Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 7 (2017), pp. 3193-3202

http://www.ripublication.com

User Signature Identification and Image Pixel Pattern Verification

Varun.S [1]
P.G Student,
Department of Computer Science Engineering
School of Computing, Sathyabama University, Chennai, India.

N.Srinivasan [2]
Associate Professor,
Department of Computer Science Engineering
School of Computing, Sathyabama University, Chennai, India.

Abstract

Online Internet applications are used widely all over the world. Especially the secured applications like banking and financial applications the basic authentication is password and one time password verification. The new system is facilitated with signature based authentication and graphical pattern authentication based on Multimodal Verification System. The new system uses contourlet based transform with co-occurrence matrix of feature generation strategy. Verification is automated by a new signature criterion. The new strategy gets the inputs of signatures from writers set of data as well as graphical pattern input in verification phase. The final outcomes are effective with secured authentication provided by means of multimodal verification using the signature and pixel pattern verification.

1. INTRODUCTION

The authentication of individual identity is mainly focussed on automating the various systems of security. The hand writing matching is used in lot of scenarios in real time

environments like banking and finance. This is the common method of identifying the person. This complex method of user identification is based on behaviour of end user hand writing. Tracking the hand writing pattern is quite complex task such that the signature written by the user can be exactly same or sometimes it might be having slight variations. And also there is a possibility of reproducing the same signature by another unknown person. So there are two possible behaviours of tracking the signature which can be written by same or different person.

Some challenges of practical and forensic process of automatic signature verification were ignored in previous hand writing matching until the last few years. There are some things that need to be followed during the hand writing matching refinement. There are two verification procedures dependent of writer and independent of writer [1] [2]. Dependent of writer creates a model for every writer, result is generated for samples and it is compared during the stages of verification. The main drawback of this model is it needs to be generated every time for new users [1]. The second approach requires limited number of reference samples for large quantity of users. During the verification step, a questioned signature is first transformed by dichotomy procedure, which will be submitted to the binary classifier that attributes the questioned signature to the accepted or rejected class [2].

2. RELATED WORKS

The experimental study reveals that in the existing internet applications, the application is authenticated by means of password and one time password verification. The verification is done by mode of password. The internet applications are widely used over all the domains. To strengthen the security over the internet applications we can use the multi modal verification pattern. Multimodal verification represents the varied authentication strategies and thereby security is enhanced.

3. PROPOSED METHOD

The proposed framework follows the multimodal verification strategy. Using the Multimodal verification, the user is validated by signature pattern and pixel point mapping.

The signature based verification and authentication is done by using back propagation algorithm of neural network. Within the Proposed system, during net banking when registering the application for the token, a signature of corresponding user is scanned and saved within the internal reminiscence of the token. The proposed new framework [Fig 1] is for verifying the handwritten signature using conjoint CT and the function dissimilarity degree [1] [2]. The verification step is carried out using best the feature dissimilarity measure for comparing signature’s resemblance. The

signatures are captured by two ways like Training set and Test set, by means the signature of user is verified. In proposed system, the implementation of Multimodal verification machine is used. The mixture of graphical based Authentication with signature verification is carried out. Neural network and Back Propagation algorithm is used for signature Verification, after authentication of signature verification, Graphical password is validated. User could be registering with two images along with its Pixels the end user has to choose the same set of Pixel Values for Authentication. The pixel values are stored and average is calculated once the user chooses the corresponding pixel area using the X and Y coordinates.

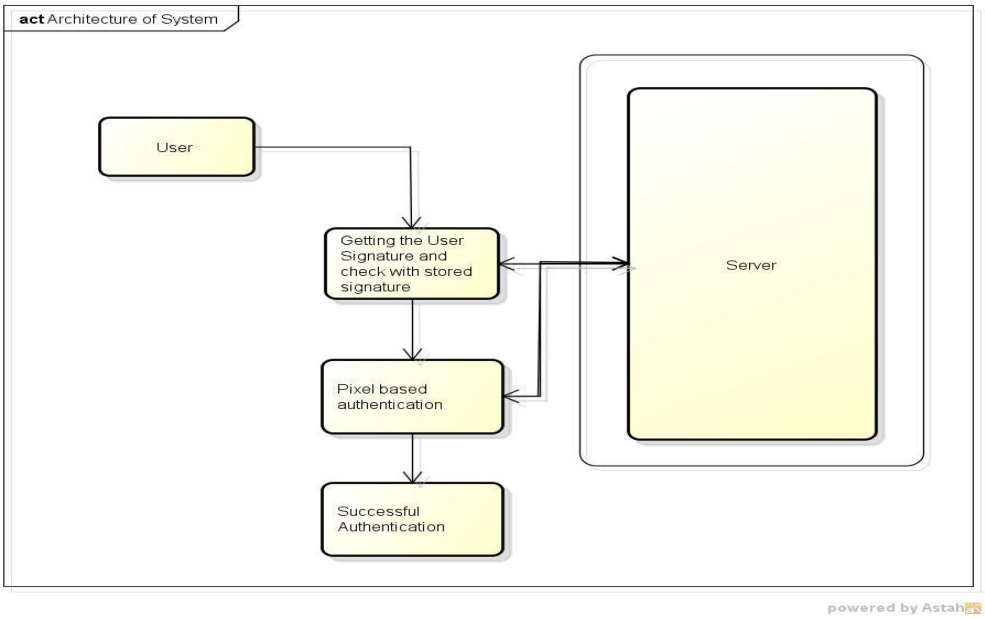

Fig 1: System Architecture

4. MODULES

User Registration

In this module, using the application the user is allowed to access the data from the Server. Here the User wants to create an account and then they are allowed to access the application. To access the Application, the Client wants to the register their details with Application Server. They have to provide their information like Name, Password, Date Of birth, Mobile Number and etc. This information will be stored in the database of the Application Server. The User is allowed to the access the application only by their provided Interface. Users register with the signature and the two images with its pixels. In this phase, the process of training the system is done by identifying the User's signature by using the signature capture device, so the user

have to give put signature to train the system to identify the correct signature to validate the user.

Server Component

The Server will monitor the client's accessing information and responds to clients requested information. The Server will not allow the unauthorized user from entering into the Network. So we can provide the network without allowing illegitimate user's activities. Also the server will identify the malicious nodes activities.

Signature Training

In this phase, the system is trained accordingly to identify the user's signature by using the mouse so the user have to give n (say n=20) times of signature to train the system, here signature device is not used which is cost effective instead mouse signature is used to validate the user.

Graphical Password

This can be done by building image verifications against specific elements for pixel-by-pixel visual verifications in tests. The image verification feature is based on an element's visual rendering rather than the properties or attributes of that element. An application with rich graphic rendering can leverage this functionality to automate some of its test scenarios that have always needed manual visual inspection to verify. The image verification in test studio allows refining verification area down to the pixel level within an element and also assigning error tolerance for the matching.

Multimodal Authentication & Transaction

In this module, design and implementation of multimodal authentication is done. By verifying the signature and pixel based images the transaction is made successful.

Computation

Training Set - A set of input &output patterns for network training.
Testing Set - A set of input &output patterns for network performance.
Learning Rate-η - A scalar parameter used to set the rate of adjustments .

To calculate the network error:
Total-Sum-Squared-Error (TSSE)

$$TSSE = \frac{1}{2} \sum_{patterns} \sum_{outputs} (desired - actual)^2$$

Root-Mean-Squared-Error (RMSE)

$$RMSE = \sqrt{\frac{2 * TSSE}{\#\,patterns * \#\,outputs}}$$

Algorithm

Weights - W
Error Value - Ev
Output - Op
Error Signals - ErSig
Weight Adjustments - WAdj

1. Choose W at initial stage radomly.
2. while Ev is large
   For every pattern of training
   a. Inputs are send to the network.
   b. Calculate the Op at neuron level.
   c. Error is calculated for Op.
   d. Estimate ErSig for pre-output.
   e. WAdj are estimated by error signals.
   f. WAdj are applied.
   Monitor the efficiency of network.

Applying Inputs from Pattern

- Feed input node with input parameter.
- Predict function of identity via nodes of input.

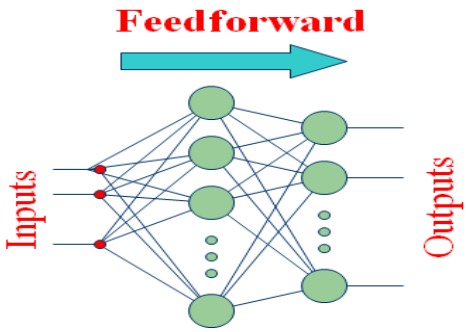

Fig 2 A pattern of Input

Output Calculation based on Pattern

Neuron - j
Pattern - Opj
Input indices - k
Weight – Wjk

$$O_{pj}(net_j) = \frac{1}{1+e^{-\lambda net_j}}$$

$$net_j = bias * W_{bias} + \sum_k O_{pk} W_{kj}$$

Example

Training set

- ((0.1, 0.1), 0.1)
- ((0.1, 0.9), 0.9)
- ((0.9, 0.1), 0.9)
- ((0.9, 0.9), 0.1)

Testing set

Use at least 100 pairs of equally spaced on the unit square and plot the results
Omit the training set (if desired)

Feed forward Network Training by Back propagation

1. Select architecture
2. Randomly initialize weights
3. While error is too large
4. Move pattern to check network output
    - Move the selected pattern to check actual network output
    - Back track error signals after estimating the errors
    - Adjust weights
5. Evaluate performance using the test set

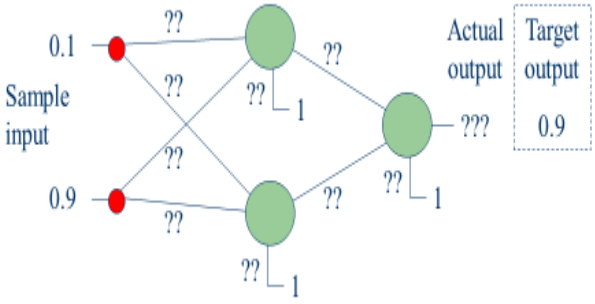

Fig 3 Neural networks with input & output

5. EXPERIMENTAL RESULTS

The following window gets the signature from the user for 'n' times as required as shown below in [Fig 4]

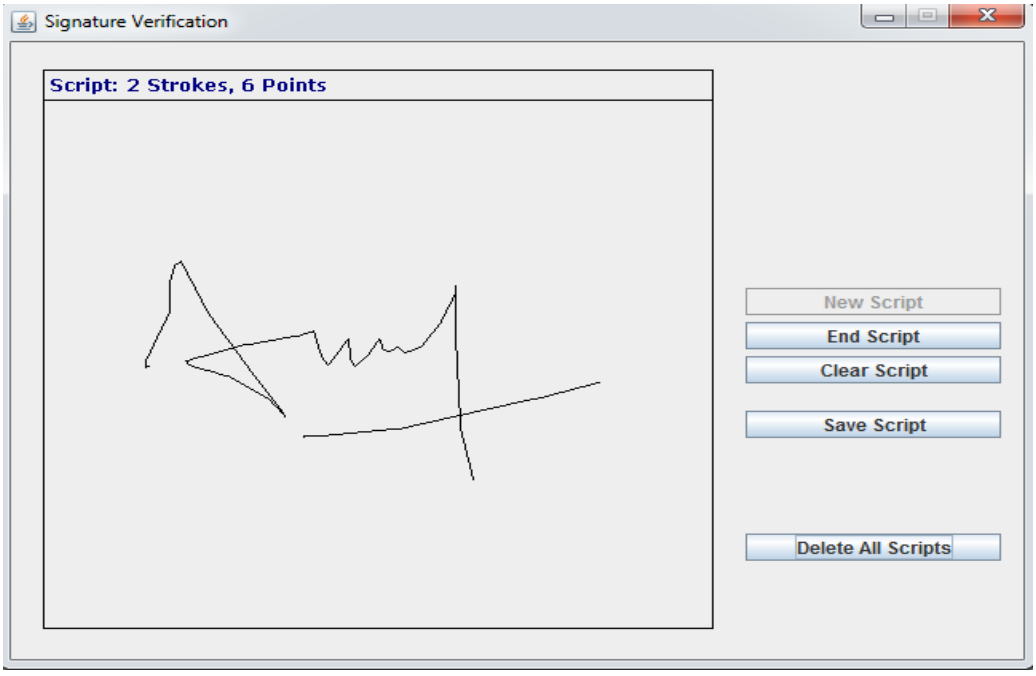

Fig 4 Screen for signature capturing.

The following window gets the graphical pattern input from the user during the registration and during the next login the user is generated with the same image and the user should select the pattern on the same image as previously given approximately. Refer below in [Fig 5]

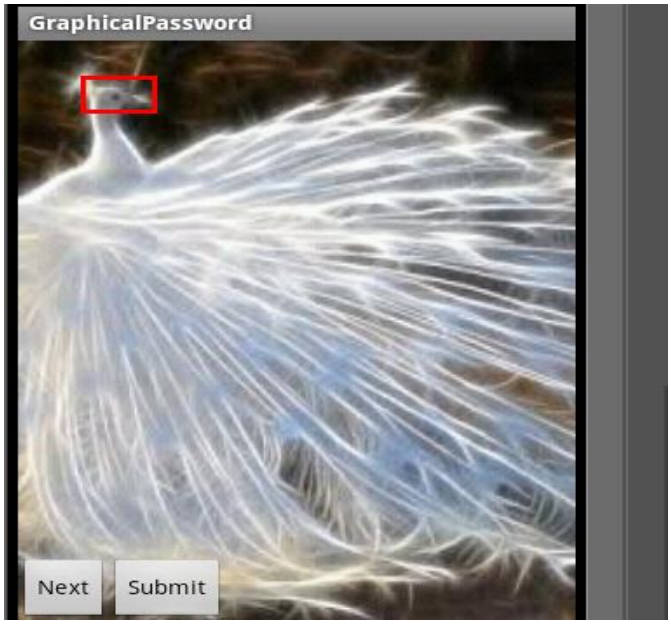

Fig 5 Graphical pattern.

After registration, during user login the user must provide the signature and graphical pattern during the secured validation. Without the proper signature verification, the user cannot able to login into the application. Refer [Fig - 6]

Fig 6. User logging without signature.

So both the modes of validation should be given and validated by the system and thus providing a secured login. Refer [Fig-7]

Fig 7. Successful Login.

6. CONCLUSION

In this paper, the online applications are provided with the additional security measures using signature verifications and graphical pattern verification. Through this secured transactions can be achieved successfully and this can be implemented with low computational cost.

REFERENCES

[1] D. Impedovo, G. Pirlo, and R. Plamondon, "Handwritten signature verification: New advancements and open issues," in Proc. 13th Int. Conf. Frontiers Handwriting Recognit., Bari, Italy, Sep. 2012, pp. 367–372.

[2] S. N. Srihari, S. H. Cha, H. Arora, and S. Lee, "Individuality of handwriting," J. Forensic Sci., vol. 47, no. 4, pp. 1–17, Jul. 2002

[3] D. Rivard, E. Granger, and R. Sabourin, "Multi-feature extraction and selection in writer-independent off-line signature verification," Int. J. Document Anal. Recognit., vol. 16, no. 1, pp. 83–103, Mar. 2013.

[4] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers," Pattern Recognit., vol. 43, no. 1, pp. 387–396, Jan. 2010

[5] S. N. Srihari, A. Xu, and M. K. Kalera, "Learning strategies and classification methods for off-line signature verification," in Proc. 9th Int. Workshop Frontiers Handwriting Recognit., Tokyo, Japan, Oct. 2004, pp. 161–166.

[6] S.-H. Cha and S. N. Srihari, "Writer identification: Statistical analysis and dichotomizer," in Advances in Pattern Recognition. Berlin, Germany: Springer, 2000, pp. 123–132.