ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (297-302), Month: October - December 2015, Available at: www.researchpublish.com

# Enhanced Security in Online Database System Using Visual Cryptography and Water Marking

[1]Divya Sahay, [2]Monalisa Merchant, [3]Suleiman Sheikh, [4]Rohan Shukla, [5]Shubhangi Suryavanshi

[1,2,3,4,5] Department of Computer Engineering, Savitribai Phule Pune University G.H.R.I.E.T., Wagholi , Pune,India

*Abstract:* **Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. Similarly due to rapid growth of internet and multimedia systems now it is easier to copyright the multimedia documents like audio, video, text, images etc. Video piracy has become an increasing problem particularly with the proliferation of media sharing through advancement of Internet services. Since digital video can be easily and perfectly duplicated and illegally distorted, appropriate schemes are needed to protect the rights of content owners or the integrity of the surveillance video . Now days there are many techniques available for providing security to multimedia documents.Video watermarking is an important emerging technique for these issues. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP) .In the system we also propose scene change detection (SCD) watermarking algorithm which is the most convenient and efficient method for copyright protection of video. This method is more robust to withstand with different types of video attacks like frame dropping, lossy compression. Here combination of both the Schemes is implemented so as to give enhanced security to the system. This makes our system robust against all type of attacks**

***Keywords*: CaRP, SCD, Visual cryptography, watermark, image security**.

## 1. INTRODUCTION

Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the colour Images means Gray Images and RGB/CMY Images. The protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a days by people. This results in recording, editing and replication of multimedia contents. Video watermarking can be used to protect data against illegal manipulations and distributions. This technique provides a robust solution to the problem of intellectual property rights for online contents.

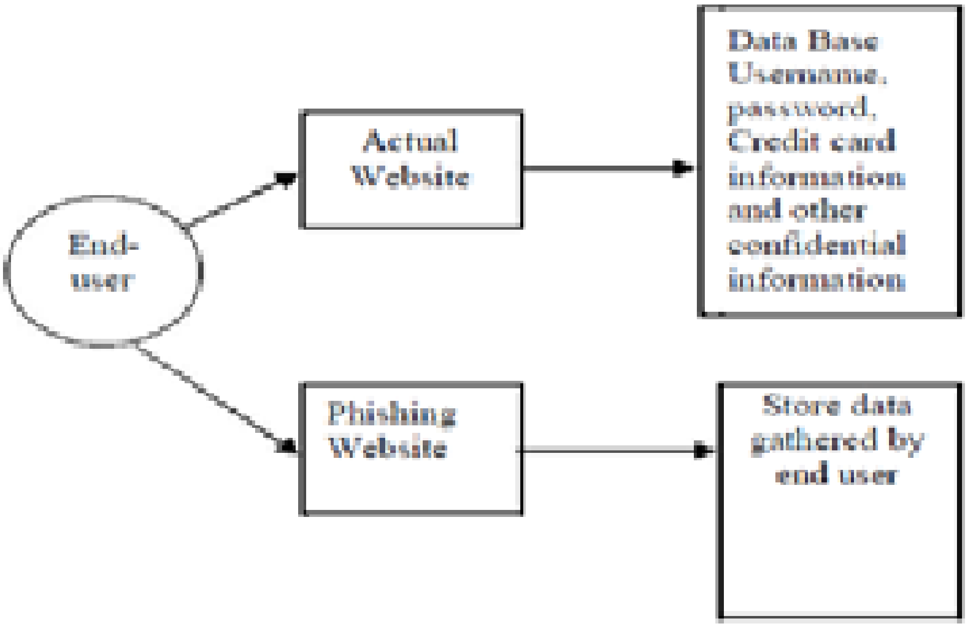
Online transactions are now a days become very common and there are various attacks present behind this. Thus the security in these cases should be very high and should not be easily tractable with implementation easiness. The concept of image processing and an improved visual cryptography is used. Visual Cryptography (VCS) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image. Watermarking is a major image processing application used to authenticate user documents by embedding and hiding some authenticated piece of information behind an image, audio or the video file. Video watermarking involves embedding a secret information in the video. For example, copyright symbols or signatures are often used. The traditional watermarking approach tends to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer. Now a days more efficient and secured approach to perform watermarking is used. It is done by using invisible watermarking technique. Video watermarking is done by using Scene change detection technique which embeds different parts of a single watermark into different scenes of a video.

The main objective of this project is to hide data in video and provide security to the same. Our methodology is based on Image CAPTCHA validation scheme using visual cryptography. Visual Cryptography is use to preserve the privacy of image CAPTCHA. Video piracy has become an increasing problem particularly with the proliferation of media sharing through advancement of Internet services. Since digital video can be easily and perfectly duplicated and illegally distorted, appropriate schemes are needed to protect the rights of content owners or the integrity of the surveillance video files. Now days there are many techniques available for providing security to multimedia documents. Video watermarking is an important emerging technique for

these issues. In our system we propose scene change detection (SCD) watermarking algorithm which is the most convenient and efficient method for copyright protection of video. This method is more robust to withstand with different types of video attacks like frame dropping, lossy compression.

## 2. LITERATURE SURVEY

***A. Current methodology:*** Visual cryptography, an emergin cryptography technology, was proposed in 1994. It was called as secrete sharing scheme. First the secrete image was encrypted and decrypted using human visual system. Secrete image is hidden in n different shares. Then these shares are stacked together to reveal the final secrete image. Any one share cannot reveal anything about secrete image. Hence, security level of the secrete image is increased when it is transmitted via internet. There are some schemes that take only binary images as secrete image. New cryptography schemes are also there that can process secrete colour images that are more complex In the current scenario as shown in the Fig, 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).


End-user
Actual Website
Data Base Username, password, Credit card information and other confidential information
Phishing Website
Store data gathered by end user

Video watermarking embeds data in the video for the purpose of identification and copyright. Many digital watermarking schemes have been proposed for images and videos. It permits only authorized users to access encrypted digital data. Video watermarking introduces some issues which is not present in image watermarking. A robust video watermarking scheme is necessary.

Our video watermarking algorithm is robust against the attacks of frame dropping,averaging and statistical analysis, which were not solved effectively in the past. In complete survey of current watermarking technologies, and noticed that none of the existing schemes is capable of resisting all attack [4] . Watermarking is a major image processing application used to authenticate user documents by embedding and hiding some authenticated piece of information behind an image, audio or the video file. Video watermarking involves embedding a secret information in the video. For example, copyright symbols or signatures are often used. The traditional watermark ing approach tends to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer [3] .Now a days more efficient and secured approach to perform watermarking is used. It is done by using sub image classification, i.e. selected frames only will contain a fractional number of total bits from the watermark image.[4] The watermark can be visible or invisible. The visible watermark appears visible to a casual viewer on a careful inspection. The invisible robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. Video watermarking can be divided into three main groups based on the domain that the watermark is embedded: spatial domain, frequency domain and MPEG code structure. Most of the current video watermarking techniques are based on the image watermarking and directly applied to uncompressed or compressed video sequences. However these methods are not sufficient for copyright protection in video data [5]. There are dfferent 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. Watermark master tool is use 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 [4].

***Limitations of existing System:*** Main limitation in todays online confidential data accessing system is there may be possibility that this data may be attacked by phishing websites therefore there comes need to identify whether website is phishing or not.[7] 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.[6] 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.

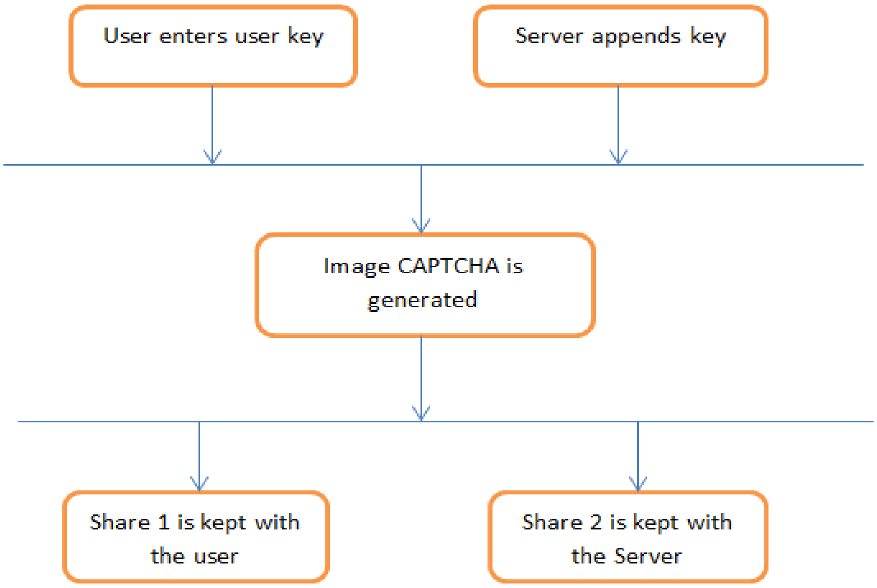
## 3. PROPOSED SYSTEM

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other con_dential information from the phishing websites. We also propose the idea of embedding di_erent parts of a single watermark into di_erent scenes of a video. We then analyze the strengths of di_erent watermarking schemes, and apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks. For implementing Watermarking Technique we are using SCD, LSB, Split,DES algorithms.

**The proposed approach can be divided into three phases:**

***A. Registration Phase:*** In the registration phase, a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combinnation of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later veri_cation during login phase.

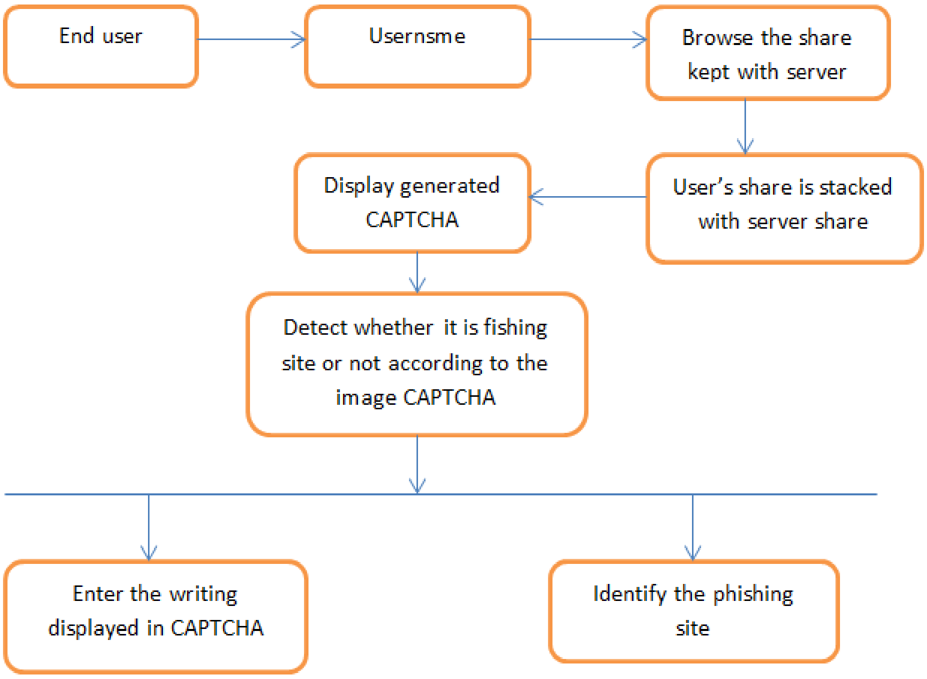
The image captcha is also stored in the actual database of any con_dential website as confidential data. After the registration, the user can change the key string when it is needed. Registration process is depicted in figure Registration phase.


User enters user key
Server appends key
Image CAPTCHA is generated
Share 1 is kept with the user
Share 2 is kept with the Server

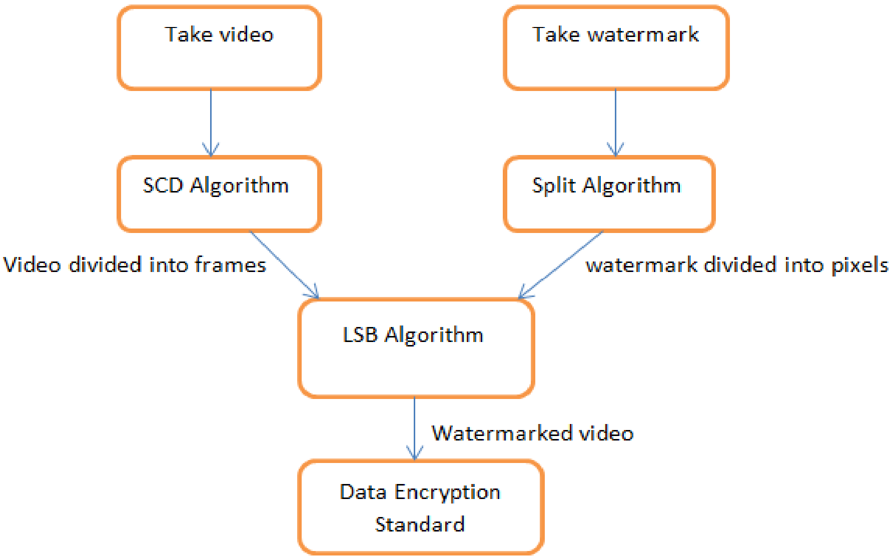
***B. Login Phase:***

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image

captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. This phase is depicted in Figure login phase.[2]


End user
Usernsme
Browse the share kept with server
User's share is stacked with server share
Display generated CAPTCHA
Detect whether it is fishing site or not according to the image CAPTCHA
Enter the writing displayed in CAPTCHA
Identify the phishing site

***C. Watermarking Phase:*** We propose the idea of embedding different parts of a single watermark into different scenes of a video. We then analyze the strengths of different watermarking schemes, and apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks. Here in this technique we are going to use 4 different schemes: 1) SCD(Scene change detection algorithm) 2)Split algorithm 3)LSB(Least Significant Bit) 4)DES(Data Encryption Standard). Following watermarking phase shows the exact flow of our Watermarking Technique. The effectiveness of this scheme is verified through a series of experiments, in which a number of standard image processing attacks are conducted.



## 4. SYSTEM ARCHITECTUTR

System design provides the understanding and procedural details necessary for implementing the system recommended in the system study. Emphasis is on translating the performance requirements into design specifications. The Design phase is a transition from a user-oriented document (System proposal) to a documented oriented to the programmers or database personnel. The proposed software has three-tier architecture. The architecture layers are the database layer, the application server layer and the client layer. The application server layer and the database server will communicate and the details are displayed to the client. Three-tier architecture is considered to be the most suitable architecture for large applications. The partitioning of the application enables rapid design and development of the system. The modularity makes it easier to make changes to just one tier without affecting the others. Separating the functions into distinct tiers makes it easier to monitor and optimize the performance of each layer. Load balancing and adding more capacity can take place independently at each layer. Multi-tier architecture also makes it simpler to scale the system across multiple processors on different machines.

1. The presentation layer delivers the application to the end users.

2. The business logic layer contains and executes the rules that run the application.

3. The database layer manages the data required by the application.

## 5. CONCLUSION

With the advent of internet, various online attacks has been increased. .Here an image based authentication using Visual Cryptography is implemented. After successfully login of the system we can upload encrypted data on the system. The process of this comprehensive video watermarking scheme, including watermark preprocessing, video preprocessing, watermark embedding, and watermark detection, is described in detail. Various improvement approaches are also presented. Experiments are conducted to demonstrate that our scheme is robust against attacks by frame dropping, frame averaging, and statistical analysis.

## ACKNOWLEDGEMENT

We are working on this project under the guidance of Mrs. Shubhangi Suryavanshi, Assistant Professor at G.H.Raisoni Institute of Engineering & Technology, Wagholi, and Pune.

## REFERENCES

[1] Akash Mehara, Emon Vuess ,Enhanced Security in Cloud Computing(IEEE 2014).

[2] Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual Cryptography (IEEE 2014).

[3] Video Watermarking for Copyright protection using Scene Change Detection Algorithm (White Paper).

[4] Pik Wah Chan, Student Member, IEEE, Michael R. Lyu, Fellow, IEEE, and Ronald T. Chin, A Novel Scheme for Hybrid Digital Video Water- marking: Approach, Evaluation and Experimentation.

[5] Hamid Shojanazeri, Wan Azizum Wan Adnam, Sharifah Mumtadzah Syed Ahmed, Video Watermarking Techniques for Copyright Protection and Content Authentication (International Journal of CIS IMA 2013).

[6] Rini T Paul, Review of Robust Video Watermarking Techniques (NCCSE 2011).

[7] Gopika V Mane, G G Chiddarwar, Review Paper on Video Watermarking Techniques (International Journal of Scienti_c Research Publication, 2013, April 2013).

.