Cryptography with video watermarking Authentication password using Hadoop

Dharmik Patel [#1], Dr. S. N. Gujar[*2.]
Department of Information Technology, Smt. Kashibai Navale College of Engg.
Pune-41, India.

Abstract *Now a day there is an upcoming challenge to Store, Manage and Distribute Big data across several server nodes, for this purpose, the new platform has been developed which are called as Hadoop. There are provided a within more than three levels of security. It's motivation to provide more security; These are levels of security. There are quite a few numbers of authentication methods are available for security. It is provided of 6-levels of security. That security is a timestamp, shoulder surfing, capture image, one-time password and image selection. The image file is sending with security video watermarking with cryptography. It had the merit of being easy to understand and use. Video watermarking is nothing but inserting a hidden object to detect deceitful alteration by hackers. The object may be regarding a secret key or password etc. The complete software implementation of 3-Level DWT algorithms and to have more secure data a secret key is used, and it used one-time password algorithm for using OTP. That system is providing to the highly secured system. There are providing to video watermarking with cryptography security it using sender to receiver.*

Keywords — *Watermarking, video watermarking, shoulder surfing, Security, Levels of security.*

I. INTRODUCTION

The security purposes every application provides user authentication. From ancient days, secret data or codes are used for hiding and giving security to information. In the user authentication, the process which we have to pass through is username and password. The authentication process is divided into token-based authentication; Biometric based authentication, and Knowledge-based authentication. The web application provides knowledge-based authentication which includes alphanumeric password are same to a graphical password. When we are having some networks and personal accounts some secure authentication scheme needs to be provided. In this paper, we present the image based authentication that can do log in. Password image is generated, and it will be downloaded from the email which is stored at the time of registration. Every time the image will be unique. In this system, the OTP-based authentication is also used.

HDFS developed by Apache Foundation takes not only full advantages of the power of high-speed computing clusters and storage but also demonstrates high performance in big data storage. The primary concern of network security is to ensure that unrelated individuals, who have no right to use but attempt to obtain the remote service, cannot read or modify the information which will be passed to other receivers. Most of the emergencies of the network security problems are because malicious people try to intercept or modify the information which does not belong to him originally, to obtain some kind of benefit or harm others intentionally. It is, of course, that to guarantee the network security not only needs to make the program without programming errors but also to guard against hackers, stalkers, especially who have abundant time and money to brute force attack the system[6].

This system provides four steps security. The security is Image matching, OTP matching, user authentication and shoulder attack based security is of color and image combination. The system is data file will be embedded using an image as a key into the video file, and the sender has sent this file to the receiver. Then the receiver extracts the data file by using the image as a key. All the video files will process using Hadoop file system. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown the text-based passwords are fraught with both usability and security that make them less than desirable solutions. Psychology studies have to know that the human brain is better at recognizing and recalling images than text. In this project, however, we have focused on another alternative: using pictures as passwords. The graphical password schemes have been proposed as a possible alternative to text-based schemes. It is motivated partially by the fact of humans can remember pictures better than text, psychological studies supports such assumption.

II. RELATED WORK

Shaikh Shoaib, R. C. Mahajan, Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks. The shoulder-surfing resistant versions hold severe round redundancy, and adversaries can exploit it. The black and white key presses during PIN entries are

unbalanced, and the enemies can use this. It is explained to all the pin entry to work black to white colors combinations [1].

Taekyoung Kwon, Jin Hong Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT. The proposed embedding process Figure 1 from the block diagram we see that after separating the video into different video shots the system will apply 3L-DWT on the blue channel of RGB frame. It is shown in figure-2.2. In the 3L-DWT coefficients, we embed preprocessed watermark image from the HL3 to HH1 sub-band consecutively and then it is transformed into 3-level inverse DWT form. At this stage, for RGB video frame we get the watermarked blue channel which is then combined with other two channels to obtain the watermarked video frame[2].

Rakesh Ahuja, S S Bedi Copyright Protection using Blind Video Watermarking Algorithm based on MPEG-2 Structure, A blind watermarking algorithm is being proposed in which the watermark information is being embedded by little alteration of some of the value of DCT coefficients of luminance part of video while encoding it in MPEG-2 style. It is evident that for any watermarking the three parameters, robustness, perceptibility and payload capacity must be simulated to provide better results. The special care must be taken that how much time the system takes to embed the watermark. The effectiveness of the proposed algorithm is that we have tested three parameters like robustness, perceptibility and elapsed time for embedding the watermark and obtained the better result as compare to the results of previous researches [3].

Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng A Shoulder-Surfing Resistant Graphical Authentication System**,** Authentication based passwords are used largely in applications for computer security and privacy. This evolution takes great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe and then directly or use external recording devices to collect users' credentials. The authentication process in public might result in potential shoulder surfing attacks. Even a hard password can be cracked easily through shoulder surfing. There are using traditional textual passwords and the PIN method, The users need to types their passwords to authenticate themselves, and these passwords can be revealed easily if someone peeks over the shoulder or uses video recording devices is such as cell phones[7].

R.Thenmozhi, K. Balachandar, Swathikha.S, RanjanaDevi.G, Authentication and Digital Video Tampering Detection Using Watermarking, It usually refers to digital image processing, but the image processing can also be done for two types optical and analog. The input are images which can be either images or video frame while the output can either to be a picture or a set of characteristics of an imaging method is very easy to implement and addresses both spatial and temporal domains. It is simple and contains very low complexity and efficient regarding capacity, transparency, and security[8].

Amir M. U. Wagdarikar, Ranjan K. Senapati, Robust and novel blind watermarking scheme for H.264 compressed video**,** This is to design and implement robust and novel watermarking scheme for H.264 encoded videos. This watermark is embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the third wavelet decomposition level by quantization. They have tested the resilience of the watermarking algorithm against series of different attacks for different H.264 compressed videos[13].

Chu-Hsing Lin, Chen-Yu Lee, Shih-Pei Chien, Digital video watermarking on cloud computing environments, The use of digital watermarking have to protect the digital copyright has become much crucial in the area of the Internet. Further, The process is video watermarking very time-consuming. For the quick implementation of digital video watermarking, in this article, we proposed the use of the Hadoop distributed computing system, where the original video is split, for the different requirements to realize watermarks are embedding. There are shown in Figure-2.3. The time consumption for applications with large computing load such as video watermarking. Also, the proposed method can also be used daily by users over the cloud environment not only by Hadoop but also others applications powered by Google and Yahoo. The computation of digital watermarking technology in cloud environments will play a very important role in the protection of intellectual property in the age of digitalization[14].

III. PROPOSED SYSTEM

The proposed system is implemented for improving security ratio. This system is providing more levels of security and image sharing system. It images to share with video watermarking and cryptography security.

A. Proposed algorithm steps

Step 1 Login Process:

At first when the user has to login the system, and for that, he has to sign to sign up the system. While signing user has to provide the whole

information about himself such as name, account details full fill and then login is user and password.

Step 2 Timestamp:

Next step is the second level of security system user is input only mail id and received mail with the image. This image is timestamp image. The user can download an image and upload image. Its image is a match then go to the next level of security.

Step 3 Shoulder surfing:

This security is protecting to shoulder attacks. It is color match security and numbers. In this paper to the 3rd level of the security system.

Step 4 OTP:

OTP is one-time password it is 4th level of security. The user is given a number when they registration. This is registration number to receive a text message and put in OTP place.

Step 5 Image processing:

It is 5th level of security. Its security is check robot. Who is operating our system to check machine ya human in this security system. It is given six images, and tick mark image is given a name.

Step 6 Image capture:

This security is the last level of security. It is shown one image with the numeric number, and this number is put down in the field, It image is a match then open the application.

Step 7 Make video watermarks:

This is the main portion of a project. It makes video watermark with the key. It is called steganography. In module to work image sharing one user to another user. It is protected to image file data and then sharing system.

Step 8 Digital Document Wallets:

This step is used for download documents. The documents are stored at one time it uses many different places. That time only download.

B. System Overview

This system has the six steps security with user authentication, Image matching, OTP matching, and shoulder attack based on color and image combination, capture image.In this system, the data file will be embedded using an image as a key in the video file, and the sender has sent this file to the receiver, And receiver extracts this data file by using the image as a key. All the video files will process using Hadoop file system. Various graphical password schemes have proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security that make them less than desirable solutions. Psychology studies have revealed that human brain is better at recognizing and recalling images than text.

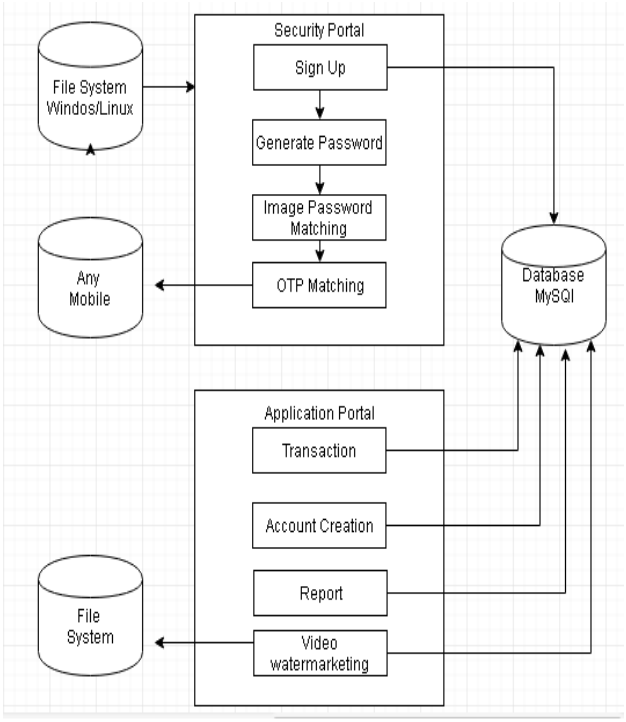

Fig 1: System Architecture

IV. MATHEMATICAL MODEL

S= {S, s, X, Y, T, f_{main}, DD, NDD, f_{friend}, memory shared, CPU_{count}}

- **S (system)**: - It is our proposed system which includes following tuple.
- **s (initial state at time T)**: -GUI of wireless indoor tracking. The GUI provides space to enter a query/input for the user.
- **X (input to the system)**: - Input Query. The user has to first enter the query. Then the query may be ambiguous or not. The query also represents what user wants to search.
- **Y (output of the system)**: - List of URLs with Snippets. The user has to enter a query into wireless indoor tracking then wireless indoor tracking generates a result which contains related and irrelevant URL's and their snippets.
- **T (No. of steps to be performed)**:- **6**. These are the total number of steps are required to process a query and generates results.
- **f_{main}(main algorithm)**: - It contains Process P. Process P contains Input, Output and subordinates functions. It shows how the

query will be processed into different modules and how the results are generated.

- **DD (deterministic data)**: - It contains Database data. Here we have considered Rooms information, floors information, route information i.e. Database which contains many rooms information. Such as routes uploaded by admin will be shown to users when requested as a result.
- **NDD (non-deterministic data)**: - Number of input queries. In our system, the user can enter numbers of queries so that we cannot judge how many queries the user enters into the single session. Hence, The Number of Input queries are our NDD.
- **f_{friend}**: - WC and IE. In our system, WC and IE are the friend functions of the main functions. Since we will be using both the functions, both are included in the f_{friend} function. WC is Web Crawler which is a bot, and IE is Information Extraction which is used for extracting information on the browser.
- **A memory shared**: - The database will store information like the list of receivers, registration details, and numbers of receivers. Since it is the only memory shared in our system, we have included in the memory shared.
- **CPU_{count}**: - In our system, we are require 1 CPU for server and minimum 1 CPU for the client. Hence, CPU_{count} is 2.

Subordinate functions:

Identify the processes as P.

S= {I, O, P....}
P= {SM, SR}

Where,

- SM is floor site.
- SR is site route.
- P processes.

SM= {U, MAX, SC}
Where,

- U= x, y co-ordinates for rooms
- MAX = {1, 2, 3, … , n}
- SC site created with number of rooms.

SR= {SC, Triangulation Algorithm, Info}
Where,

- SC is input which contains rooms and path information

Triangulation algorithm is used to calculate user's current x, y co-ordinates from the current physical location over site map on the phone.

V. Result and Discussion

These system parameters are throughput, processing time, efficiency, security level. There is existing system and proposed a system to security level is very high. The system is working more efficiency. These systems are taken low processing time.

There is 6 level of authentication system so the take more times. But processing time is very low. It is shown in Table 1.

Table 1 Result parameters

Sr. no.	Parameter	Existing system	Proposed system
1	Throughput	1 step authentication in 20 seconds	1 step authentication in 15 seconds
2	Processing time	20 seconds	15 seconds
3	efficiency	20 %	80%
4	Security level	High	Very High

This system result is graph shown in figure 2 the graph is exiting system vs. propose system.

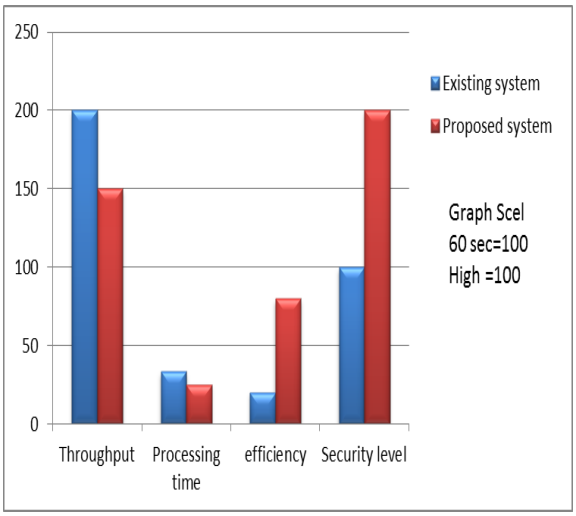

Fig 2: Existing system vs. proposed system

VI. Conclusions and Future Work.

This proves that the graphical password is a more desirable alternative to alphanumerical passwords. In this system provide the image based authentication that can do log in. Password image is generated, and it will be downloaded from the email which is stored at the time of registration. In this system, the OTP-based authentication is used. The four steps security with user authentication, Image matching, OTP matching, and shoulder attack based on color and image combination. The data file will

be embedded using an image as a key in the video file, and the sender sends this file to the receiver, and the receiver extracts the data file by using the image as a key. Video watermarking is the process where this image is going to send to the receiver for increasing level of security. In future, the digital wallet is stored important image and take to when use to image that time download and share images.

ACKNOWLEDGMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We would also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend heartfelt gratitude to friends and family members.

REFERENCES

[1] Taekyoung Kwon, Jin Hong, "*Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks*," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015.

[2] Shaikh Shoaib, R. C. Mahajan, "*Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT*", 2015 International Conference on Communication, Information & Computing Technology (ICCICT), 978-1-4799-5522-0/2015.

[3] Rakesh Ahuja, S S Bedi, "*Copyright Protection using Blind Video Watermarking Algorithm based on MPEG-2 Structure*", International Conference on Computing, Communication and Automation 978-1-4799-8890-7/15/ ©2015 IEEE.

[4] P. Viswanathan, P. Venkata Krishna, "*A Joint FED Watermarking System Using Spatial Fusion for Verifying the Security Issues of Teleradiology*," IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 3, MAY 2014.

[5] Somayyeh Mohammadi, Kerman, Iran, "*A Novel Video Watermarking Algorithm based on Chaotic maps in the Transform Domain*," 2015 International Symposium on Artificial Intelligence and Signal Processing.

[6] S. Saranya, M. Sarumathi, B. Swathi, P. Victer Paul, S. Sampath Kumar, T. Vengattaraman, *"Dynamic Preclusion of Encroachment in Hadoop Distributed File System"* 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

[7] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "*A Shoulder-Surfing Resistant Graphical Authentication System*," 10.1109/TDSC.2016.2539942, IEEE Transactions on Dependable and Secure Computing.

[8] R.Thenmozhi, Swathikha.S, RanjanaDevi.G, R. Saravanan, "*Authentication and Digital Video Tampering Detection Using Watermarking*," ICARCSET '15, March 06 - 07, 2015, Unnao.

[9] Rupali Walker, Priyanka More, "*Digital Audio Watermarking and Image Watermarking for Information Security*," International Conference on Pervasive Computing (ICPC)

[10] Rupali D. Patil, Shilpa Metkar, "*Fragile Video Watermarking for Tampering Detection and Localization*," 2015 International Conference on Advances in Computing, Communications, and Informatics (ICACCl).

[11] Santhoshi Bhat, Arghya Ray, Avishake Ghosh, Ananya Ray, "*Image Steganography and Visible Watermarking using LSB Extraction Technique"*, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015.

[12] M.Hindusree, Dr.R.Sasikumar, "*Preventing Shoulder Surfing in Secure Transactions"*, 2015 International Conference on Computing and Communications Technologies (ICCCT'15).

[13] Amir M. U. Wagdarikar, Ranjan K. Senapati, "*Robust and novel blind watermarking scheme for H.264 compressed video*", SPACES-2015, Dept of ECE, K L UNIVERSITY.

[14] Chu-Hsing Lin, Chen-Yu Lee, Shih-Pei Chien, " *Digital Video Watermarking On Cloud Computing Environments*," ijirct.