Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

IMAGE SURVEILLANCE SYSTEM TO WITHSTAND GAINSTPLAUSIBLE DENIABILITY

Gandhile Madhuri, Dixit Sayali, Ghodake Ajinath,
Information Technology, MITAOE Alandi, Pune-India.

Abstract- *Now a day's various business organization as well as public and private sectors are storing their important data or the information in the soft copy format rather than a hard copy format. The protection of this data is very important. Security plays a vital role in securing this private data. The unauthorized access should be denied and secured environment is provided to protect the data. The normal security level includes a text based password which is not sufficient for such applications. It includes the user-name and password. The user entering the correct user name and password can access the confidential data, which may include some unauthorized users. Security level can be improved by authenticating the user by structured images along whit text based password. This can avoid the unauthorized users,But if someone forces the authorized user to access his account and tell him to perform some actions which actually he doesn't want to do it i.e. the plausible attack, then the system will not withstand for such kind of attack. To protect the system from such kind of attack the application is developed to protect the data. The application is proposed in such a way that when the user enters the user name and password images are been captured and analysis is done and if malicious object is found or not depending on that user gets logged in into guest account else at administrator account.*

1. INTODUCTION

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. The first type of authentication is accepting proof of identity given by a credible person who has first hand evidence that the identity is genuine. Second type of authentication is comparing the attributes of the object itself toknown objects of that origin. Third type of authentication relies on documentation. Authentication is provided in terms of effective security. General authentication includes user name and password not knowing about the person who is accessing the account in which information is stored. Keeping the system completely protected from crime is impossible but the traces can found by the surveillance system which can detect crime or by capturing images of the criminals after the crime. It can capture the images in dark surrounding and it uses a digital camera which has a powerful motion detector or malicious object detector. The additional security provided along with the user name and password provides more secure environment and which can give less attention of the hackers in hacking the password.

2.EXISTING SYSTEMS NEW SYSTEM

2.1Existing System

An intelligence monitor sensor is been developed in which no one is allowed to enterthat premises and if any motion is been detected the alert signals will be send so that security can take necessary actions. User name and password have a burden on users to keep in mind the long password hence a biometric is been used instead. Such systems are list below.

1. Webcam Based Intelligent Surveillance System.
2.Human Activity Recognition from Basic Actions Using Finite State Machine.
3. ComparingPasswords,Tokens, and Biometrics for User Authentication.
4. Designing Image Processing Surveillance System.

2.2 New System:

When the user will try to access the account the camera will capture the multiple images from various static angles. The dataset consist of images of malicious objects. The newly captured images produced from various cameras situated at various locations will compare the images with the malicious data objects stored in dataset. Analyzing the images is done by the Surf algorithm using the opencv library by scanning the images and comparing it with the malicious object images and newly captured images. Pluggable Authentication Module (PAM) consists of various modules which contains various functions.

3. LITERATURE SURVEY

Image surveillance is term used for provide more security to system by providing password in terms of images or motion and sequence of images. “ASops-based Surveillance System” book gives the complete information regarding to image processing and “Objects Detection and Recognition in Digital Image” gives the information about detection of objectwith containingproblems. With the reference of the paper “Lawrence O Gorman, Avaya Labs, Basking Ridge, NJ,USA, ComparingPassword, Token, and Biometric to User Authentication” and provides with a comprehensive survey of all important aspects and the latest developments in this field object detected in captured image.

4. PROPOSED METHODOLOGY

4.1 Data Collection

First stage in Image Surveillance system is Data Collection of malicious object(e.g. knife, gun, etc.) .This Images are required to doing an analysis between captured images and themselves.

4.2 Image Capturing

The second stage of the system is image capturing at the time of entering username and password. The objective of this System is to develop a system that monitors the area in which it is implemented also where we need to detect any object. For thiswebcamera is used. By combining the software and camera we can usethis system as aImage Surveillance System. TheWeb-Camera is used to capturethe images of the area in which it are being implemented.Captured images are stored in particular folder. The storedimages will be then used to find the malicious object in the images. And the malicious object sample images are store in database which are required to compare with the capturing images.

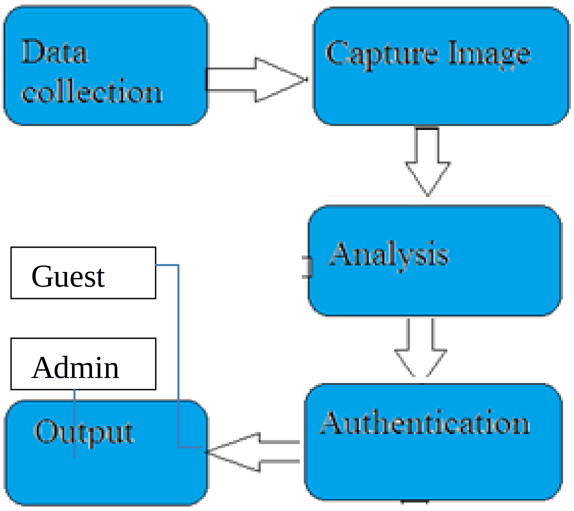

Fig1: Proposed System Architecture

4.3 Authentication

Authentication is an act of confirming the truth of an attribute of a single piece of data claimed true by an entity.The first type of authenticationis an accepting proof of identity given by a credible person who has first-handevidence that is the identity is genuine. When authentication is required of art or physical objects, this proof could be an anyfriend, any family member or colleague attesting to the item's provenance, perhaps by having witnessed the item in its creator's possession. Authentication is commonly done through the use of login passwords or pass-phrases; knowledge of such is assumed to guarantee that the user is authentic. Thus, when you are asked to "authenticate" to a system, it usually means that the you enter your username and/or password for that system.

4.4.Analysis

4.4.1.Image Analysis for Object detection

Image Analysis is the important stage in these system in which object from the captured image is detected by using SURF algorithm.

4.4.2.SURF Algorithm

In OpenCV(Open Source Computer Vision) SURF(Speed Up Robust Feature) is a local feature detector and descriptor algorithm. It can be used for doing some task like object recognition or detection, Classification. SURF is partly inspired by SIFT descriptor (Scale-Invariant Feature Transform).

1. To detect interest points SURF

Uses an integer approximation of the determinant Hessian blob detector. Points can be computed with three integer operations by using a precomputed integral image. SURF descriptor is used for locate and recognize objects.

SURF Algorithm has three parts:

1. Interest Point Detection
2. Local Neighborhood Description
3. Matching

1. Interest point Detection

The SURF approach uses Square-Shaped filter as an approximation of Gaussian Smoothing. Which is defines as:

$$S(x,y) = \sum_{i=0}^{x}\sum_{j=0}^{y} I(i,j)$$

SURF also uses determinant of the Hessian for selection of the scale. Given a point p=(x, y) in an image I, the Hessian matrixH(p, σ) at point p and scale σ and it is defined as follows:

$$H(P,\sigma) = \begin{pmatrix} Lxx(P,\sigma) & Lxy(P,\sigma) \\ Lxy(P,\sigma) & Lyy(P,\sigma) \end{pmatrix}$$

Where *Lxx(P,σ)* etc. are the second-order derivatives of the Gray scale image.

The interest point can be found in different scales, partly because the correspondence often requires images where they are seen at different scales. Images are smoothed with a Gaussian filter repeatedly. Scales in SURF are implemented by applying box filters of different size therefore scale space is analysis by up-scaling the filter size rather than reducing the image size.

$$\sigma_{approx} = \left(\frac{\text{Base Filter scale} * \text{Current}}{\text{Base Filter Size} \quad \text{filter size}} \right)$$

2. Local Neighborhood Descriptor

The goal of descriptor is to provide unique and robust description of an image feature. Description is obtained for every point of interest identified previously. The dimensionality of the descriptor has direct impact on both its computation complexity and point matching robustness or accuracy. Short descriptor may be more robust against appearance variation and thus gives too many false positives. In first step a circular region is constructed around the point of interest. And then square region is aligned to selected orientation and then extract SURF descriptors from it. And it not invariant to image rotation and hence it is faster to compute.

3. Matching

The images are been compared by the obtained descriptor points from local neighborhood descriptor and mating pairs are found.

4.5. Output

4.5.1. Login to Guest Account

When the malicious objects are detected in the in the captured images then the login will be done at guest account.

4.5.2.Login to Admin Account

When the captured images do not contain any malicious object then the login will be done at administration account.

5.FLOW OF SYSTEM AT ADMIN ACCOUNT LOGIN

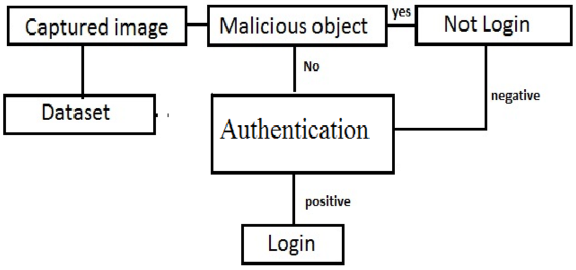

Fig2:Flow of system login at
ADMIN account

6. IMPLEMENTATION

In Linux environment we are modifying the library file , the PAM folder which consist of account files, session files, authentication files and the password file. The modified files are forced to initialize the camera when the application starts or when it starts its execution. The camera will capture the images from various views and stores the images in database. The analysis is done on these images by detection of malicious object is done and according to the result of analysis sets the user login either to the guest or administrator account.
Authentication is the first parameter on which the right user can access the account by entering correct user name and password.
Time complexity is the measure issue in every aspect it defines the performance of the application. Detecting objects in continuously changing environment is complicated, and the decision depending on the scanning of environment takes major time. To reduce the time required to do all this operation must be reduced by using OpenCV library and SURF algorithm. The number of elements used to give the decision defines the time complexity. The total time taken and the number of elements included define by the constant factor in the application. The time required to perform may vary every time according to the inputs to the application of same size. The worst case time complexity of an algorithm is T (n), which defines maximum time taken for a given set of inputs. The average case time complexity is defined by the nature of function T(n) which is exponential bin nature. Peak Signal to noise ratio (PSNR) is the ratio between the powers of corruption noise to the fidelity of it, as the signals have dynamic range the PSNR sets this range in a predefined and proper scale. It is defined by the root mean squared error method(MSE). The MSE manages the noisy approximation. When scanning the image the temporary co-ordinates are set according to the size of the image, the grids are set for scanning of image. The regarding of axis is done on the grids according to the contents and also specified region of interest on the given input of image.

7. CONCLUSION

To survive against plausible deniability we proposed an application which is used against plausible deniability attacks. So we propose a system in whichif plausible deniability happens By providing images at the time of enteringUsername and password in which malicious objects are found then User getlogin at guest account. Image analysis is done by using SURF algorithm andwhole system will be developing by modifying PAM. In proposed system,if malicious objects are found in captured image means plausible deniable happens at the time of entering user name and password then user will get login in Guest account. At that moment user will get some time to escape and within this time period system will inform to security department by providing some message or by ringing of an alarm. Like this system will be more secure against plausible deniability. Secure environment for protection of the information against unauthorized access is necessary. Text based passwords are not secure enough for such applications. User authentication can be improved by using both text passwords and structured images.

References:

[1] Lawrence O Gorman, Avaya Labs, Basking Ridge, NJ, USA,"Comparing Passwords, Tokens, and Biometrics for User Authentication", IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 2003 IEEE.

[2] BrahmanandhaPrabhuR,ArulPrabharA,GarimaBohra,Implementation of webcam based sytem for surveillance monitoring,Proceeding of ASCNT-2010,CDAC,Noida,India,Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 2003 IEEE.

[3] Oliver, N. M., Rosario, B., Pentland, A. P. (2000),"'A Bayesian com- puter system for modeling human interactions.IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(8), 831843.

[4] Makris, D., Ellis, T. (2005). Learning semantic scene models from ob- serving activity in visual surveillance.IEEE Transactions on Systems, Man and Cybernetics, 35(3), 397408.

[5] M. Howard, Designing Secure Web-Based Applications for Microsoft Windows, 2000, Microsoft Press, 2000, pp. 407-421.

[6] B. Ozer and W. Wolf, Human detection in compressed domain, IEEE Conf. on Image Processing, 2001.