Confidential log-in to real user using Visual Cryptography and upload encrypted data on Database System using Steganography

Shah Shrenik[1], Shetyanavar Shubham[2],Waghmare Manoj [3],Gandhi Saurabh[4]

Department of Computer Engineering

AISSMS College of Engineering

Shivajinagar, Pune 01

Guide: Professor A.S. Deokar

Abstract - *Data is an important asset for any individual or organization and must be protected from intruders or hackers. The need to hide data from hackers has existed since ancient times, and nowadays, there are developments in digital media, such as audio, video, images, and so on. To secure secret information, different media methods are used and steganography is one. This project presents video steganography with digital watermarking algorithms as an efficient and robust way for protection. This paper is a combination of Cryptography, Steganography and watermarking algorithms which provides a strong backbone for its security and hiding data in different multimedia files. This proposed system not only hides data but also limits the perceivable distortion that might occur while processing it.*

Database security is provided by using image CAPTCHA created using Visual Cryptography algorithm. The data is store in database using steganography and watermarking algorithms behind the multimedia files. The proposed System provides the Confidential Login to user using Visual Cryptography and upload encrypted data, Data System using base Steganography. It has the objective 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.

Key Words: SCD,LSB,CaGP,AWT.

1.Introduction

Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation, the existence of hidden communication cannot be detected by third parties.

What distinguishes historical steganographic methods from the modern ones is, in fact, only the form of the cover (carrier) for secret data. Historical methods relied on physical Steganography the employed media were: human skin, game, etc. Further advances in hiding communication based on the use of more complex covers, e.g. with the aid of ordinary objects, whose orientation was assigned meaning. This is how semagrams were introduced. The popularization of the written word and the increasing literacy among people had brought about methods which utilized text as carrier. The World Wars had accelerated the development of Steganography by introducing a new carrier the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. The latter may apply to network protocols as well as any other communication protocol (e.g. cryptographic).

The way that people communicate evolved over ages and so did steganographic methods. At the same time, the general principles remained unchanged.

1.2 Problem Statement

Globalization has led to the rapid growth of the Internet through which consumers can send and receive large amounts of data (e.g., text, audio, video, and images). In modern communication systems, securing data is of utmost importance. Yet sending and receiving secret files over the Internet is still insecure, and therefore hiding data in an effective way protects this secret information. Data is important to any organization. They must be protected from the unauthorized access. Data should only visible to the sender and receiver of transmitted data, and they should be hidden from hackers. Hiding data is nothing more than protecting the data in some medium or encrypting the data. There are many techniques that use the concept of hiding data; cryptography and Steganography are among them.

The problem statement of our project is "Confidential log in to real user using Visual Cryptography and upload encrypted data on Database System using Steganography".

The main focus of this project is to develop a Confidential Login by real user using Visual Cryptography and create encrypted data on Database System using Steganography.

- To design an improved Login system using Visual Cryptography to keep data secure.
- To design an application that enable the hiding of valuable data in multimedia file by means of Steganography.
- To test the the improved Login system and the application used for Steganography.

1.2 Purpose

The aim of the project is to build more secure system than previous classical security system.

2. Literature Survey

Main limitation in today's 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. 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.

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.

The image hiding method, combine the cryptography and information hiding. On the one hand, by using information hiding does not change the visual characteristic of cover image, On the other hand, by using digital signature and encryption technology of cryptography, we can make the unauthorized users can not know the location of the embedded secret information, so that the secret information cannot be extracted. The domain of biometrics authentication over error-prone networks has been examined. Since Steganography by itself does not ensure secrecy, it was combined with a chaotic encryption system. The proposed procedure, except of providing results that are imperceptible to the human visual system, it also outputs a stegno object that can resist different signal distortions, and steganalytic attacks.

3.Methodology

3.1 Visual cryptography:

Visual Cryptography is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system .We can achieve this by one of the following access structure schemes.

(2,2) Threshold VCS - This is a simplest

threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig denotes the shares of a white pixel and a black pixel. The choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white subpixel.

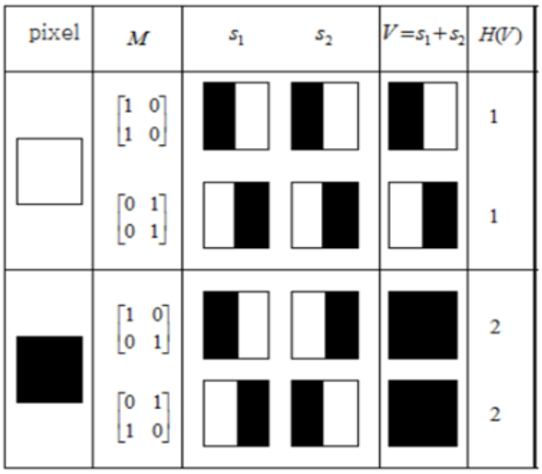

pixel
M
s_1
s_2
$V=s_1+s_2$
$H(V)$
$\begin{bmatrix}1&0\\1&0\end{bmatrix}$
1
$\begin{bmatrix}0&1\\0&1\end{bmatrix}$
1
$\begin{bmatrix}1&0\\0&1\end{bmatrix}$
2
$\begin{bmatrix}0&1\\1&0\end{bmatrix}$
2

Fig. Encrypting algorithm of 2 by 2 VCS

3.2 Steganography:

To perform Steganography, we are using Scene Change Detection Algorithm, Split Algorithm and Least Significant Bit Algorithm .

The file in which the data is to be hide is broken into frames and changes are detected which is done by using Scene change detection . Now the data which need to be hide is broken into the chunk by Split algorithm . After this the process of hiding the data starts with the least significant bit.

3.2.1 Split algorithm

Input - Watermark image
Output - Watermark image broken into chunks
Steps:-

```
1. Take watermark as input.
2. Decide number of rows and columns to split the watermark.
3. No. of watermark parts=rows*cols
4. Chunkwidth= imagewidth/cols
5. Chunkheight= imageheight/rows
6. For i=0 to rows do
7.   for j=0 to cols do
8.     imgs[Count]=new BufferedImage(chunkwidth, chunkheight, image.getType());
9.     Count ++;
10. End for.
11. End for.
```

Time Complexity - O(n*m)

3.2.2 Scene change detection

Input - Video frames and chunks of watermark
Output - Encryption of watermark into frames
Steps –

1. A few least significant bits are substituted within data to be hidden.
2. The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.
3. Let n LSBs be substituted in each pixel.
4. Let d= decimal value of the pixel after the substitution.
   d1 = decimal value of last n bits of the pixel.
   d2 = decimal value of n bits hidden in that pixel
5. If $(d1 \sim d\,2) \le (2^n)/2$
   then no adjustment is made in that pixel. Else
6. If(d1 <d2)
   $d = d - 2^n$. If(d1 >d2) $d = d + 2^n$.
6. This d is converted to binary and written back to pixel

Time Complexity - O(n)

4. Proposed System

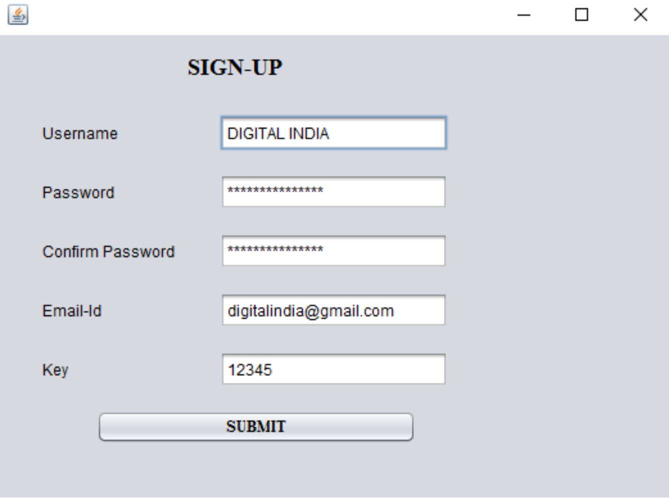
For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites. We also 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. For implementing Watermarking Technique, we are using SCD, LSB, Split algorithms.

The overall system design consists of following modules:

a. Registration phase,
b. Login phase,
c. Steganography Phase.

(a) Registration phase

To work with this application first user needs to Sign up. In Sign-up user needs to choose the Username and password along with this user need to enter email id and along with that to generate the CaGP user need to enter a special key which contains the string made of A-Z, a-z,0-9 combinations.


SIGN-UP

Username: DIGITAL INDIA

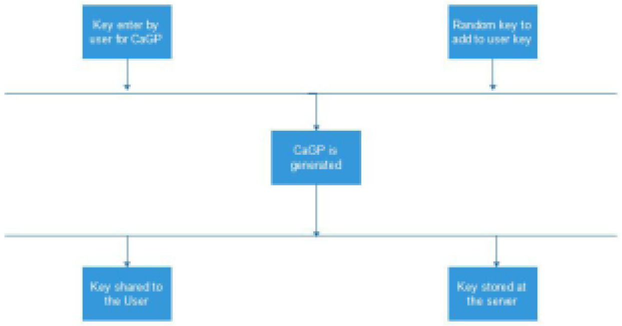
Password: ***************

Confirm Password: ***************

Email-Id: digitalindia@gmail.com

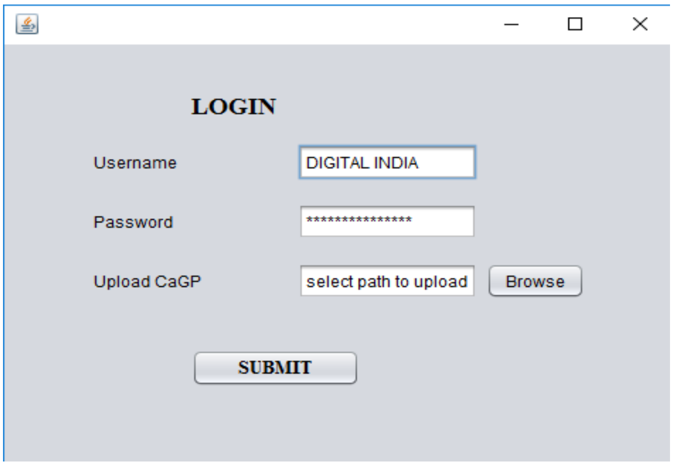
Key: 12345

At server side the key is generated by adding a random key which is made from combinations of A-Z, a-z,0-9 and then the key is generated in the form of CAPTCHA by using Visual cryptography. The generated CaGP is then mail to user for further process.



(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) and Password. Then the user is asked to enter his CaGP which is kept with him.

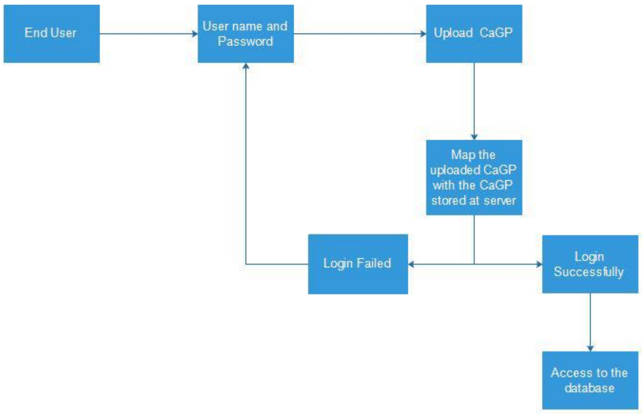

LOGIN

Username: DIGITAL INDIA

Password: ***************

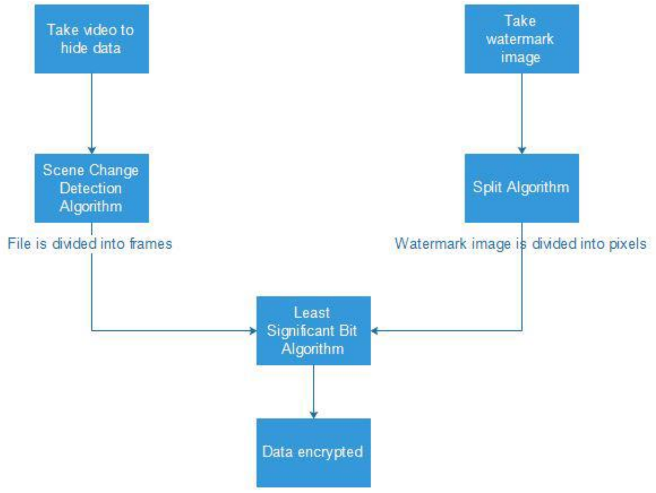
Upload CaGP: select path to upload

Now the entered CaGP is verified at server site, then user gets access to the application.



(c) Steganography Phase

Now user needs to upload the data that he wants to hide, along with he needs to upload a file in which he wants to hide the data. After uploading the data, the actual process starts. Following phase shows the exact flow. The effectiveness of this scheme is verified through a series of experiments.


Take video to hide data
Take watermark image
Scene Change Detection Algorithm
Split Algorithm
File is divided into frames
Watermark image is divided into pixels
Least Significant Bit Algorithm
Data encrypted

Firstly, the file in which the data is to be hide is broken into frames. This is done by using SCENE CHANGE DETECTION ALGORITHM. Now the data which need to be hide is broken into the chunk by SPLIT ALGORITHM. After this the process of hiding the data starts with the Least Significant Bit(LSB).

5. Results & Discussions

Application will be able to successfully encrypt the data into the file with the help of data provided by user. The data generated is not easy to detect normal human's eyes and it provide security from intruders and hackers. Because of the modified Login system and with the help of Scene Change Detection(SCD), the system will be more secure than previous one and the valuable data of user will not be compromised.

6. Conclusion

The application that we have built has a more secure Login system and data is protected from intruders and hackers. The data that user want to keep safe, secure and preserve is done by hiding it in in another file without destroying the file used to hide. The safety measures, legal are all maintain without exploiting the rules.

Thus, on the basis of literature survey and by analyzing the existing system, we have come to a conclusion that the proposed system will not only provide the secured Login to system but also it will help to keeps its data safe.

ACKNOWLEDGEMENT

We would like to thank the publishers, researchers and Ms. A.S Deokar for their guidance. We would also thank the college authority for providing the required infrastructure and support. Last but not the least we would like to extend a heartfelt gratitude to friends and family members for their support.

REFERENCES

[1] CAPTCHA as Graphical Passwords A New Security Primitive Based on Hard AI Problems Bin B. Zhu, Je. Yan, Guanbo Bao, Maowei Yang, and Ning Xu

[2] An Improved Method for LSB Based Color Image Steganography Combined with Cryptography 1Xinyi Zhou, 2Wei Gong, 3WenLong Fu, 4Lian-Jing Jin 1,2,4Information Engineering School, Communication University of China, CUC 1,3Neuroscience and Intelligent Media Institute, Communication University of China Beijng, China xinyi

[3] Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks KLIMIS NTALIANIS1, (Member, IEEE), AND NICOLAS TSAPATSOULIS2, (Member, IEEE) 1Department of Marketing, Athens University of Applied Sciences, Athens, Greece 2Department of Communication and Internet Studies, Cyprus University of Technology, Limassol CY-3036, Cyprus CORRESPONDING AUTHOR: N. TSAPATSOULIS

[4] A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY Mounika Reddy.M1, Madhura Vani.B2 Student, Department of CSE, MLRIT, Hyderabad, India 1 Asst.Professor, Department of CSE, MLRIT, Hyderabad, India

[5] A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework Qia Wang, Wenjun Zeng, Fellow, IEEE, and Jun Tian, Member, IEEE

[6] Security Enhancement in Image Steganography a MATLAB Approach M. Kameswara Rao, K. Pradeep Reddy and K. Eepsita Saranya Middle-East Journal of Scientific Research 23 (2): 357-361, 2015 ISSN 1990-9233IDOSI Publications,2015 DOI:10.5829/idosi.mejsr.2015.23.02.22127 Security Enhancement in Image Steganography a MATLAB Approach M.Kameswara Rao, K. Pradeep Reddy and K. Eepsita Saranya Middle-East Journal of Scientific

Research 23 (2): 357-361, 2015 ISSN 1990-9233IDOSI Publications, 2015 DOI:10.5829/idosi.mejsr.2015.23.02.221

[7] LSB Based Audio Steganography Using Pattern Matching Mr. Ratul Choudhary and Prof. Samir Kumar Bandyopadhyay Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 3159-0040Vol. 2 Issue 11, November 2011