirated videos from being uploaded. A digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect. A digital watermark when embedded into a video or image does not alter the data. The information watermarked includes owner, recipient and distributor details, transaction dates, serial numbers, etc. which play an important role in determining the source of piracy.

Keywords - Watermark, DWT, Fingerprinting, Piracy.

The paper is organized as follows. Section I describes the Introduction of the proposed system. The motivation behind this proposed work is mentioned in Section II. Section III presents the related work of the system. The proposed system is described briefly in Section IV. Future scope of the proposed system is listed in Section V. Section VI presents the conclusion of the paper.

I. INTRODUCTION

Digital multimedia is widely used in our daily life. However, their authenticity cannot be taken for granted with the advent and growing popularity of various sophisticated editing software. Therefore, effective technique methods for multimedia forensics are in great demand. Many types of websites offer users the ability to upload video content. Site like YouTube exist solely for this reason, but many social networking sites also allow this capability. The immense popularity of such sites has attracted their content producers who are getting serious about protecting their copyrights and putting real pressure on the owners of these types of sites to eliminate illegal infringement. A large amount of copyright protected material from clips from movies and TV shows to music and music video is readily available for download by visitors to these types of online video hosting services. While the site operators claim that they are operating under the Fair Use doctrine, content producers and large media companies aren't buying it. They have deep pockets and armies of lawyers at their disposal, and they are gearing up to take legal action. With the advancement in technology the distribution of video data is much easier and faster. Since digital video sequences can be easily manipulated,

concerns regarding authentication of the digital video are increasing. In situations where the video data should be credible, that is when it needs to be used as evidence, this issue becomes serious. So we need authentication techniques to maintain authenticity, integrity, and security of digital video content. A digital watermark is a distinguishing piece of information that is embedded in the data that it is intended to protect. By adding a transparent watermark to the multimedia content, we can verify the ownership of the digital media and detect video piracy.

II. MOTIVATION

The extent of piracy is most frequently measured in monetary term, revenues that might otherwise have resulted from the authorized sale of the goods that were illegally copied instead. In day to day life, Internet is an important channel for digital source, but many intruders are misusing by constructing illegal copies and leaking the information which creates bad environment in the film industry. The threat that there are number of perfectly congruent copies of audio, video and image in the file led to the urge of preventing piracy.

III. RELATED WORK

HouriaKelkoul et.al.[1] proposed an idea of preventing piracy by combining both audio and video streams. Video watermarking consists of adding a pattern of bits that is unnoticeable to the human eye, into the video file which you want to authenticate. Video fingerprinting is a technique in which software identifies, extracts, and then compresses characteristic components of a video, enabling that video to be uniquely identified by its resultant "fingerprint". Video fingerprinting is technology that has proven itself to be effective at identifying and comparing digital video data. Also, digital video fingerprinting enables to recognize videos with a different resolution compared with the original (smaller or larger), and to recognize videos that have been modified slightly (blurring, rotation, acceleration or deceleration, cropping, insertions of new elements in the video), and videos where the audio track has been modified. Characteristics such as audio data is extracted, analyzed and transformed into a fingerprint matrix so that a movie can be identified after use or alteration.

The approach represents the system which is designed to detect pirated videos and prevent them from piracy. Khushboo Choudhary[2] proposed this system uses digital watermarking and hashing techniques for the same. The objective is to create a web server in which user can upload, download and play media content. When an user uploads a video on this server, the system will embed a watermark in the video for key frames extraction and generate hash keys for the video which will be stored in the database. When some other user wants to upload video its hash keys will be matched with the database and if it matches the video cannot be uploaded and the user will be notified about this. if the video is cropped, match percent will be checked and if it exceeds.

To implement the proposed system Anjali Tiwari[3] et.al. has proposed a system to detect video piracy using invisible watermark. Invisible Digital Watermarking is a technique of steganography. Invisible Digital Watermarking is a technique of steganography to manipulate frames of the video by modifying the pixels scattered across the frame . The detection of video piracy is relatively easier, simpler and secure due to the password protected key which is available only to the owner of the video. However, it is quite difficult to implement and if the password key gets leaked then it may create a problem.

The machine learning approach used by Nilesh Kumar Dubey[4] et.al. has presented various techniques to prevent camcorder piracy in theaters as a new application of the watermarking technique. Every technique has their MAE (mean absolute error) for the final result. This paper helped us understand how pirates can be tracked. Paper gave us basic understanding of how a video can be embedded with watermark. Process of tracking down of pirate is illustrated which consists of several steps such as recovery of watermark from pirated video(distorted), extracting the watermark, estimating position of pirate using LACF is introduced in this paper. Also, basic audio and video watermark techniques are discussed. Difficulties in embedding Watermark in video are discussed. Overall this paper helped us to understand Piracy Source and various techniques to track it.

Hamid Shojanazeri[5] et,al. proposed how to analyze the different techniques of Watermarking and also discussed about relative requirements about watermarking techniques. Each Watermarking technique is compared with each other on the basis of effects of requirements on techniques with same data set. The main requirements are fidelity, speed, robustness, use of key, capacity, real-time detector capacity. In spatial domain, there is least significant bit technique ,and in frequency domain there is discrete cosine transform technique for Watermarking, techniques based on MPEG coding .

Ref.	Highlights	Observations
No.		
[1]	It presents a survey of various techniques such as digital watermarking and fingerprinting for the detection of pirated videos.	Various techniques such as digital watermarking and fingerprinting are discussed based on their performances but implementation is not given and there is scope of optimization.
[2]	It proposes a system to detect and prevent pirated videos using digital watermarking and hashing techniques.	The system maintains privacy of owner. But if the match percent is less than 65% then piracy will not be detected and video will be successfullyuploaded.Video of only compatible formats can be uploaded.
[3]	It presents the notion of Watermarking and the features required to design a watermarked video for piracy deterrence.	Several watermarking techniques are studied. Techniques to track down the pirate are illustrated.Watermark needs to be recovered in order to extract payloads.Embedding Watermark can degrade acoustic quality.
[4]	The aim of this paper is to detect pirated videos using invisible watermark. Invisible Digital Watermarking is a technique of steganography	Watermarks cannot be leaked to other person as they are invisible. The detection of video piracy is easier, simpler and secure due to the password protected key which is available only to the owner of the video. The proposed system is difficult to implement and creates a problem if password key is leaked.

TABLE I Summary

[5]	The aim of this paper is to detect pirated	Various techniques based on domain are
	videos using invisible watermark. Invisible	discussed. Not enough attention is devoted to
	Digital Watermarking is a technique of	computational complexities and time of
	steganography	extracting algorithms.

IV. PROPOSED SYSTEM

A system architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

The below figure explains the working of the system. The video uploaded on website(channels) like telegram are examined and then features are extracted like watermark. Release date of video is checked. If video is released before official date of release then it is detected as pirated and permanently source of website is blocked. If video is released after official date of video release then according to DWT(Discrete Wavelet Transform) the position of watermark is compared with the actual position of watermark stored in key file, If the match is found for position then video is from official source otherwise it is from illegal source.

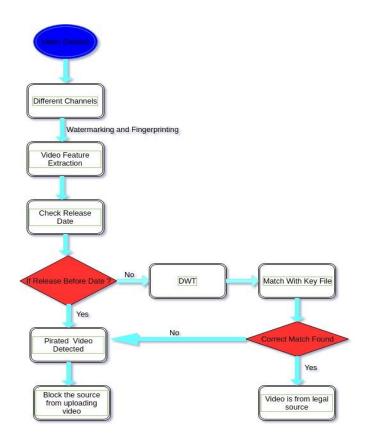


Fig. 1 System flow for video piracy detection and prevention system

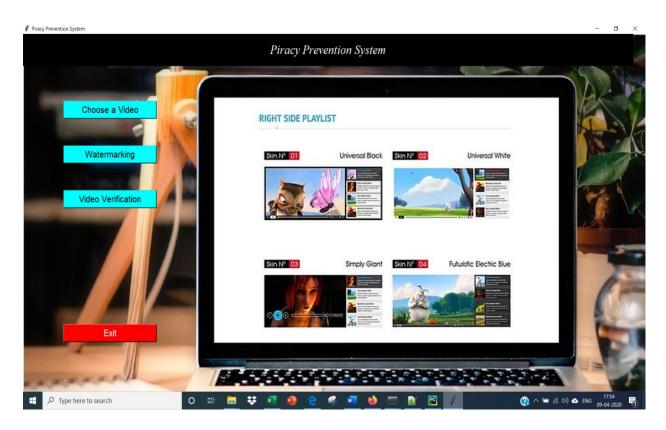
Discrete Wavelet Transform (DWT): DWT is most commonly used algorithm for digital watermarking due to its excellent spatial localization and multi-resolution characteristics. DWT discretely samples the wavelets. It is useful for processing of non-stationary signals. DWT splits the signal into low and high frequency parts. High frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges.

In two dimensional applications, for each level of decomposition DWT is performed in the vertical direction and horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. In second level decomposition, the DWT is applied to LL1. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. Then based on the need, extracting or embedding of watermark is done using extracting and embedding function in DWT. Later, inverse DWT is applied on these 10 sub-bands to get the watermarked image.

V. RESULTS AND DISCUSSION

For video piracy implementation, the following results were obtained -

(5.1) This is the user interface of our system which shows three options for choosing a video, watermarking and video verification.



(5.2) These frames are formed when a video is chosen to be watermarked. Each of these frames is watermarked with the original watermark.

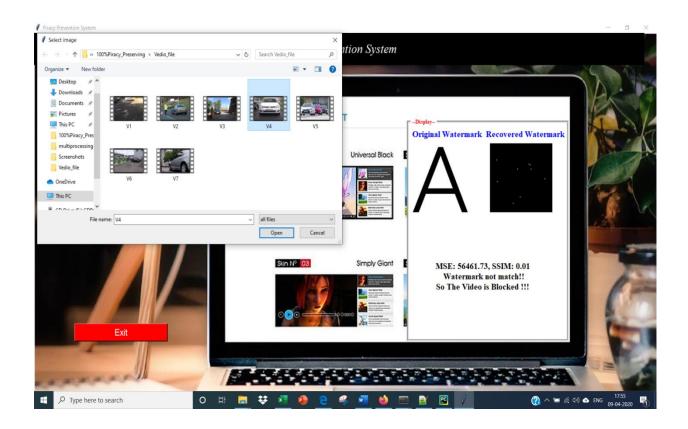
International Journal of Future Generation Communication and Networking Vol. 13, No. 3s, (2020), pp. 128–137

Quick Copy Paste	View Picture To Cut Copy path Paste shortcut	Copy to *	ame New folder	access • Properties	Copen - Copen Select	none selection						
Clipboard → ✓ ↑ 📕 > T	his PC > Windows (C:)	> SHUBHAM > 10	New 0%Piracy_Preserving	Op 100%Piracy_Preser		ect					~ O :	Search Frames
Quick access	frame12	frame13	frame14	frame15	frame16	frame17	frame 18	frame 19	frame20	frame21	frame22	frame23
OneDrive This PC												
Network	frame24	frame25	frame26	frame27	frame28	frame29	frame30	frame31	frame32	frame33 frame45	frame34	frame35
	frame48	frame49	frame50	frame51	frame52	frame53	frame54	frame55	frame56	frame57	frame58	frame59
	frame60	frame61	frame62	frame63	frame64	frame65	frame66	frame67	frame68	frame69	frame70	frame71
	frame72	frame73	frame74	frame75	frame76	frame77	frame78	frame79	frame80	frame81	frame82	frame83
	frame84	frame85	frame86									1

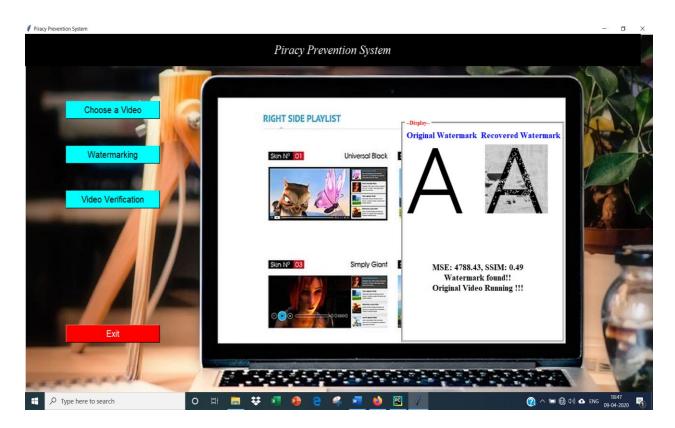
(5.3) This screenshot shows how the frames are formed during watermarking in the background.

00%Piracy_Pro	eserving) 🖿 10												 GUI_MasterP	₽▼ @	
Project 👻		÷ + -	– 🔥 GULJ	/lasterPP.py ×	👸 F_to_V.py	🛛 🕹 🏀 dwt		RGB.py ×	👆 _initpy						
1 ↑ C:\ . in															
_ in															
C:\ in															
		Piracy_Pres	erving(10	Uspiracy_P		ames\frame	/e.png								
		Piracy Pres	serving\10	0%Piracy P		ames\frame									
		Piracy_Pres		0%Piracy_P:			30.png								
	SHUBHAM\100%	Piracy Pres	serving\10	Spiracy P		ames\frame									
		Piracy_Pres		0%Piracy_P:			84.png								

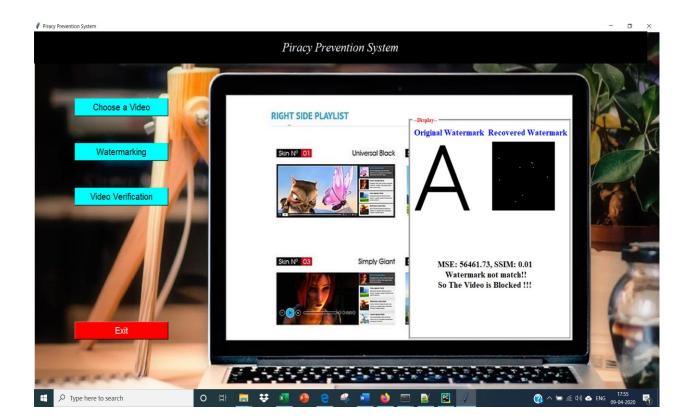
(5.4) This screenshots shows how a video is chosen for watermarking or video verification.



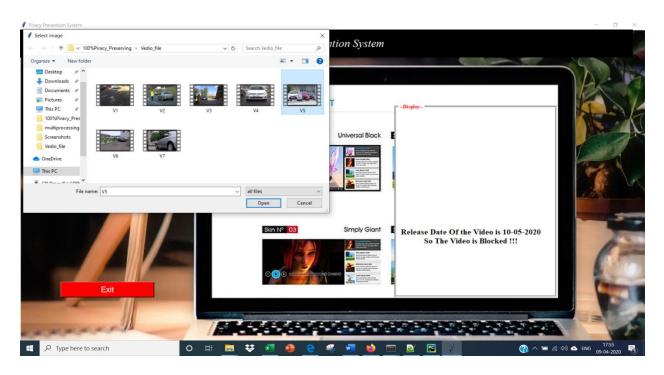
(5.5) If the video contains a watermark then the watermark is recovered and is matched with original watermark. If the recovered and original watermark matches the video runs and the message in the screenshot displays.



(5.6) If the watermark is not found in the video or the recovered and original watermark does not match then the video is blocked and the message is popped as shown in the screenshot.



(5.7) The release date of the video stored in the database is compared with the actual date and if the actual date is after the release date the message shown in the screenshot is displayed.



(5.8) This screenshot shows the database which has the release dates of the videos.

A Cut Clipboard A A Aname Rela 10-2 10-3 10-3	t Painter rs I X B	Calibri B I U V fr C	✓ 11 Font 10-02 D	✓ A A (3) - ▲ -2020			- €‡ W	Tell me wha	- E		~	1		Normal	Bac	1			× 🖬	Σ AutoSu	um • A-	P_sh
Clipboard + A hame Rele 07- 2 10- 3 10-	B B BeleaseDate of 7-02-2020	✓ fi C dwtMark	Font 10-02 D	-2020			- £b ₩ • E M Alignment	frap Text erge & Center	- E	neral 1 - % 1	~	围		Normal	Bac	ŧ)		- B	× 🖬	Σ AutoSu	m · Ar	Q
Clipboard + A hame Rele 07- 2 10- 3 10-	B B BeleaseDate of 7-02-2020	✓ fi C dwtMark	Font 10-02 D	-2020	•	(= •]	N Alignment	ierge & Center	- 12	- % +		(1-1) ±										
Clipboard + A hame Rele 07- 2 10- 3 10-	B B BeleaseDate of 7-02-2020	✓ fi C dwtMark	Font 10-02 D	-2020	D	r = 13	Alignment			7 70 7			Format as	Good	Mai				te Format	🕂 fill -	Sort 8	Find &
Clipboard + A hame Rele 07- 2 10- 3 10-	B B BeleaseDate of 7-02-2020	✓ fi C dwtMark	Font 10-02 D	-2020	F2		Alignment				- % * 10 +1			0000	ive.	utiai			-	↓ Fill - Z T > Sort & Find &		
A Rele tame Rele t 07- 2 10- 3 10-	B eleaseDate o 7-02-2020	C dwtMark	D							Number				Styles				Cell	5		Editing	
name Rel 07- 2 10- 3 10-	eleaseDate o 7-02-2020	dwtMark		E																		
name Rel 07- 2 10- 3 10-	eleaseDate o 7-02-2020	dwtMark			F	G	н	l i i	j.	к	1	м	N	0	Р	0	R	S	T	U	V	w
2 10- 3 10-		1													1100							
3 10-	-03-2019		0																			
		1	0																			
10-	0-01-2020	1																				
	0-05-2020	1																				
	-02-2020	1																				
7 17-	7-02-2020	1	0																			
dw	vt_WMark	6		-						1			1	4								-

VI. FUTURE SCOPE

The system is mainly for cinematic universe where there's always a possibility of copyrights of the original video which causes serious revenue loss to the film industry. The intended use of this system is to detect piracy and avoid pirated videos from being uploaded on internet which helps in avoiding leakage and possible revenue loss due to copyrights. In near future, this project can be extended as per the need by the websites who wants to use this system for piracy prevention.

VII. CONCLUSION

This paper introduces an approach for detecting pirated videos and preventing piracy. The system is primarily motivated from movie industry. This system helps in preventing piracy by blocking the pirated videos from getting uploaded and blocking the site. This method is enough reliable and efficient.

REFERENCES

 HouriaKelkoul, Youssef Zaz, Hicham Tribak and Gerald Schaefer, "A Robust Combined Audio and Video Watermark Algorithm Against Cinema Piracy", 978-1-5386-6220-5/18/31.00 c,2018 IEEE.
 Chunit Kapadne, Khushboo Choudhary, Mir Kekaoos, Vikash Kumar Singh, "Piracy Protection using DWT Hashing", International Research Journal of Engineering and Technology (IRJET),2015.
 Anjali Tiwari, Harsh Shah, Unnati Thube, Nasim Shah, "Video Piracy Detection using Invisible Watermark", International Journal of Engineering Research Technology (IJERT),2015.

[4] Nilesh Kumar Dubey, Shishir Kumar, "A Review of Watermarking Application in Digital Cinema for Piracy Deterrence", Fourth International Conference on Communication Systems and Network Technologies, 2014.

[5] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad,M. Iqbal Saripan 2011,11th International Conference on Hybrid Intelligent Systems (HIS) International Social Science Conference (ISSC),2013 "Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography".