International Journal of Engineering & Technology, 7 (3.24) (2018) 454-460

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

General Regression Neural Network Approach for Image Transformation Based Hybrid Graphical Password Authentication System

P. Baby Maruthi, Research Scholar, SPMVV, Tirupathi.

Prof. K. Sandhya Rani, Dept. of Computer Science, SPMVV, Tirupathi.

Abstract

In this digital generation, computer, and information security plays a prominent role for both individuals and business organizations. In this interconnected business environment, information is the most valuable asset and it is of utmost importance to both individuals and organizations. The task of protecting information can be achieved through authentication. Today, textual password authentication is with username and password combination commonly used for many web applications. But textual passwords are the weakest form of authentication and it is easily guessed by the attacker by applying the various techniques such as brute force, dictionary attack, etc. To provide security from vulnerable attacks, graphical passwords are another alternative authentication mechanism for replacing the textual passwords. This paper proposes image transformation based hybrid graphical password authentication model utilizes general regression neural network model and feature extraction methods for user identification. Three types of image transformations such as normal image, mirror image and shift image are considered to enhance security. In this paper, three types of feature extraction techniques such as SURF, LBP and HOG are considered for extracting image features. The performance of the proposed model is analysed, in terms of usability, security and storage space analysis and the results proved that the proposed system is resistant against various attacks like brute force, dictionary attack, shoulder surfing etc.

Keywords: *Image Transformation, Feature Extraction, Graphical Passwords, General Regression Neural Network*

1. Introduction

Today, information security has become a prominent role and it becomes a part of human life. The task of protecting information can be achieved by means of authentication. It is the process of verifying the user’s identity to whom it claims to be. Authentication provides limited access to authorized users to utilize the resources and prevents access from unauthorized persons. Now a day, most popular widely used authentication is textual password authentication. On the other hand, text passwords are easily guessed by the attackers. However, there is an alternative method for replacing the textual passwords is graphical passwords in which authentication can be achieved either by means of selecting icons, pictures or by means of drawing symbols or signature. Graphical passwords are developed based on the fact that humans can remember more pictures than text and also provides more resistant to dictionary attack, brute force attack, etc. For that reason, graphical passwords are growing in such a way in web applications and mobile applications.

2. Related Work

In paper [2], the author proposed password authentication model using Hopfield Neural Network for both textual and graphical passwords. Here, the passwords are converted into probabilistic values. This paper presents how the user authentication can be done for both textual and graphical passwords by using probabilistic values. The author claimed that the proposed graphical user authentication model provides better accuracy and quicker response time to registration and password changes.

In [3], user authentication with back propagation for both graphical passwords and text passwords is proposed. Both text password and graphical password should be normalized before it is supplied as an input to the multi forward back propagation neural network consisting of one or more hidden layers. In this model, only weights are stored in the database and the server does not maintain the password table. The training times of different networks of input can be evaluated using HNN, Back Propagation Neural Network (BPNN), Brain-State-in-A-Box (BSB), Bidirectional Associative Memory (BAM). The BAM takes less time when compared to other networks and feed forward networks.

In paper [4], the password authentication using associative memories like Hopfield neural networks (HNN), bidirectional associative memory, Brain-State-In-A-Box (BSB) is proposed. To eliminate the drawbacks in password authentication using HNN, a bidirectional associative memory (BAM) has been introduced. The other neural networks like BSB, HNN, BAM and context sensitive associative memory (CSAM) also introduced and compared with

).

their corresponding training time. CSAM takes less training time when compared to the other associative memory models. The memory capacity and accuracy results are compared and presented in this paper.

Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS) is proposed in [5] and it provides authentication for both textual and graphical passwords using neural networks. S3PAS generates random images at the time of login session. Username is given as input to the feed forward neural network and weights are stored for mapping.

3. General Regression Neural Network

A General regression neural network (GRNN) is proposed by Donald F. Specht [5] in 1991. It is basically non-linear regression theory for function approximation or function estimation. GRNN is one pass learning algorithm with parallel structure used for classification and prediction problems. It requires a fraction of time for training samples and creating the network and it is very much faster than a regular standard feed forward neural networks. It consists of four basic layers namely, input layer, pattern layer, summation layer, and output layer. The block diagram of general regression neural network is shown in figure 1. The input layer retrieves input from the input vector and transmits data to the pattern layer. The second layer is pattern layer and number of neurons in this layer is equal to the training samples i.e. the number of neurons in the input layer is equal to the number of neurons in the pattern layer. This layer computes the Euclidean distance between stored patterns and input pattern. Gaussian function is also applied in order to obtain the high accuracy estimation. The output of pattern layer are transferred as input to the next layer i.e. summation layer.

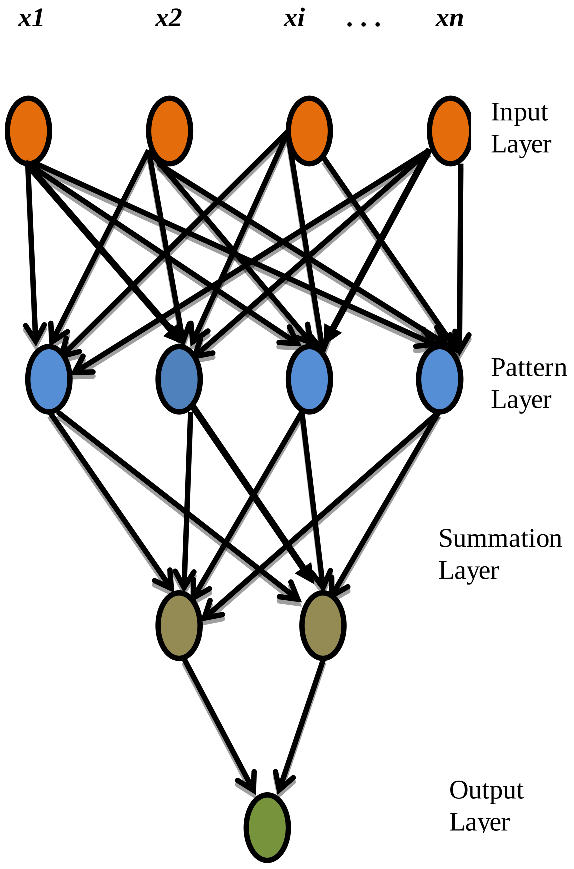

Fig. 1: General Regression Neural Network

The summation layer consists of two parts namely numerator part and denominator part. Numerator part consists of summation of product of training output data and activation function. Denominator part consists of summation of all activation functions. In the output layer, one neuron calculates the output when dividing the numerator part of the summation layer to the denominator part. The value of the output is calculated by using the following equation.

$$D_i^2 = (X - X_i)^T . (X - X_i)$$

$$Y(X) = \frac{\sum_{i=1}^{n} Y_i \, exp\left(-D_i^2/2\sigma^2\right)}{\sum_{i=1}^{n} exp(-D_i^2/2\sigma^2)}$$

Where ‘***X***’ is the input sample and X_i is the training sample. D_i^2 is the Euclidean distance between the vectors x and $x_{i.}$

In the above equation, the output function and accuracy of GRNN is pretended by smoothing factor σ. The large values of smoothing factor is appropriate for irregular data, whereas small value of smoothing factor is suitable for regular data in order to acquire good performance.

4. Feature Extraction

Feature extraction plays a significant role in the task of image identification and verification. Features are nothing but the valuable information which is extracted from the images. The primary goal of feature extraction technique is to reduce the original input image by evaluating specific features which are capable of distinguishing the other input image patterns. Image features are extracted and turns into lower dimension than the original image. Rather, storing an entire image in to the database, the proposed model employs feature extraction techniques to extract significant features from image and those features were given as target vector and username as input for training the neural network. Here, image is converted into feature vector. In this paper, three types of features were considered, such as Speed up Robust Features (SURF), Local Binary Pattern (LBP), and Histogram of Oriented Gradients (HOG) [7-13].

➢ *SURF*

SURF descriptor is used to find out the interest points in an image using determinant of hessian matrix. SURF finds extreme interest points over the space and feature direction to generate feature vectors. Thus, SURF is very useful to determine the similarity of the images.

➢ *LBP*

LBP is a texture based feature extraction technique in which the image is divided in to small regions called cells. For calculating LBP pixel values, each cell in a pixel is compared with its eight neighboring pixel values. After computing LBP values for each pixel in an image, histograms for each cell is calculated and it can be viewed as 256 dimensional feature vectors. Now, concatenate the histograms of all cells and the outcome is the feature vector of an entire image.

➢ *HOG*

The histogram of oriented gradients is another feature extraction method used for object detection and is a dense feature extraction method as it extracts features from all locations of image or from region of interested portions of an 1image. It counts the frequency of gradient orientations in local portions of an image. To get the local portions of an image, image is divided into small portions called blocks. Each cell contains fixed number of gradient orientation bins. Now, HOG is calculated for each cell consists of weighted gradient to its corresponding angular bin. To achieve robustness, normalization is done for each histogram vector in a block.

5. Proposed System

The combination of click based and text based approaches are used in the proposed model to improve the strength of graphical user authentication in terms of usability and security. The proposed model uses image transformation technique for graphical passwords and it classifies images into three different types of transformations such as normal image, mirror image and shift image. During registration, only one text password is assigned to the user after the selection of graphical password. In authentication phase, the user has to enter the text password based on the type of image transformation appeared. In addition to image transformations, General Regression Neural network (GRNN) and feature extraction techniques are considered in the proposed model which consists of two phases namely registration phase and authentication phase.

➢ *Registration Phase*

In the registration phase, new user can register here for their enrolment. User has to enter unique username and then he has to enter number of images that have to be selected as a graphical password. Image grid is displayed to the user in which user has to choose images for making the graphical password. The maximum number of images that the user has to be selected as a graphical password from the image grid is three. After image selection, server forwards a four digit text password to the user and finally the orientation screen is displayed to the user. The orientation screen helps the user to understand the concept of image transformations involved in the authentication phase and to know about how the passwords are transformed from one image transformation to the other. There are three types of image transformations such as normal image, mirror image and shift image. If the normal image is displayed in the screen, user should enter his text password which is already assigned in the registration phase. Suppose mirror image is displayed on the screen and then user should enter his text password in reverse order. If the displayed image is shift image then user should enter his text password and the last character of text password must be zero. The detailed description of registration process is explained in [1]. After registration has been completed, feature extraction techniques are applied on graphical passwords. The feature extraction techniques adopted in this paper are discussed in the following section.

a) Training General Regression Neural Network with Graphical Passwords

In the proposed model, General Regression Neural Networks are considered for graphical password authentication. For training GRNN, three types of feature extraction techniques namely SURF, LBP, and HOG are considered and these features are extracted from graphical passwords which are selected by the user. Three types of General regression neural networks are designed for three types of feature extraction techniques. Let us assume that, GRNN1 creates the network for SURF features, GRNN2 creates the network for LBP features and GRNN3 creates the network for HOG features. In the registration phase, users have a choice to select images up to maximum of three. In the proposed model, 300 significant image features are taken from each feature descriptor. Suppose user select one image as a graphical password extract 300 image features by using SURF feature descriptor and store it into a feature vector. Similarly, 300 features are extracted by using LBP feature descriptor and 300 features are extracted by using HOG feature descriptor, and store it into a separate vector. For instance, user should select two images as graphical password. Now, extract 150 SURF features from the first image and the next 150 SURF features from the second image. Now concatenate both the feature vectors into a single vector. This resultant feature vector contains 300 SURF features of both the two images. Simultaneously, extract the graphical password features from other two feature descriptors (LBP and HOG) also. Every time apply the same procedure always whenever the user selects two images as a graphical password. Suppose user select three images as a graphical password, now extracts 100 features from the first image, 100 features from the second image, and the last 100 features from the last image. The resultant feature vector is obtained by concatenating all the three image features into a single vector. Whenever the user selects three images as a graphical password, apply the same procedure and extract features from three various feature descriptors (SURF, LBP, and HOG). Likewise, collect all the users' graphical passwords, and apply three types of feature extraction techniques and then extract features by using the above procedure and store these features in to separate vectors. Three types of GRNN are considered for recognition of user given graphical passwords and it is shown in the following figure2. For the convenience of training the input vectors are converted into ASCII format.

b) Training General Regression Neural Network with Textual passwords

The proposed image transformation based hybrid graphical user authentication model utilizes three types of text passwords which are considered for three types of image transformations such as normal image, mirror image and shift image. For normal images, text passwords are assigned by the server to the user at the time of registration. For mirror images, the text passwords must be transformed in reverse order then it is called as mirror text password. For shift images, the text passwords are transformed so that the last digit of the text password must be zero.

To improve security with text passwords, three types of GRNNs are designed for three types of text passwords such as normal, mirror and shift text password. For the convenience of training, the input vectors are converted into the ASCII values of user names.

For recognition of text password which is assigned for normal image, the General Regression Neural Network GRNN4 is trained with usernames as input vector and normal text password as target vector. For recognition of mirror text passwords which is assigned for mirror images, the General Regression Neural Network GRNN5 is trained with usernames as input vector and mirror text password as target vector. For recognition of shift text passwords which is assigned for shift images, the General Regression Neural Network GRNN6 is trained with usernames as input vector and shift text password as target vector. If these networks are properly trained then three types of networks stores the pairs of usernames and three different passwords.

➢ *Authentication Phase*

The user recognition can be done through authentication phase. General Regression Neural Network approach for Image Transformation based Graphical Password Authentication System (GRNNITGPAS) uses two factor authentications. Typically, the first one is graphical password authentication and the next one is text password authentication. In order to provide more security, user needs to prove his identity by submitting two types of credentials at the time of authentication in order to improve security. In the authentication phase, user has to enter a valid username and then image grid is displayed to the user. In the first level of authentication, user should recognize the correct graphical password and also the correct order in which he had been selected at the time of registration. Once, the graphical password is verified successfully, and then user should be allowed to enter into second level of authentication. In the second level, user should prove his identity by entering the proper text password based on the displayed transformation i.e. normal, mirror and shift image.

The procedure of GRNNITGPAS system during authentication phase can be divided into three types of modules. They are Main Module, Graphical Password Verification Module and Text Password Verification Module.

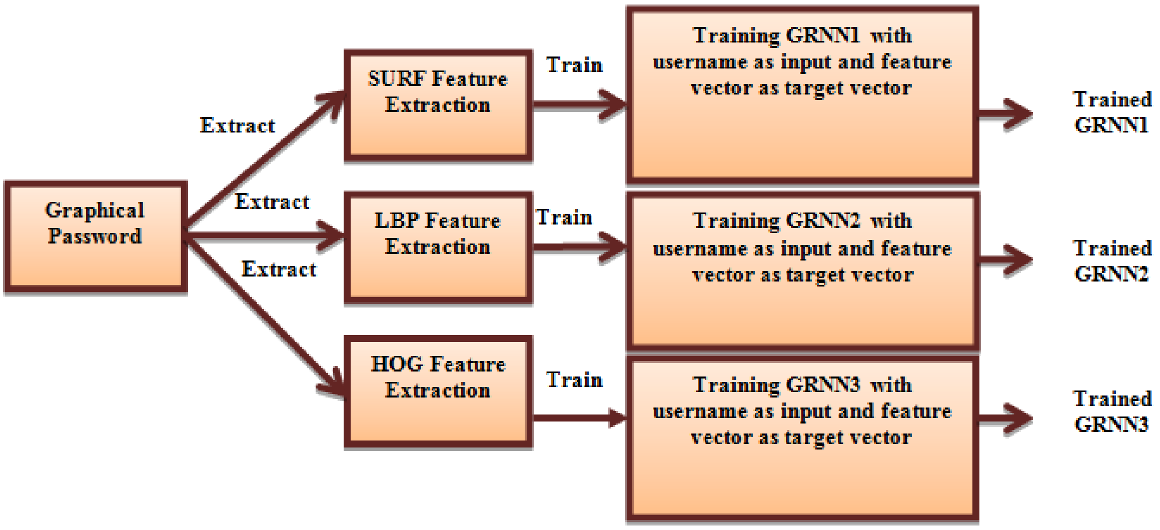
Graphical Password
Extract
Extract
Extract
SURF Feature Extraction
LBP Feature Extraction
HOG Feature Extraction
Train
Train
Train
Training GRNN1 with username as input and feature vector as target vector
Training GRNN2 with username as input and feature vector as target vector
Training GRNN3 with username as input and feature vector as target vector
Trained GRNN1
Trained GRNN2
Trained GRNN3

Fig. 2: Training GRNN for Recognition of Graphical Passwords

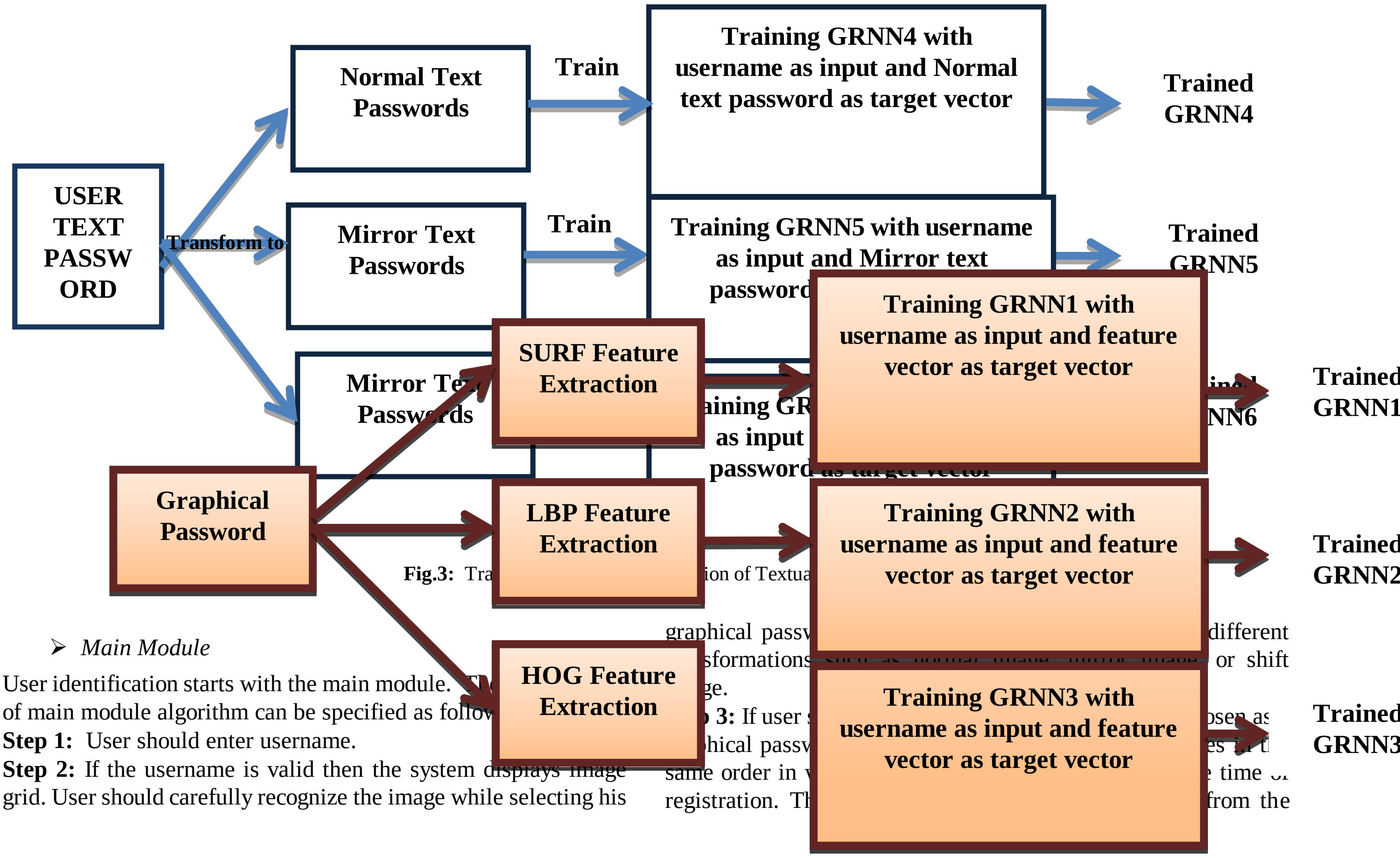
USER TEXT PASSWORD
Transform to
Normal Text Passwords
Mirror Text Passwords
Mirror Te Passwords
Train
Train
Training GRNN4 with username as input and Normal text password as target vector
Training GRNN5 with username as input and Mirror text password
aining GR as input password
Trained GRNN4
Trained GRN5
NN6
Graphical Password
SURF Feature Extraction
LBP Feature Extraction
HOG Feature Extraction
Training GRNN1 with username as input and feature vector as target vector
Training GRNN2 with username as input and feature vector as target vector
Training GRNN3 with username as input and feature vector as target vector
Trained GRNN1
Trained GRNN2
Trained GRNN3

Fig.3: Tra ion of Textua

➢ *Main Module*

User identification starts with the main module. T of main module algorithm can be specified as follo

Step 1: User should enter username.

Step 2: If the username is valid then the system displays image grid. User should carefully recognize the image while selecting his

graphical passw different sformations or shift ge.

3: If user s osen as hical passw es same order in time of registration. Th from the image grid is three.

Step 4: To determine the user selected graphical password belongs to which type of transformed image, the mean of all normal images in a grid are calculated and stored into a vector, and the value of N_i in this vector represents the mean value of i^{th} image in the grid.

Step 5: Now compute the mean value 'M' of user selected graphical password.

Step 6: Find transforming factor 'T' by using the following equation.

$T= M-N_i$

Transforming factor 'T' determines each image selected by the user from the grid belongs to which type of transformed image.

Step 7: Compute T for each image selected by the user as a graphical password.

```
If T =0 then,
    Normal image<-User selected image
    update status S='N'
    Else
        If 0< T<1 then,
            Mirror image<-User selected image
            update status S='M'
        Else
            User selected image is shift image
            Update status S='S'
```

Step 8: The user selected each graphical image and its status are given as input to the graphical password verification module.

- *Graphical Password Verification Module*

Graphical password verification module retrieves the user selected graphical password along with status from main module. The proposed model uses three types of feature extraction techniques such as SURF, LBP and HOG. The sequence of steps in graphical password verification module can be specified as follows:

Step1: The most significant three types of image features (SURF, LBP and HOG) are extracted from user selected each image as per procedure explained in 5.1.1 and it is stored in three different feature vectors.

Step 2: The ASCII value of username is given as input to the trained GRNN1. The output of the GRNN1 is compared with stored user selected graphical password.

Step 3: To compare the similarity between feature vectors across the images, compute cosine similarity, correlation, and Euclidean distance. The cosine similarity and correlation always be one for similar feature vectors and Euclidean distance approximates to zero.

Step 4: The ASCII value of username is given as input to the trained GRNN2. The output of the GRNN2 is compared with stored user selected graphical password.

Step 5: Go to Step 3.

Step 6: The ASCII value of username is given as input to the trained GRNN3. The output of the GRNN3 is compared with stored user selected graphical password.

Step 7: Go to Step3.

Step 8: Once, graphical password verified successfully, the user selected each graphical image and its status are given as input to the textual password verification module.

The procedure for text password verification module is explained below.

- *Textual Password Verification Module*

Text password verification is at the second level of authentication, when user authenticates graphical password verification successfully then, user should enter text passwords based on the transformed graphical image displayed on the screen. This module receives the user selected graphical password and it status information. The sequence of steps in text password verification module is specified as follows.

Step 1: User should recognize that the displayed graphical password belongs to which type of image transformation.

Step 2: Let us consider, the user selected one image as a graphical password and then he needs to enter one text password for one image.

2.1: If the user selected graphical password is a normal image that is displayed on the screen, then user should enter a text password for normal images which is same as already assigned in the registration phase.

2.1.1: The ASCII value of username is given as input to the trained GRNN4 and the output of the network is compared with the user entered text password.

2.1.2: If it is matched then the authentication is successful. Otherwise, authentication failed.

2.2: If the user selected graphical password is a mirror image that is displayed on the screen, then user should enter a text password in reverse order.

2.2.1: The ASCII value of username is given as input to the trained GRNN5 and the output of the network is compared with the user entered text password.

2.2.2: If it is matched then the authentication is successful. Otherwise, authentication failed.

2.3: If the user selected graphical password is in mirror image that is displayed on the screen, then user should enter a text password in reverse order.

2.3.1: The ASCII value of username is given as input to the trained GRNN6 and the output of the network is compared with the user entered text password.

2.3.2: If it is matched then the authentication is successful. Otherwise, authentication failed.

Step 3: If user selects more than one image as a graphical password, then he should enter his text password as many times number of images selected as a graphical password. But the text password is not same for all the cases and it should be differ based on the transformed image.

Step 4: If user enters his text passwords correctly then the user is authenticated otherwise authentication failed.

Three types of trained GRNN neural networks are used for textual password authentication but depending on the type of image transformation of graphical password only the corresponding GRNN trained network is invoked for text password authentication and the other two trained networks are not considered in authentication process. As only one trained network is considered, the response time of text password authentication is fast.

The performance of the proposed GRNNITGPAS model explained in the following section.

6. Experimental Results

The effectiveness of the proposed graphical password authentication system can be determined by its usability and security. Usability is much more important for developing a good user authentication model to achieve efficiency, effectiveness, and satisfaction.

- Training Time

Once, the participants were registered successfully, in order to store an entire graphical password in to the database. The proposed prototype uses three types of feature extraction techniques such as SURF, LBP and HOG. To evaluate the performance of each feature extraction descriptor, these three feature vectors are given to the three different GRNNs. The training time of three types of GRNNs is calculated and it is shown in the following Table I.

Table i: training time using grnn for graphical passwords

No. of	Training Time in secs	Total

Participants	GRNN with SURF	GRNN with LBP	GRNN with HOG	Images
20	6.79	5.25	6.18	39
50	8.89	7.34	8.32	107
100	12.72	11.89	11.93	216

In the above table, by using SURF feature descriptor, the training time of GRNN for 20 participants takes 6.79sec. By using LBP and HOG feature descriptor, the training time of GRNN is 5.25and 6.18 sec. The training time of LBP takes very less time when compared to the other two feature descriptors shown in the above table. Three types of neural networks are designed for three types of text passwords. The training time of three different GRNN by using three different text passwords such as normal text password, mirror text password and shift password is computed and it is shown in the following Table II. The training time of GRNN for three feature descriptors and the total number of participants' registration time were concluded in the following graph.

Table ii: training time using grnn for text passwords

No. of Participants	GRNN4 with Normal Text password	GRNN5 with Mirror Text Password	GRNN6 with Shift Text Password
20	1.34	1.31	1.56
50	1.43	1.41	1.66
100	1.47	1.45	1.73

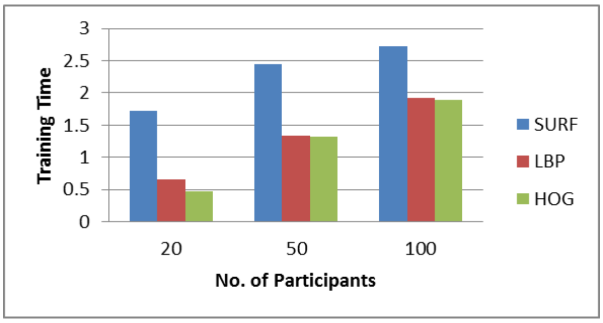

Fig 3: Login Time of GRNN with Three Feature Descriptors

In the above graph, it is clear that SURF feature descriptor takes more time to create the network than the other two feature descriptors such as LBP, HOG.

➢ *Login time*

Participants' login time also recorded in order to evaluate the effectiveness of the proposed prototype. The login time of three different feature extraction methods is determined in the following Table III.

The average login time of the proposed prototype by using SURF feature descriptor is 48.15 sec. By using LBP feature descriptor, mean is 46.95 sec and with HOG feature descriptor login time is 46.3 sec.

Table iii: login time of grnn

Total No. of Participants=20 Total Number of images=39				
Feature Descriptor by using GRNN	Login Time sec	Mean sec	Median sec	Standard Deviation
SURF	963	48.15	53	16.82
LBP	939	46.95	51	15.26
HOG	926	46.3	50	15.15

➢ *Storage Space Analysis*

The proposed prototype utilizes very less space for accommodating graphical passwords. The comparison of storing an entire image in to a database and storing the graphical password by extracting features from each feature descriptor is shown in the Table IV.

Table iv: storage space nalysis

Participants	Storage space For graphical passwords in a database in KB.	After applying feature extraction techniques using GRNN in KB.			Total Number of images
		SURF	LBP	HOG	
20	612	49	40	44	39
50	1731	118	95	104	107
100	3502	221	178	195	216

Table v: standard error rate measures

Feature Descriptor	MSE	R value	RMSD	NRMSD	MAPE
SURF	1.5050e-09	0.9999	3.8795e-05	0.0016	0.1290
LBP	0.1022	1.0000	0.3196	3.1215e-04	0.9576
HOG	1.0543e-06	1.0000	0.0010	0.0015	0.1481

The total number of images chosen by the user for creating graphical passwords by 20 participants is 39. The storage space for storing their entire graphical password (image) into a database is 612 kb. In the above table, it clearly defines that the storage space for the proposed graphical user authentication model contains graphical passwords accommodates less space by using feature descriptors and GRNN. The storage space of feature descriptor utilizes only 10% when compared to the images actually stored into a database. The proposed model occupies very less space for accommodating graphical passwords. Three types of measures were implemented to evaluate the performance; Mean Squared Error (MSE), R (Regression) value, Root Mean Square Deviation (RMSD), Normalized Root-Mean-Square Deviation (NRMSD) and Mean Absolute Percentage Error (MAPE) calculated and shown in the following table.

In Table V, it is clear that the MSE, RMSD, NRMSD, MAPE is very low and R value is close to 1 by using GRNN. The satisfactory results were obtained by using GRNN. The following section describes the common security attacks against proposed hybrid graphical password authentication models.

➢ *Shoulder surfing*

When authenticating systems placed in public places, should surfing attack is quite common and people may capture the password by viewing direct observation and also there may be a chance of recording an entire authentication session. In the proposed system, it is very hard to login even they record the entire session. The reason is images are shuffled in a grid and also image transformations also applied on the images in a grid. During login session the user has to enter text passwords which are changed dynamically based on the image transformations. Hence, the proposed system provides security against shoulder surfing attack.

- *Dictionary Attacks*

In general, by using dictionary attacks, the attacker can easily guess the textual password for authentication, whereas in case of graphical password authentication, it is not possible to guess the text password. The proposed system uses the graphical password selection as a primary authentication method on top of it, after that only the text password authentication is performed. Moreover, these text passwords are not available anywhere in the database. Dictionary attacks are completely infeasible because no pre-existing information is available regrading graphical passwords and text passwords.

- *Spyware Attack*

The proposed system protects against spyware attack because the graphical password recognition is at the preliminary step. Usernames and user credentials are not stored anywhere in the database. Attacker gets succeed only when he knows that the passwords are available and it is somewhere in the database. So, it is almost impossible for the attacker by using such type of spywares in its own and it is mostly time effort and cost overhead to the attacker.

7. Conclusion

In this paper, the proposed graphical password authentication system utilizes image transformations and also three types of feature extraction techniques such as SURF, LBP and HOG. General Regression Neural Network is adopted for graphical password authentication. Three types of GRNN are developed for three types of feature descriptors such as SURF, LBP and HOG. The response time of three types of trained GRNN for graphical passwords are measured and compared among the three types of feature descriptors. Three types of text passwords such as normal, mirror and shift text passwords are also trained by using GRNN and its response times are also computed. The performance of GRNN is measured in terms of various error measure metrics and satisfactory results are obtained. The various usability and security features are also analysed and presented in this paper. The security analysis of proposed general regression neural network approach for image transformation based hybrid graphical password authentication system is performed and obtained satisfactory results. It is also proved that the proposed system is robust against shoulder surfing, brute force attack, dictionary attack and spyware attack.

References

[1] P., Baby Maruthi and Dr.K., Sandhya Rani, Image Transformation Based Hybrid Graphical Password Authentication System (February 7, 2018). 2018 IADS International Conference on Computing, Communications & Data Engineering (CCODE) 7-8 February. Available at Elsevier SSRN: https://ssrn.com/abstract=3168339 or http://dx.doi.org/10.2139/ssrn.3168339

[2] ASN Chakravarthy, P S Avadhani, PESN Krishna Prasasd "A Novel Approach For Authenticating Textual Or Graphical Passwords Using Hopfield Neural Network", Advanced Computing: An International Journal (ACIJ), Vol.2, No.4, July 2011.

[3] ASN Chakravarthy and Prof.P S Avadhani," A Probabilistic Approach for Authenticating Text or Graphical Passwords Using Back Propagation," IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011.

[4] P. E. S. N. K. Prasasd, A. S. N. Chakravarthy and B. D. C. N. Prasad, "Performance evaluation of password authentication using associative neural memory models," International Journal of Advanced Information Technology (IJAIT), vol. 2, no. 1, pp. 75–85, 2012.

[5] Vachaspati, Pranjal, A. S. N. Chakravarthy, UCEV and Vizianagaram. "A Novel Soft Computing Authentication Scheme for Textual and Graphical Passwords." (2013).

[6] Specht D (1991) A general regression neural network. IEEE Trans Neural Networks 2(6):568–576.

[7] Jacob Toft Pedersen, "Study group SURF: Feature detection & description" Published 2011, Q4 2011.

[8] Herbert bay, T Tuytelaars, L Van Gool," Speed Up Robust Features (SURF)", Computer vision and Image Processing, Elsevier preprint,2008.

[9] Matti Pietikäinen, Abdenour Hadid ,Guoying Zhao, Timo Ahonen, " Local Binary Patterns for still images ", Computational Imaging and Vision book series (CIVI, volume 40), pp 13-47.

[10] Ojala, T., Pietikäinen, M., Mäenpää, M.: " Multiresolution gray-scale and rotation invariant texture classification with local binary patterns". IEEE Trans. Pattern Anal.Mach. Intell. 24(7), 971–987 (2002)

[11] M. Heikkilä, M. Pietikäinen, and C. Schmid, "Description of interest regions with local binary patterns", Pattern Recognition, vol.42, issue.3, pp.425-436, 2009.

[12] Awad, Ali & Hassaballah, M. (2016). Image Feature Detectors and Descriptors; Foundations and Applications. 10.1007/978-3-319-28854-3.

[13] Dalal, N. and Triggs, B. (2005). Histograms of oriented gradients for human detection. IEEE Computer Vision and Pattern Recognition(CVPR).886-893.