NOVEL ALGORITHM FOR OBJECT BASED PASSWORD TECHNIQUES USING DISTANCE BASED CALCULATION

Omveer Singh[1], Dushyant Singh[2], Monika Modi[3]
[1]M.Tech Scholar, [2,3]Assistant Professor.
Department of Computer Science & Engineering Chandravati Group of Institutions, Bharatpur

Abstract: Authentication is always an issue when securing an important resource. The important information is required to be protected from the unauthorized access. In our research, we have presented the novel scheme for using the object as the password and validating images using the distance based calculation providing the more precise method or way of authenticating the user.

Keyword: Object Detection,Object Password ,Jama, Distance Based Image Comparison.

I. INTRODUCTION

Human factors are regularly considered the weakest connection in a computer security system. There are three noteworthy ranges where human-computer interaction is imperative: authentication, security operations, and developing secure systems. Here we concentrate on the authentication problem.

The most widely recognized computer authentication strategy is for a client to present a client name and a content secret word. The vulnerabilities of this technique have been outstanding. One of the principle problems is the trouble of recollecting passwords. Thinks about have demonstrated that clients tend to pick short passwords or passwords that are anything but difficult to recollect.

1.1 Object Detection Methods

A. Background Subtraction

This strategy is especially a regularly utilized procedure for movement segmentation as a part of video pictures. It recognizes moving districts by performing total differencing between the present edge pixel-by-pixel and a reference background picture that is delivered by averaging outlines after some time in an introduction period [4][10]. The fundamental thought of background subtraction strategy is to instate a background through background demonstrating and after that subtracting current edge with background edge to identify moving objects. Besides, background picture must be overhauled so it can adjust to the conditions as far as changes of light, wind movement or impediment of different undesirable objects. This strategy is less perplexing and simple to acknowledge, additionally precisely extricates the attributes of target object. However this technique is delicate to the change of outer environment. Background subtraction techniques can be further partitioned into a few different calculations: Frame contrast strategy, Approximate median, Running Gaussian normal and Mixture of Gaussian [4] [10]. The casing differencing strategy is the least difficult type of background subtraction. In this technique essentially current casing is subtracted from the background outline. In the event that the total contrast in pixel values for each pixel is more prominent than an edge Ts, then pixel is considered as a part of the closer view [4]. In Approximate median strategy, the median separating cushions the past N casings of video information. Background casing is then computed from the median of the cushioned edge and the background is subtracted from the present casing to deliver frontal area pixel. This technique checks whether the pixel in the present casing has an esteem that is bigger than the relating background pixel. In the event that that is the situation, the background pixel is increased by one. Nonetheless, if the pixel in the present edge has an esteem that is littler than the comparing background pixel, the background pixel is decremented by one [4][7]. The Running Gaussian normal calculation depends on fitting a Gaussian likelihood thickness work (PDF) to the keep going n pixel's qualities.

This strategy is processed with a specific end goal to abstain from fitting the PDF sans preparation at the season of each new edge [4]. The mixture of Gaussian is a strategy that can deal with multimodal dispersion. In this technique all objects can be sifted through and every pixel area is spoken to by a mixture of Gaussian capacities that meet up to frame a likelihood dissemination work [4].

Background subtraction has mainly two approaches:

1. Recursive Algorithm

Recursive strategies [3] don't keep up a buffer for background estimation. Rather, they recursively redesign a solitary background display in light of every info outline. Thus, input outlines from far off past could affect the present background demonstrate. Contrasted and non - recursive strategies, recursive systems require less capacity, however any blunder out of sight model can wait for an any longer timeframe. This system incorporates different strategies, for example, inexact median, versatile background, Gaussian of mixture

2. Non-Recursive Algorithm

A non-recursive method [6] utilizes a sliding-window approach for foundation estimation. It stores a cradle of the past L video edges, and gauges the foundation image in light of the worldly variety of every pixel inside the cushion. Non-recursive systems are exceedingly versatile as they don't rely on upon the history past those casings put away in the cushion. Then again, the capacity prerequisite can be huge if an expansive support is expected to adapt to moderate moving movement.

B. Temporal differencing

This strategy utilizes a few adjoining outlines in light of time arrangement image to subtract and gets distinction images. It is especially like foundation subtraction, after the subtraction of image it gives moving target data through threshold esteem. This strategy is basic and simple to actualize contrasted with different calculations of moving article detection. Be that as it may it is profoundly helpless against dynamic scenes, it for the most part comes up short in identifying entire important pixels of a few sorts of moving articles. This strategy is not pertinent for still questions detection, complex scenes calculation and can't be utilized for real time applications [4] [7].

C. Optical flow

Optical flow [7] method uses the motion target of the vector characteristics which changed with time to detect motion area in image sequences. Optical flow is a dense field of displacement vectors which defines the translation of each pixel in a region. It gives better results under conditions of moving camera, but this algorithm is very complex and complicated computation. However, most flow computation methods are computationally complex and very sensitive to noise, and cannot be applied to video streams in real time without specialized hardware [13].

D. Multi-component Object Detection Method

In this method two phases are there,

1. Training phase
2. Detection phase[2].

In the training phase, a two-layer model is trained to capture and aggregate the components of an object category from data. Each first-layer model is a binary classifier trained with a seed and a list of aligned objects with the seed based on keypoint. A second-layer classifier takes the outputs of these component classifiers as input, and produces a final category-level classification score. In the detection phase, bouncing boxes are created for each picture utilizing determination scheme. In the wake of scoring these crates with two-layer show, non-greatest concealment is connected to create last detection comes about. The segment models which get are both simple to learn and profoundly ready to perceive little contrasts. A moment layer classifier is found out to whole the yields of part models into conclusive scores.$H(C,i) = \sum S(a) \times \text{Area}\,(B(a)\ \Omega\ B(C)\ ) \times 1(\ I(a) = I\ )$

$\text{Area}(\ B(a)\ )$ Eq. 1

The algorithm achieves good imperceptibility and robustness for object detection[2].

E. Multi Class Hough Transform Approach

This approach is utilized for distinguishing adaptable multi-class object[3]. Versatility of question detectors as for the quantity of classes is a vital matter for applications where numerous protest classes should be recognized. The single-class detectors give serial many-sided quality to assessment and the multi-class detectors compel all articles without a moment's delay, lessens identification accuracy. To defeat these confinements, an adaptable multi-class identification approach is utilized which measures sub-directly with the quantity of classes without diminishing the location accuracy. As conveyed unfair components are measured by adapting every one of the classes and recognition is additionally performed for all classes parallel, brings about great arrangement, and increment the exhibitions of the multi-class protest location.

For bunching, it changes it into a symmetric difference matrix D by,

$D = 1 - \frac{1}{2}\ (\ S + ST\ )$ Eq. 2

This approach also benefits from sharing features and an automatically built category taxonomy for robust scalability without degrading accuracy[3]. This algorithm improves the classification accuracy for detecting multi-class object.

F. Latent Hough Transform (LHT)

Latent hough transform based object detection technique take in a codebook of voting components, for example, the picture highlights, overwhelming picture pieces are so on which are extricated and coordinated in order to encode the area and size of the object in the image[4]. This transformation permits fractional perception of the preparation objects to convey a solitary object theorem and delivers wrong positives by amassing votes that are predictable in area yet conflicting in different properties like pose, color, shape or type. To beat these disadvantages, the Hough transform is utilized with inert factors as a part of order to enforce consistency among votes. Therefore, the votes which take after the task of the dormant factors are considered to support a solitary theory and Latent Hough Transform based preparing approach which has numerous weights assignments is connected for getting better detection precision. The approach can enhance the imperceptibility and robustness extremely well.

G. Boosted Haar Cascade Technique

This procedure is utilized for sliding window object detection without spatial bunching. This strategy attracts thoughtfulness regarding the way that now a day sliding window object detection procedure gets to be exceptional because of its flexibility with critical detection performance. [4].

1.2 Security Attacks(Second Section)

Brute force search

The main defense against savage constrain hunt is to have an adequately huge secret word space. Text-based passwords have a secret word space of 94^N, where N is the length of the watchword, 94 is the quantity of printable characters barring SPACE. Some graphical secret word techniques have been appeared to give a watchword space like or bigger than that of text-based passwords. Acknowledgment based graphical passwords have a tendency to have little secret key spaces than the review based methods.

It is more hard to complete an animal constrain assault against graphical passwords than text-based passwords. The assault programs need to naturally produce precise mouse movement to emulate human info, which is especially troublesome for review based graphical passwords. In general, we trust a graphical secret key is less defenseless against beast constrain assaults than a text-based watchword.

Dictionary attacks

Since acknowledgment based graphical passwords include mouse contribution rather than console input, it will be unreasonable to complete word reference assaults against this kind of graphical passwords. For some review based graphical passwords, it is conceivable to utilize a word reference assault yet a computerized lexicon assault will be a great deal more perplexing than a text based word reference assault. More research is required around there. In general, we accept graphical passwords are less defenseless against word reference assaults than text-based passwords.

Guessing

Shockingly, it appears that graphical passwords are regularly unsurprising, a difficult problem ordinarily connected with text-based passwords. For instance, considers on the Passface system have demonstrated that individuals frequently pick powerless and unsurprising graphical passwords [19]. Nali and Thorpe's review uncovered comparable consistency among the graphical passwords made with the DAS procedure. More research endeavors are expected to comprehend the way of graphical passwords made by certifiable clients.

Spyware

With the exception of a couple of special cases , key logging or key listening spyware can not be utilized to break graphical passwords. It is uncertain whether "mouse following" spyware will be a viable apparatus against graphical passwords. Nonetheless, mouse movement alone is insufficient to break graphical passwords. Such data must be corresponded with application data, for example, window position and size, and in addition timing data.

Shoulder surfing

Like text based passwords, the majority of the graphical passwords are helpless against shoulder surfing. Now, just a couple acknowledgment based techniques are intended to oppose bear surfing. None of the review based techniques are considered ought to surfing safe.

Social engineering

Contrasting with text based secret key, it is less advantageous for a client to give away graphical passwords to someone else. For instance, it is extremely hard to give away graphical passwords via phone. Setting up a phishing site to get graphical passwords would be additional tedious.

By and large, we trust it is more hard to break graphical passwords utilizing the conventional assault methods like animal constrain seek, lexicon assault, and spyware. There is a requirement for additional top to bottom research that examines conceivable assault methods against graphical passwords.

Advance we will read about the means required and approaches utilized by specialists. At that point equipment and programming necessity will be given in detail with references.

In this section we have seen that the security is a tremendous problem that needs arrangements. There are numerous specialists who give numerous arrangements in field of security. These all are essential strides to secure the data.

In next part writing audit is given that will inform us concerning the methods and arrangements that have been utilized by the analysts as of not long ago.

Promote we will read about the means required and philosophies utilized by analysts. At that point equipment and programming prerequisite will be given in detail with references.

II. LITERATURE REVIEW

[Mohammad Ziaullah et al., 2016] This paper presented a novel architecture for Image based authentication for wireless channel [1] which is noise resilient and tampers proof. The server database stores set of images and a symmetric key is generated through Advanced Encryption Standard (AES) key generation for each user. Each user chooses an image as password from database; features are extracted from image and are encrypted with above key, and transmitted via AWGN channel with tampering and noise addition. A modified approach of authentication for image content is proposed which enhance the level of robustness and security.

[Anjitha K et al., 2015] they presented an enhanced security [3] for the CaRP (Captcha as graphical Passwords) scheme i,e CaRP with motion-based Captcha. The proposed scheme consists of enhancing the Captcha schemes with motion through video embedding technology. The Captchas are provided with random movement so that the objects will be in motion. Also changing complex background texture, leads to dynamic change in target and background characteristics distribution. Attacks based on vision techniques can be overcome. They provide users with a random set of characters (codeword) moving in a dynamic fashion, and solving the captcha by entering the correct codeword. For enhanced security, this movement will be in different trajectories. The dynamic motion creates difficulty in predicting motion.

[S.Molina Giraldo et al., 2015] They propose [4] to use background subtraction techniques to restrict the search of candidate regions to be classified as persons only over the foreground regions. Additionally, we include information about the scene spatial model in order to spread candidate regions in a more efficient way. The performance of our approach is evaluated as far as computational cost and precision by looking at against the general population locator of the OpenCV library. To this, video records from true situations drawn from open datasets are utilized.

- [Wanjari Nilima et al., 2015] The proposed system [5] used graphical password for normal authentication but in threat it is using gesture detection. Viola Jones algorithm utilized the Haar like features for facial feature detection instead of analyzing the pixels. They used just removed elements of the picture to filter two eyes, half nose and brow according to the need of venture.

[Jiaxi Wang, 2015] SURF algorithm [6] is used in include detection and OpenCV is used in programming. Picture mosaics are used in moving item detection with dynamic camera. With the change framework, picture mosaicking is conceivable and one of the mosaicking strategies can be done the work.Some techniques for include point detection and all encompassing picture mosaic utilizing OpenCV have been presented. Picture obtaining and preprocessing is important so the outcome is more precise before all encompassing picture mosaic. Each edge in video is contrasted with all encompassing foundation with identify the moving item.

[Prathamesh Timse et al., 2014] The Adaboost algorithm is used [7] for face detection and PCA is used for face recognition. If unknown person is being detected then the system will send an email to the owner of the system using SMTP. The door lock system can be accessed remotely by using dropbox account. Adaboost classifier cascades based on haar like features are used. Haar course classifier is prepared on a great many human faces which is later utilized by the classifiers to recognize faces. Indispensable picture is a technique used to compute the trademark esteems. By setting the scale increase rate higher, makes the detector run faster but if it's too high then you may jump between scales and miss faces .The minimum neighbors' threshold which sets the cutoff level for discarding or keeping rectangle groups as face or not based on how many raw detection are their in group.

[Ashish Pant et al., 2012] IPL image (IPL is the main data type of OpenCV which represents image) [8] of OpenCV are analyzed and basic library functions for image handling are used. They utilized the defined pointers to traverse all image data in order to make various operations easy. Combining with Arnold transformation the image has been encrypted. Library work is used for stacking pictures and, making window, sparing picture, making a picture. Arnold change is used for changing the directions of pixels which is called area scrambling. Multi-dimensional Arnold change is used for shading scrambling.

[Shervin Emami et al, 2012.] The application is created [9] that would enable client to access to a specific machine based on a top to bottom examination of a man's facial elements. The pre-processing techniques are applied to standardize the images that you to face recognition system. OpenCV has an in-built face detector which includes advanced capabilities – face detection, face tracking, face recognition, kalman filtering, and a variety of artificial intelligence methods in ready to use form. It provides the set of algorithms that can be packaged in a portable framework. It provides the human machine interaction when user is to be authenticated through face detection and face recognition.

III. PROBLEM STATEMENT

3.1 Objectives of study-

In the proposed dissertation we follow the following procedure, study the existing systems for authentication by review of literature, provide the more secure way to access the system, by providing the video based authentication, propose a advanced solution by capturing motion images using OpenCV ,implementation of proposed method, to analyze the results, to conclude and provide future scope.

In this chapter, we studied various research work done in this area and the problem statement derived on the basis of literature review. Now in the next chapter, we would be discussing the theoretical aspects of our target work.

3.2 Open CV

Image processing is the process of manipulating picture information keeping in mind the end goal to make it reasonable for computer vision applications or to make it appropriate to present it to humans. For instance, changing shine or differentiation is a picture processing assignment which makes the picture outwardly satisfying for humans or reasonable for further processing for a specific computer vision application.

Computer vision which goes past picture processing gets pertinent data from pictures and settle on choices in view of that data. At the end of the day, computer vision is making the computer see as humans do. Fundamental strides for a run of the mill computer vision application as takes after.

1. Image acquisition
2. Image manipulation
3. Obtaining relevant information
4. Decision making

3.3 JAMA

In the proposed usage we have made utilization of the JAMA, Open CV and Histogram Analysis of Images with a specific end goal to create and imaginative Motion Images authentication system.

JAMA is a fundamental straight polynomial math bundle for Java. It gives client level classes to building and manipulating genuine, thick lattices. It is intended to give adequate usefulness to routine problems, bundled in a way that is regular and reasonable to non-specialists. It is planned to fill in as the standard lattice class for Java, and will be proposed thusly to the Java Grande Forum and after that to Sun.

JAMA is included six Java classes:

i. Matrix
ii. CholeskyDecomposition
iii. LUDecomposition
iv. QRDecomposition
v. SingularValueDecomposition
vi. Eigen valueDecomposition.

The Matrix class gives the essential operations of numerical direct polynomial math. Different constructors make Matrices from two dimensional varieties of twofold accuracy drifting point numbers. Different gets and sets give access to sub matrices and framework components. The essential math operations incorporate lattice expansion and duplication, network standards and chose component by-component exhibit operations. An advantageous grid print technique is additionally included. Five crucial framework deteriorations, which comprise of sets or triples of grids, stage vectors, and so forth, create brings about five disintegration classes. These disintegrations are gotten to by the Matrix class to register arrangements of concurrent straight conditions, determinants, inverses and other network capacities. The five disintegrations are

- Cholesky Decomposition of symmetric, positive unmistakable grids
- LU Decomposition (Gaussian end) of rectangular systems
- QR Decomposition of rectangular structures
- Eigenvalue Decomposition of both symmetric and nonsymmetric square structures
- Singular Value Decomposition of rectangular grids

IV. PROPOSED SOLUTION

In the previous chapter, we discussed the theoretical aspects of our targeted research work. Here we will elaborate the methodology along with design specification and the details of hardware / software / tools planned to be used in the work.

4.1 Design Specification

In the proposed work we are creating the framework, which will be used for authenticating the user on the basis of the video as password. In this we will implemented the registration as well as a login process to simulate the work. In the registration process, we have create the following database table structure.

Fieldname	Description
UserName	User Name
EmailID	Email ID
Video	Capture 1

Table 1: Database table

4.1.1 Registration Process

The concept of the registration process is explained using the following steps:
1. Capture the Video using the Open CV.
2. Split the video in the frames and encrypt the image using the Image encryption algorithm.
3. Capture the details user the form and store in the database.

4.1.2 Login Process

The concept of the login process is explained using the following steps:
1. Capture the Video using the Open CV.
2. Split the video in the frames.
3. Capture the details user the form.
4. Fetch the details on the basis of the user name from the database and get the path related details from the database.
5. Decrypt the image and compare it using the Histogram based techniques and if the comparison is exceed or equal to the threshold value for the comparison then the user authentication is considered as successful.

4.3 Proposed method Algorithms

In our proposed system, the users are first registered and in the registration process, following algorithm is followed.

- Capture the Video using the Open CV.
- Enter the other details like username, email id.
- Split the video in the frames and encrypt the image using the Image encryption algorithm. And the video is split into 16 images which are stored in the folder with the same name that of the username.
- Capture the details user the form and store in the database

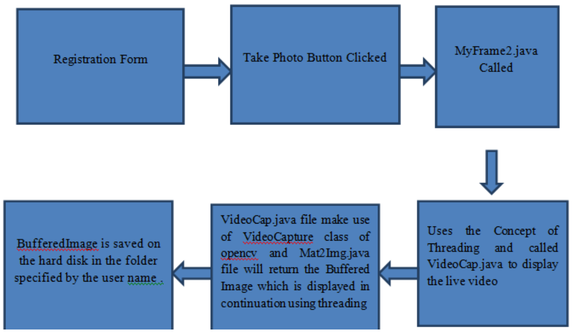

Registration Form
Take Photo Button Clicked
MyFrame2.java Called
Uses the Concept of Threading and called VideoCap.java to display the live video
VideoCap.java file make use of VideoCapture class of opencv and Mat2Img.java file will return the Buffered Image which is displayed in continuation using threading
BufferedImage is saved on the hard disk in the folder specified by the user name .

Figure 1: Registration Process

Now, the login process follows the following algorithm

1. Capture the Video using the Open CV.
2. Split the video in the frames of 16 Images.
3. Capture the details user the form.
4. Fetch the details on the basis of the user name from the database and get the path related details from the database.
5. Compare the 16 Images using Cholesky Decomposition ,LU Decomposition ,QR Decomposition ,Eigenvalue Decomposition ,Singular Value Decomposition provides by JAMA and compare it using the Histogram based techniques and if the comparison is exceed or equal to the threshold value for the comparison then the user authentication is considered as successful.

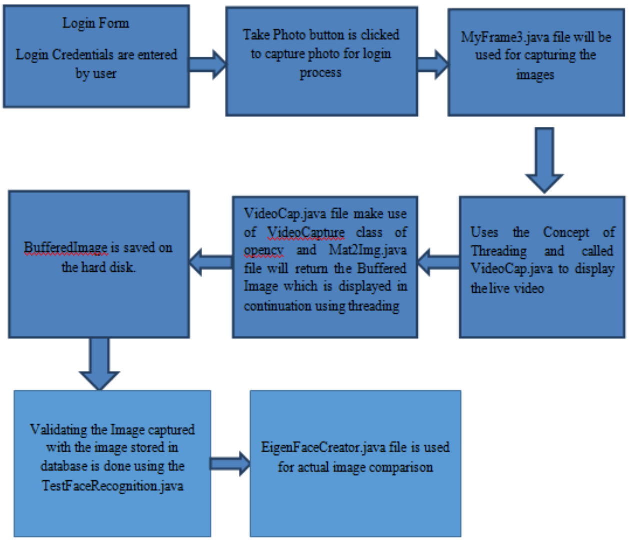

Login Form
Login Credentials are entered by user
Take Photo button is clicked to capture photo for login process
MyFrame3.java file will be used for capturing the images
Uses the Concept of Threading and called VideoCap.java to display the live video
VideoCap.java file make use of VideoCapture class of opencv and Mat2Img.java file will return the Buffered Image which is displayed in continuation using threading
BufferedImage is saved on the hard disk.
Validating the Image captured with the image stored in database is done using the TestFaceRecognition.java
EigenFaceCreator.java file is used for actual image comparison

Figure 2: Login Process

Here are the general strides to scramble/decode a document in Java:

1. Create a Key from a given byte cluster for a given algorithm.
2. Initialize the Cipher with a suitable mode (encode or unscramble) and the given Key.
3. Invoke do Final (input bytes) strategy for the Cipher class to perform encryption or decoding on the information bytes, which restores a scrambled or unscrambled byte exhibit.
4. Read an info record to a byte cluster and compose the encoded/decoded byte exhibit to a yield document in like manner.

The AES algorithm requires that the key size must be 16 bytes (or 128 piece). So on the off chance that you give a key whose size is not equivalent to 16 bytes,a java.security. InvalidKeyException will be tossed. In the event that your key is longer, you ought to consider utilizing a cushioning component that changes the key into a frame in which its size is products of 16 bytes.

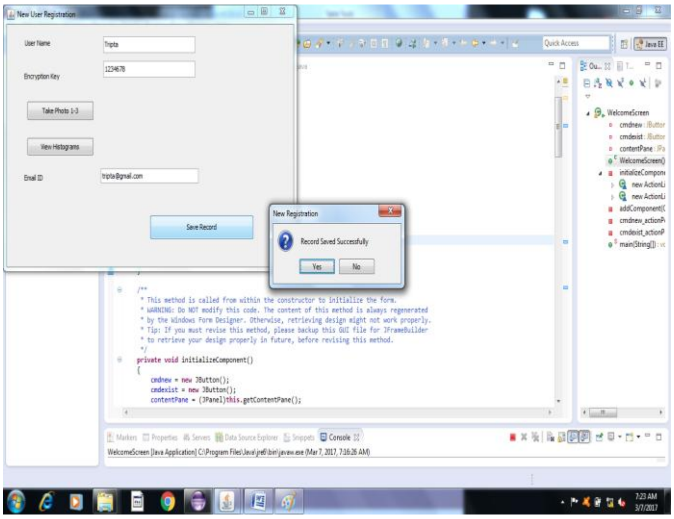
In this part we think about the goals of exhibited work and distinctive procedure used by specialists likewise introduced. We read the outline particulars and the stage required for the work. In next part we will see the outcomes. References are given toward the finish of the part.

V. IMPLEMENTATION

In the previous chapter we have seen the methodologies that have been used by different researchers. Here we are going to state configuration parameters set up for the simulation of experiment and analyze the results obtained from our experimentation.

We have performed the number of test run of our implementation to work on the objects as we as on the human face related images. Some of the sample of the registration form and images dataset and the input image at the login is given below.

6.1 Test Data


New User Registration

User Name: Tripta

Encryption Key: 1234678

Email ID: tripta@gmail.com

New Registration: Record Saved Successfully

```
/**
 * This method is called from within the constructor to initialize the form.
 * WARNING: Do NOT modify this code. The content of this method is always regenerated
 * by the Windows Form Designer. Otherwise, retrieving design might not work properly.
 * Tip: If you must revise this method, please backup this GUI file for JFrameBuilder
 * to retrieve your design properly in future, before revising this method.
 */
private void initializeComponent()
{
    cmdnew = new JButton();
    cmdexist = new JButton();
    contentPane = (JPanel)this.getContentPane();
```

WelcomeScreen [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe (Mar 7, 2017, 7:16:26 AM)

Figure 3: Registration form

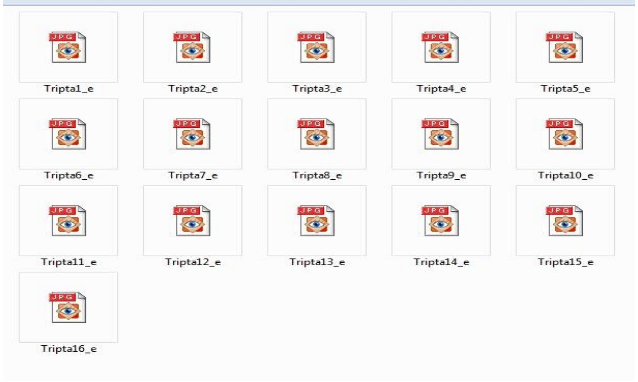
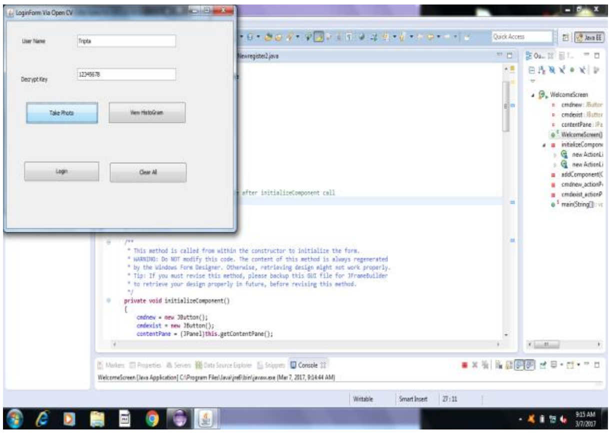


Figure4 Encrypted frames


LoginForm Via Open CV

User Name: Tripta

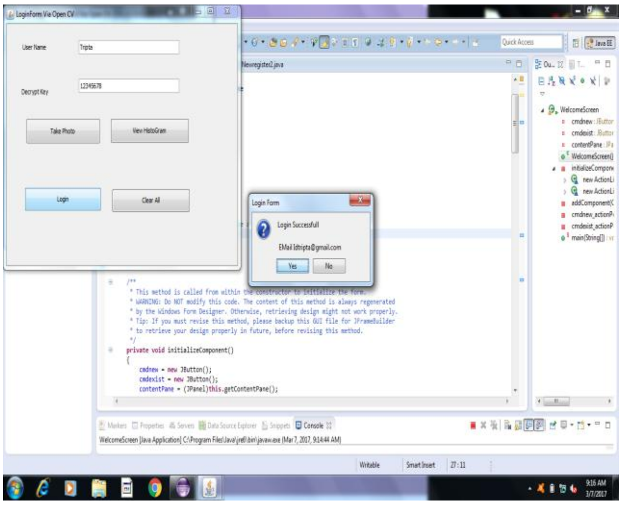
Decrypt Key: 12345678

```
after initializeComponent call

/**
 * This method is called from within the constructor to initialize the form.
 * WARNING: Do NOT modify this code. The content of this method is always regenerated
 * by the Windows Form Designer. Otherwise, retrieving design might not work properly.
 * Tip: If you must revise this method, please backup this GUI file for JFrameBuilder
 * to retrieve your design properly in future, before revising this method.
 */
private void initializeComponent()
{
    cmdnew = new JButton();
    cmdexist = new JButton();
    contentPane = (JPanel)this.getContentPane();
```

WelcomeScreen [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe (Mar 7, 2017, 9:14:44 AM)

Figure 5 Login process


LoginForm Via Open CV

User Name: Tripta

Decrypt Key: 12345678

Login Form: Login Successfull

EMail Id:tripta@gmail.com

```
/**
 * This method is called from within the constructor to initialize the form.
 * WARNING: Do NOT modify this code. The content of this method is always regenerated
 * by the Windows Form Designer. Otherwise, retrieving design might not work properly.
 * Tip: If you must revise this method, please backup this GUI file for JFrameBuilder
 * to retrieve your design properly in future, before revising this method.
 */
private void initializeComponent()
{
    cmdnew = new JButton();
    cmdexist = new JButton();
    contentPane = (JPanel)this.getContentPane();
```

WelcomeScreen [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe (Mar 7, 2017, 9:14:44 AM)

Figure 6 Login successful

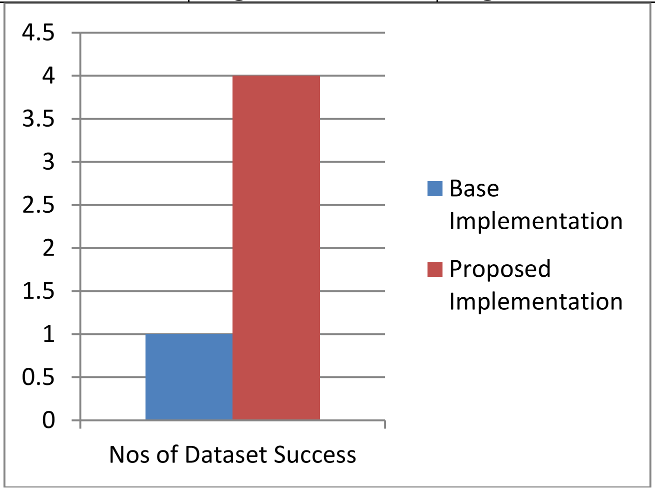
Password Authentication Scheme which we proposed lead to better results and more accurate results.

In this chapter we discussed the results obtained from the experiment. It proves that the video as a capture provides much more security than previously used methods. So it can be used efficiently. Also objectives of the experiment have been achieved.

Similarly, we have made the comparison using the 4 dataset and the result probability of correctness is better due to the concept of video capture we have adopted.

Table 2: Comparison of table Implementation.

	Base Implementation	Proposed Implementation
DataSet1	Login Failed	Login Successful
Dataset2	Login Failed	Login Successful
Dataset 3	Login Successful	Login Successful
Dataset 4	Login failed	Login Successful



VI. CONCLUSION

Security is a common phenomenon that exists in almost every application. Number of methods has been devised to deal with security issues. However, the problem is still open and requires significant research. In this thesis attempts have been made to provide a more efficient way for security.

My work is focus on to provide a method which will be more accurate as compared to existing security systems. However, the proposed scheme works better than the existing systems. In our proposed dissertation, we have presented an innovative approach of storing the password by capturing the video as the password. In order to further enhance the security we have encrypted the frames captured using the AES algorithm which are decrypted during the login process.

REFERENCES

[1] Mohammad Ziaullah et al.,"Image Feature Based Authentication and Digital Signature for wireless Data Transmission", International Conference on Computer Communicationand Informatics (ICCCI), Coimbatore India, (2016).

[2] Anne V.D.M. Kayem, "Graphical Passwords-A Discussion", International Conference on Advanced Information Networking and Applications Workshops, 596, (2016).

[3] Anjitha k et al., "Captcha as Graphical Passwords-Enhanced With Video-Based Captcha For Secure Services", International Conference on Applied and TheoreticalComputing and Communication Technology (iCATccT) 213,(2015.)

[4] S.Molina-Giraldo et al., "People detection in video streams using background subtraction and spatial-based scene modeling", IEEE, (2015).

[5] Wanjari Nilima et al., "Advanced authentication System Using Graphical Password ", International Journal of Computer Science and Information Technology (IJCSIT), 6(6),5077-5079 (2015).

[6] Jiaxi Wang et al., "Panoramic Image Mosaic based on SURF Algorithm using OpenCV", IEEE, (2015).

[7] Prathamesh Timseet al.," Face Recognition Based Door Lock System Using Opencv and C# with Remote Access and Security Features", International Journal Of Engineering and Applications (IJERA),4(4), 52-57 (2014).

[8] Ashish Pant et al.," Sophisticated Image Encryption Using OpenCV", International Journal of Advanced Research in Computer Science and Software Engineering,2(1),(2012).

[9] Shervin Emami, et al., "Facial Recognition using OpenCV",Journal of Mobile,Embedded and Distributed Systems, 4(1), 38-43 (2012).