International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May-2018 www.irjet.net p-ISSN: 2395-0072

Piracy Protection using DWT & Hashing

Chunit Kapadne[1], Khushboo Choudhary[2], Mir Kekaoos[3], Vikash Kumar Singh[4]

[1, 2, 3, 4]*Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Maharashtra, India*

Abstract - *"It is said that "Piracy is a crime. As it kills creativity" Piracy can create a huge security issues and monetary losses. When a user uploads any media content he/she is not aware about the hackers sitting at the next corner. Anyone can download the media content and use it and upload it again to gain certain benefits therefore a copyright and piracy protection System is needed to prevent piracy. With Increase of multimedia usage along with the increase in piracy and copyright violations a system is needed to prevent. The project aims to develop a Web Based Service to provide secure and piracy proof environment for Multimedia data which will enable copyright protection and prevent piracy. Using this system a user will be enabled with a facility to provide a web based uploading platform for videos. In which two level security will be provided for the videos uploaded by user using digital watermarking techniques and hashing techniques. Thus preventing the media content duplication and enabling copyrights protection. The main aim of system is preventing piracy and notifying user in case of media content is being uploaded repeatedly. This system will help user in copyright protection and avoiding piracy. Any user who shares their media content on web can use this system along within the organization or provide media content sharing platform to user.*

Key Words: *DWT, CNN, Hashing, Digital watermark.*

1. INTRODUCTION

Today's generation believe in posting wherever they go or whatever they do. Using this system a user is enabled with a facility to provide a uploading platform for media content where while uploading a video watermarks using DWT are applied. Key frame extraction is done.

Hash key is generated and then stored in the database. If anyone is uploading a media content watermarks are applied and hash key is generated. As all the contents of the video are already present that media content cannot be uploaded. If anyone tries to crop that video then the video is checked that how much percent of the video gets matched and email is sent to user and notified about the piracy. Hackers are identified using this system.

2. MOTIVATION

1. To protect originality of content on web platforms.
2. To Stop the piracy of the multimedia content.
3. To develop a piracy free platform for sharing multimedia content.

3. OBJECTIVE

1. To create a web server in which user will upload, download, and play media content.
2. To create a system which will do digital watermarking of the media content and produce hash keys for the media content which is being uploaded
3. To create a system which will check the media content that is being uploaded on the system is already present in the system with help of digital watermark and hash key matching.
4. To notify the original user if his/her is being uploaded by another user and report it to admin.

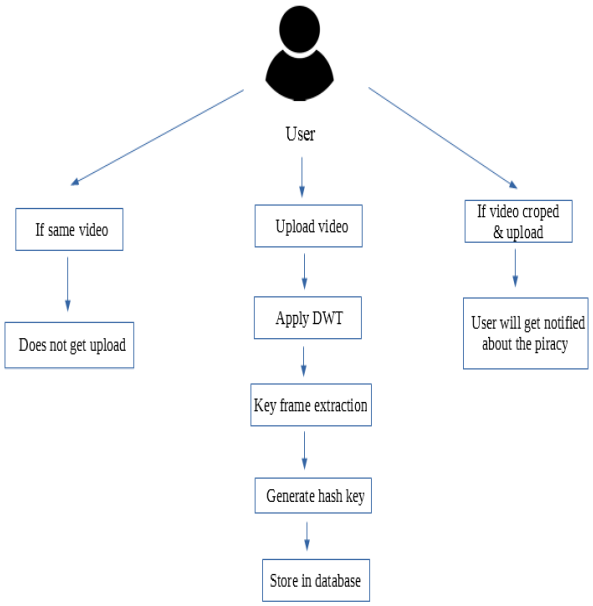
4. LITERATURE SURVEY

[1] Rita Choudhary, Girish Parmar, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT) ", 2016, IEEE discuss the 2 level watermarking technique using DWT in which invisble watermark will be embedded in the video after transforming using inverse transforms which cannot be easily manipulated. Variable visibility factor is used for the insertion of watermark into the low frequency component of the host image. Simulation results show that the feature of the watermarked image and the recovered watermark are dependent only on the visibility factors and also show that the 2-level DWT give superior results than 1-level DWT.

[2] IYu-Gang Jiang, Jiajun Wang, "Partial Copy Detection in Videos: A Benchmark and An Evaluation of Popular Methods", 2015, IEEE. In this Deep learning methods are used to extract the key frame in the video along with use of convolution neural networks to extract different properties of key frame which can be further use for video matching. VCDB is good approach but with extremely low precision therefore future research is needed on frame matching process.

[3] Rong boWang, Hao Chen, Jin liang Yao, Yutian Guo, "Video Copy Detection Based On Temporal Contextual Hashing ", 2016, IEEE. Most video copy detection methods only focus on the contents of key frames and ignore their temporal context information. in this paper, it is proposed to express the temporal context of key frame as binary codes, and compare the key frames' binary codes. Main aspect in future is reducing the number of key frames for hash key generation.

5. ARCHITECTURE



6. TECHNOLOGIES TO BE USED

- **MYSQL:**

MySQL is the most popular Open Source Relational SQL Database Management System. MySQL is one of the best RDBMS being used for developing various web-based software applications. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is the most popular Open Source Relational SQL Database Management System. MYSQL Enterprise edition includes the most comprehensive set of advanced features & management tools for MYSQL. MYSQL is the world's most popular open source database. Whether you are a fast-growing web property, technology ISV or large enterprise, MYSQL can cost-effectively help you deliver high performance, scalable database applications MYSQL is popular choice of database for used in web application & is a central component of widely used LAMP open source web application software stack. MYSQL Query Analyzer: To optimize performance by visualizing query activity and fixing problem SQL code.

- **JSP Servlet:**

Servlets. JSP is a webpage scripting language that can generate dynamic content. Servlets are Java programs that are already compiled which also creates dynamic web content. JSP run slower compared to Servlet as it takes compilation time to convert into Java Servlets. Servlets run faster compared to JSP.

OVERALL DESCRIPTION :

6.1 PRODUCT PERSPECTIVE:

Main perspective of the system is to protect data from getting pirated. To develop an application which will help to secure data? Data will be stored at the server.

6.2 REQUIREMENTS:

SOFTWARE REQUIREMENTS:

Operating system: Windows 7, Ubuntu
Language:
1) Java
2) JSP
Database proposed: MySQL

HARDWARE REQUIREMENTS:

1) 250 GB HD
2) 4 GB RAM

6.3 PRODUCT FUNCTION:

User:

1) Registration, Login

2) Upload media content
- Apply DWT
- Key frame extraction
- Generate hash key
- Store

3) If same media content uploaded, DWT algorithm is applied on it, and generate hash key, if the hash key is same then media content can't be uploaded.

4) If media content cropped then video will be matched percentage wise & email to user

Admin:

1) Manage users
2) View users

7. MATHEMATICAL MODEL

S= { s, X, C, main, DD, NDD, Y, Success, Failure }

• S (system):- Is proposed system which is Digital copyrights protection for multimedia

includes following tuple.

• s (initial state at time T) :- GUI of Video Uploading Server. The GUI provides user

login/Registration for the system where user can upload the video. • X (input to system):-

Upload video. The user has to first login in the system using login credentials if already

registered otherwise register and then upload the video.

• C(Constraints.) = { C1, C2 }

C1 :- Size of the video should not exceed 5 mb.

C2 :- Compatible video formats- 3gp, mp4.

• fmain(main algorithm) :- To embed a watermark in video using DWT and generate hash keys

for key frames.

• DD (deterministic data):- It contains video database along with the hash keys of the videos

already present in the system. • NDD (non-deterministic data):- the new video which is being

uploaded and the hash keys of the video that is being uploaded.

• Y (output of system):- Hash keys are generated for the video which is being uploaded and

stored in database and if video is not present in system it is uploaded. .

• Success= {S1, S2}

S1 :- When video is uploaded successfully

S2 :- When Piracy of video is detected.$\mathbf{CPU_{count}}$: - 1. In our system, we require 1 CPU for server.

• Failure= {F1, F2}

F1 :- System fails to upload video.

F2 :- Piracy of videos is not detected.

Subordinate functions:

Where

s=Start State

e=End State

X= {Set Of Inputs} = {x1, x2,x3, x4}

Where

x1= User Registration and Login

x2= Upload video

x3= If same video upload again

x4= If different video is uploaded

Y= {Set of Outputs} = {y1, y2,y3, y4}

Where

y1= Registration successful

y2= Apply DWT, Key frame Extraction and generate hash key

y3= the video will be matched percentage wise and percentage is greater than65 % then send

mail to owner

y4= video is uploaded successfully and hash keys are stored in database.

Fmain = {Set of procedure} = {f1, f2, f3, f4, f5, f6, f7, f8}

Where

f1= Take x1 input

f2= Give y1 output

f3= Take x2 input

f4= Give y2 output

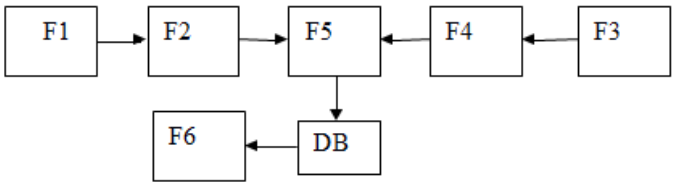
f5= Take x3 input

f6= Give y3 output

f7= Take x4 input

f8= Give y4 output

Functional Dependency Diagram:



Function 1 = F1 = Username, Password
Function 2 = F2 = Upload video
Function 3 = F3 = Download video and upload again
Function 4 = F4 = upload watermark video and generate hash key
Function 5 = F5 = cannot be uploaded, if uploaded display matching percentile.
Function 6 = F6 = Video uploaded on server successfully, hash keys are stored in database.

State Transition Diagram:

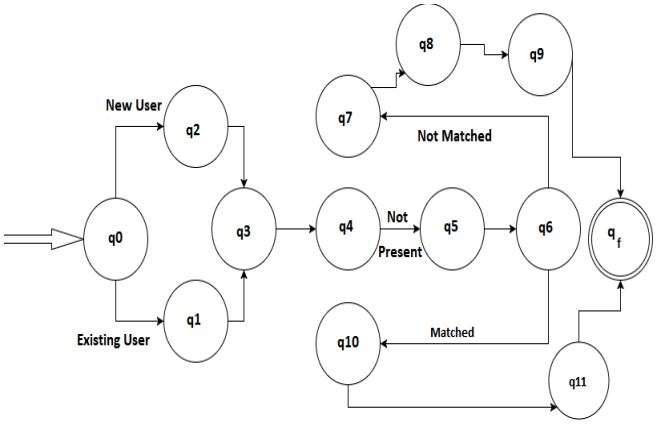


Fig: State Transition Diagram

q0=Initial State
q1=Login
q2=Register
q3=Select Video to Upload
q4=Check for Watermark
q5=Generate Hash keys
q6=Check for Hashing
q7=Piracy free video
q8=Apply Watermark
q9=Store in System
q10=Piracy Detected
q11=Reject Video and inform user
qf = Final State

8. ADVANTAGES

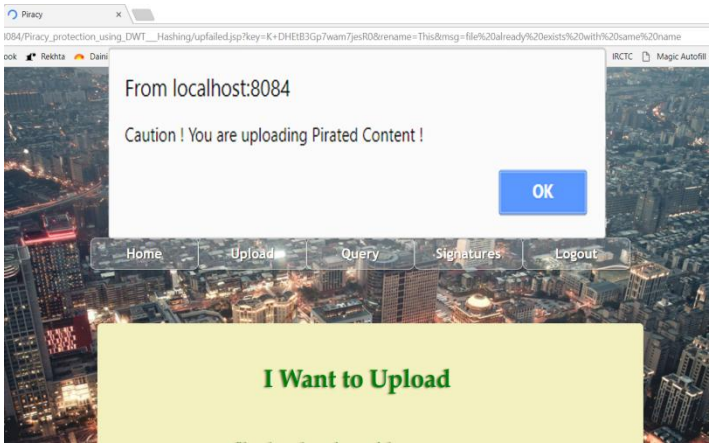
- Identity or sensitive data about record owners are to be hidden.
- Maintaining customer privacy.
- In this technique different attributes are preserved independently.
- Use pseudo data rather than altered data. This method is very real in case of stream data.
- Transformed data are exact and protected. Better privacy compare to randomized approach

9. CONCLUSION

This system is very suitable for the protection of the photographs and videos which are used by users to prevent copyright of owner. It will provide authentication as well as copyright security in multimedia data uploaded with watermark.

10. RESULT

The interface we built detects any contents matching with the one in the database and notify the user about the piracy as you can see in the picture below. If any content is partially similar to the one in the database then there is a provision for sending an email notifying directly the user about the possible piracy.



11. ACKNOWLEDGEMENT

We take this opportunity to thank our project guide **Mrs. S. A. Chiwhane**, for her valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Computer of NBNSSOE, Pune for their valuable time, support, comments, suggestions and persuasion.We would also like to thank the institute for providing the required facilities, Internet access and important books.

12. REFERENCES

[1] Rita Choudhary, Girish Parmar, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT) ", 2016, IEEE

[2] Yu-Gang Jiang, Jiajun Wang, "Partial Copy Detection in Videos: A Benchmark and An Evaluation of Popular Methods ", 2015, IEEE

[3] Rong bo Wang, Hao Chen, Jin liang Yao, Yu tian Guo, "Video Copy Detection Based On Temporal Contextual Hashing ", 2016, IEEE

[4] Secure transmission of data using audio watermarking with protection on synchronization attackR. V. Sobha; M. Sucharitha, 2015 Global Conference on Communication Technologies (GCCT),Year: 2015

[5] Movie piracy tracking using temporal psychovisual modulation, Yuanchun Chen; Guangtao Zhai; Zhongpai Gao; Ke Gu; Wenjun Zhang; Menghan Hu; Jing Liu, 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Year: 2017

[6] Image watermarking with path based selection using DWT & SVD, P. Srilakshmi; Ch. Himabindu, 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Year: 2016.

[7] B. NEWS, "The fact and fiction of camcorder piracy," [Online].Available: http://news.bbc.co.uk/2/hi/technology/6334913.stm, 2015