Enhanced Security in Online Database System

Minal Nerkar¹, Priya Talreja², Komal Pawar³, Radha Gosavi⁴, Devika Dhadphale⁵
Department of Computer Engineering, AISSMS IOIT, Pune, India

Abstract—In this era due to unbelievable development in internet, various online attacks has been increased. From all such attacks most popular attack is phishing. This attacks are done for extracting confidential information such as banking information, passwords from unsuspecting victims for fraud purposes. Confidential data can’t be directly uploaded on website since it is risky. Here in this paper data is encrypted in video and visual cryptography for login purpose in our online database system for providing more security.

Keywords—CAPTCHA, watermark, LSB, DES, SCD, Split algorithm.

I. INTRODUCTION

Nowadays, security has become major concern in online transactions. Phishing websites are those websites that extracts the confidential information of the user. For detecting such sites here is the provision of VCS (Visual Cryptography Schema). For giving more protection to user’s data we are encrypting the data in video which will be invisible to human eye.

In this paper first part will be VCS and second will be Watermarking. In first part we are covering how to provide security to login phase. For this in register phase user is asked for key then using this key image CAPTCHA is created. This image CAPTCHA is split into two shares. One is kept with user and other on server. Then at the time of login help of this shares is taken for validating purpose.

In second part how watermarked video can be made for hiding confidential data is covered. Firstly video is taken & watermark is also taken then by applying LSB (Least significant bit), SCD (Scene Change Detection), DES (Data Encryption Standard), Split algorithm watermarked video is created. This watermark will be invisible due to which human eye cannot recognise if there is any hidden information.

II. LITERATURE SURVEY

In the current scenario as shown in the Fig(a), when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page.

But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input[1].

Fig I Current Scenario

Now something about video watermarking, there are different existing tools for video watermarking process such as video watermark factory, video watermark pro, watermark master etc. Video watermark factory is full featured and easy-to-use software that allows placing a digital watermark or logo or text over an existing video in the batch mode. Watermarks can be used for protection or adding comments to your video. Video watermark master tool is used to protect video or graphics file from illegal copying by putting watermark (text or graphics information) over an image. This tool provides ability to apply a great number of various effects to a watermark, including dynamic effects and also it is possible to put subtitles onto a video frame. Video Watermark Pro is a professional video processing tool that lets user to add text, images and shapes as watermarks to clips. Although it packs some pretty advanced features, the utility bundles an intuitive layout, making the procedure easier to handle by less skilled users[3].
A. Limitations of existing system

As internet access for small as well as for important purpose has become common, hacking risk also get increased. Phishing attacks can be done for confidential information. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. [1].

Existing video watermarking tools uses visible watermark. The main disadvantage of visible watermarking is that it destroys the video quality and watermark can be easily removed from video. In contrast, invisible watermarking is imperceptible to those viewing the video and the watermark is still present in the multimedia data even after various signal processing or transmission distortions [3].

III. METHODOLOGY

A. Login Phase

In register phase, user is first asked to fill details along with the key. The key string to be entered can be combination of alphabets and numbers which will be concatenated with the randomly generated string from the server. Creation of CAPTCHA and division of shares will be obtained at the end of this phase. Image verification is done by the human visual system to verify whether the displayed image CAPTCHA is similar to the CAPTCHA generated during registration phase.

In the login phase user is first asked for the username and then is asked to enter the share kept with him. This share is sent to the server where the user share is stacked with the share stored in the server. After stacking of shares the image CAPTCHA is displayed and is used to verify whether the website to which the user is trying to login is original or not. [6]

B. Video Watermarking Phase

In this phase, user is asked for video and watermark. Scene change detection algorithm is applied to video for breaking the video in smaller frames. SCD algorithm with different parameters is used for breaking video in larger frames. Split algorithm is applied to watermark/data to split into frames. One frame of watermark is combined with larger frame of video with the help of LSB algorithm and then combined with smaller frames. LSB algorithm is used to encrypt the data in video. DES algorithm is used to convert the video in unreadable form. [5]

IV. MATHEMATICAL MODEL

Let 'S' be the system that solve problem of “copyrighting of multimedia documents”, 'X' be the input consist of video and watermark, 'Y' as output consists of extracted watermark from video.

\[ S = \{ y, x, f_s | \Phi_s \} \]  
be a partial design where

\[ Y = f_s(x) \text{ that follows } \Phi_s \text{ and} \]

\[ X \epsilon V U W : \text{Video and Watermark Text} \]

\[ f_s : x \rightarrow y \]

\[ Y \epsilon W' , \text{Where W'} \text{ is Extracted watermark.} \]

Objectives:

1) **Outcome**: Watermark is detected in video and it is extracted from video

2) **Constraint**: X should not belong to NULL set.
Success and Failures of problem:

Success: Extracted watermark and original watermark are same.
F(X)={Wi | Wi ∈ X is Original watermark}

Failure: Watermark is not present.
i.e. f(x)=Φ

Design Analysis:
The approach taken is to view the entire set of video as universe set (Un) from which we would analyze a subset of video (V) and watermark Text(W).

Let 'S'={y, x, fs | Φs}
Where Y= {Wi ∈ W’ where W’ is Extracted watermark}

Where X=input consists of video and watermark.
Let Un= V U W is a universal set of input set.

Where, ‘V’ is video given as input i.e. V ∈ U.
And this video is divided into number of frames. i.e F ∈ V
F=[F1, F2, F3, .......Fn]

‘W’ is the set of watermark parts i.e. W ∈ U
W={W1, W2, W3, .......,Wn}

Mathematical Relations:
1) I= V + W

This relation shows that input consists of video and watermark therefore video and watermarks are the subsets of input set so it can be shown by following relation.

F1”, F2”, F3”, ....,Fn” are the frames which contains watermark parts . On these frames watermark extraction algorithm is applied which will extract watermark part from each frame. These extracted watermark parts can be numbered as W1’, W2’, W3’ ......Wn’. Then these watermark parts are merged together to get final extracted watermark (W’). Here W’ is nothing but ‘Y’ which is extracted watermark.
V. FUTURE SCOPE

1. The generated CAPTCHA may be attacked by the phisher so security to the shares can be provided in future. Instead of using black and white pixel scheme we can also use color scheme.

2. This system can be also used in cloud computing which will enhance the security. Backup server can also act as muticloud.

REFERENCES


[5] Enhancement an algorithm to hide a text into a digital image as a steganography technique.