ISSN No: - 2456 - 2165

Visual Cryptography with Image Watermarking

Prof. S.V. Shelke
Assistant Professor,
Bharati Vidyapeeth's College of Engineering for Women,
Pune, India

Vrushali Sonawane
Bharati Vidyapeeth's College of Engineering for Women,
Pune, India
vrushalisonawane45@gmail.com

Prerna Dinkar
Bharati Vidyapeeth's College of Engineering for Women,
Pune, India
prerna182@gmail.com

Abstract :- Visual Cryptography is a technology that is used to mask the secret image into transparencies and these transparencies are distributed to the intended recipients. A novel video watermarking scheme based on visual cryptography and scene change detection in discrete wavelet transform domain is proposed. In this we provide the image based authentication that can do login. 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. Main objective of this system is to provide security for information using cryptography with video watermarking.

I. INTRODUCTION

Some of the serious work needs to be done in order to maintain the availability of multimedia information but in the mean time industry must come up with ways to protect the intellectual property of creator, distributer, or simple owner of such data. This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital images protection schemes. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest. Some features of robust watermarking are Visibility, Robustness, Security and capacity. Areas where watermarking can be used are broadcast monitoring, copy protection, data authentication and data hiding.

II. SYSTEM ARCHITECTURE

There are four steps involved in the procedure. First step include sign up process, the person who wants to send and receive the data needs to sign up to the portal and then login . In the second step once logged in to the system person insert the image to be hidden and then the password is generated. Third step is otp generation and matching. And the last step is the transaction or decryption.

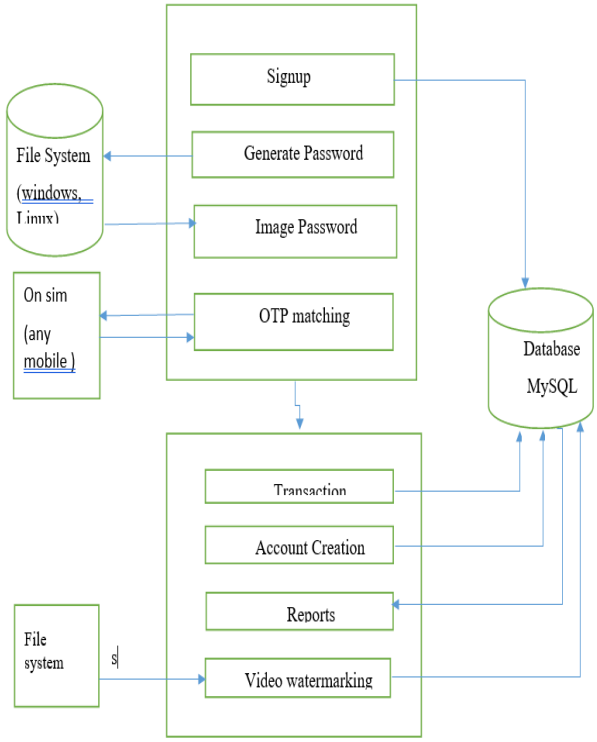

Fig 1. System Architecture For Cryptography

III. REQUIREMENT SPECIFICATION

A. Hardware Requirements

- RAM 4GB
- Hard Disk 500 GB

B. Software Requirements

- Operating system: Windows version 7.
- Languages: Java
- Software with version:
  - JDK 7 or above
  - Net Beans 7 or ab
- Database Proposed: MySQL

ISSN No: - 2456 - 2165

IV. TECHNOLOGIES TO BE USED

A. Steganography Algorithm

It is the practice of hiding secret data into an Image. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

B. Advanced Encryption Standard (AES) Algorithm

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

The features of AES are as follows:

- Symmetric key symmetric block cipher.
- 128-bit data, 128/192/256-bit keys.
- Stronger and faster than Triple-DES.
- Provide full specification and design details.
- Software implementable in C and Java.

- *C. K-N Sharing*

Visual cryptography is a method offering a plan which uses pictures circulated as shares in such a way that when the shares are stacked, a sensitive or secrete image is uncovered. According to extended visual cryptography, the offer pictures are built to hold the scattered images together, simultaneously opening a way to assist biometric security and visual cryptography methods.

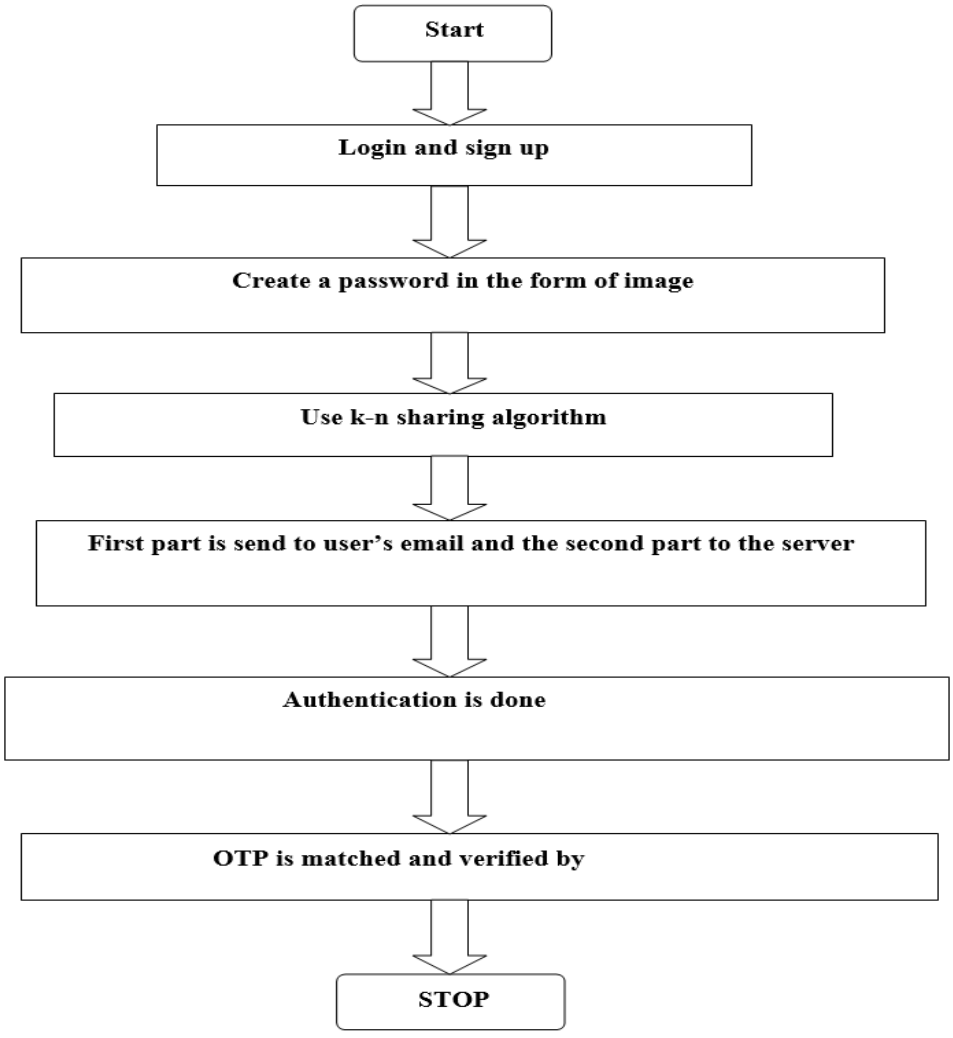

Fig 2 System flowchart

V. SOFTWARE DESIGN

A. Java Development Kit

The Java Development Kit is a collection of tools that developers use to deploy applications written in Java. We looked at JDK Version 8 for 32-bit Windows.

B. Net Beans

Net beans is a software development platform written in Java. The Net Beans Platform allows applications to be developed from a set of modular software components called *modules*. The Net Beans IDE is primarily intended for development in Java, but also supports other languages, in particular PHP, C/C++ and HTML5.

VI. OVERALL DESCRIPTION

A. Product Perspective

- Steganography is used for embedding the data inside the image and Cryptography is used for cipher text to rearrangement of the text.
- System consists of three steps: K-N sharing, OTP generation, Video watermarking.

B. Product Function

- In this system there will be the two user's one receiver and second is sender.
- Sender will send the data with image that contains the embedded image.
- Receiver will retrieve the data by sending the image as key and then image key is match the data is retrieve and store in to the file.
- User registration contains the image as password and the image password splits into the two parts using K-N Sharing algorithm.
- User authentication contains to send the user share on to the mail and share contains the watermark text for matching purpose.
- If image match found next step is OTP sending on to mobile number.
- If OTP is match then the bank system start that contains the functionality of video watermarking.

C. User Characteristics

- User Registration and user login form contains the image selection.
- Video and data file selection form for watermarking the text of file .

D. Constraints

- Registration time image size must be 50X50.
- Internet connection for getting OTP on mobile.
- This is a Standalone application.

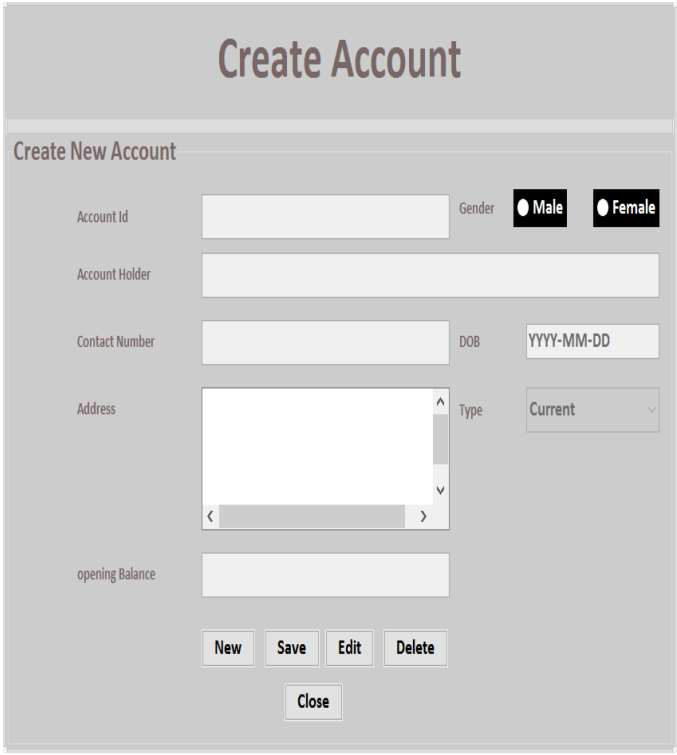

Fig 3. Account Creation

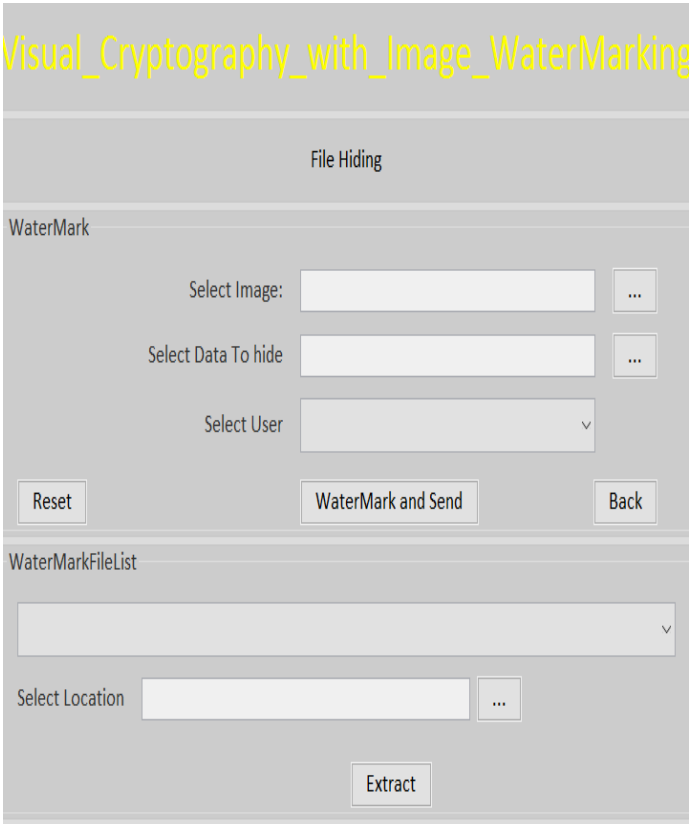

Fig 4. File Hiding

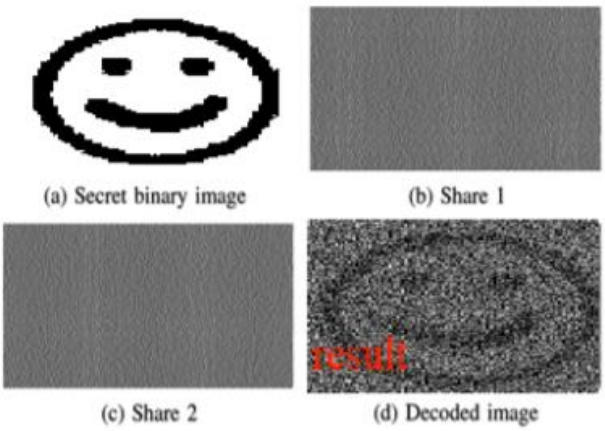

Fig 5. Random pattern of encoded image with two shares. Resulted image is decoded image by the overlaying of generated transparencies

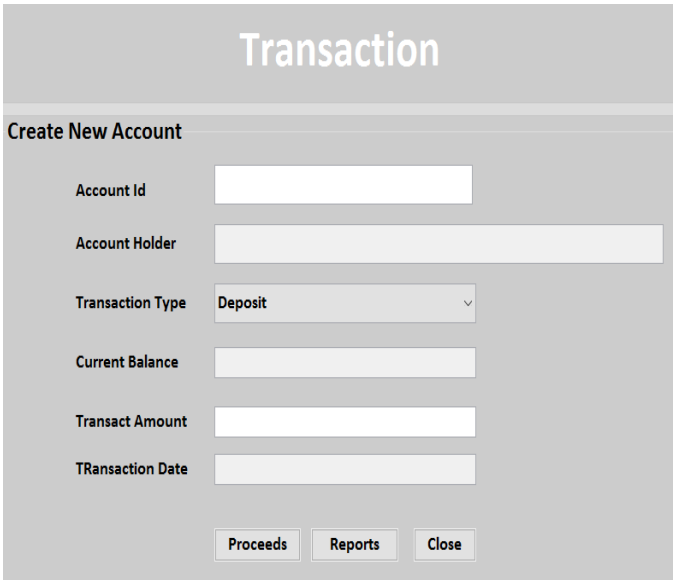

Fig 6. Transaction

VII. CONCLUSION

In this system we have implemented cryptography with image water marking. This system avoids the cyber attack or third party handling of the secret data we share to a specific person we wish to send. Using the KN sharing algorithm has enhanced the security of the secret data by diving it into two different share using time stamp. Cryptography has proven to be a simple, robust and non-intrusive watermarking technique.

VIII. FUTURE SCOPE

Visual cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended recipient even realizes the original image, a form of security through obscurity. System provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption. The scope of the System provides a friendly environment to deal with images.

REFERENCES

1) Scott Wolchok , Eric Wustrow, Dawn Isabel and J. Alex Halderman (2012) “Attacking the Washington D.C Internet Voting System” , In Proc. 16th Conference on Financial Crytography And Data Security.

2) Rajendra Basavegowda, Sheshadri Seenappa (2013) “Electronics Medical Report Security Using Visual Secret Sharing Scheme” , UKSim 15th International Conference on Computer Modelling and Simulation Proceedings.

3) B Surekha , Dr G N Swamy, Dr K Srinivasa Rao, A Ravi Kumar “A Watermarking Technique based on Visual Cryptography ” Journal of Information Assurance and Security4(2009).

4) Saleh Saraireh “A Secure Data Communication System using Cryptography and Steganography”