International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

Password Authentication Based On Modify Bidirectional Associative Memory (MBAM)

Rusul Hussein Hasan[1], Nisreen Abd Alhadi Jabr[2], Emad I Abdul Kareem[3]
[1, 2, 3] *College of Education in Computer Science, AL Mustansiriya University, Iraq. Baghdad.*

Abstract: Password authentication is popular approach to the system security and it is also very important system security procedure to gain access to resources of the user. This paper description password authentication method by using Modify Bidirectional Associative Memory (MBAM) algorithm for both graphical and textual password for more efficient in speed and accuracy. Among 100 test the accuracy result is 100% for graphical and textual password to authenticate a user.
Keyword: Associative memory, Authentication, Password

I. INTRODUCTION

Computer security has become a very important part of human life. Recently authentication has become an important issue among many access control mechanisms. Secure networks allows only intended recipient to intercept and read a message addressed to him. Thus protection of information is required against possible violations than compromise its secrecy [6]. Secrecy is compromised if information is disclosed to users not authorized to access it. Password authentication is one of the mechanisms that are widely used to authenticate an authorized user. [7]

The main limitation in using the traditional password authentication method is that, a server must maintain a password table that stores each user's ID and password. Therefore, the server requires extra memory space to store the password table. When a user logs to a computer types in the ID and password. The server searches the password table and checks if the password is legal. However, this method is dangerous. The password information table could be read or altered by an intruder. An intruder can also append a new ID and password into the table. Password table is protected using hash functions later and instead of password table [8]. Verification table containing hashed password (encrypted) will be stored in the server. Even though password is encrypted still there is a chance of modification of the verification table since it is open access environment. There are many disadvantages in using this type of approach. [9]

- Attacker can easily change the details of users by using attacks like SQL-Injection.
- Password table occupies a lot of memory.
-

To avoid this problem proposed a password authentication method using Neural Network algorithms for both alphanumeric password (textual) and graphical password. [1]

II. RELATED WORK

ASN Chakravarthy and P S Avadhani (2011) this paper described method for password authentication using graphical and alphanumeric passwords, by used Back Propagation algorithm by which the level of security can be enhanced. This paper along with test results illustrate that converting user password in to Probabilistic values enhances the security of the system. [1]

ASN Chakravarthy et al, (2011), this paper decried Password authentication using Hopfield Neural Network, which explain Hopfield Neural Network Scheme for graphical password and textual, convert the input Password into probabilistic values. In comparison to existing layered neural network

techniques, the proposed method provides better accuracy and quicker response time to registration. [3]

P.E.S.N. Krishna Prasad and et al, (2012), this paper descripted Password authentication using Context-Sensitive Associative Memory Method (CSAM). Which is proposed performance analysis of password authentication using CSAM and Associative memories using graphical Images. observe that in comparison to existing layered and associative memories techniques for graphical images as password, the CSAM method provides better accuracy and quicker response time to registration and password changes. [10]

ASN Chakravarthy and P S Avadhani (2011), in this paper descripted method using Bidirectional Associative Memory (BAM) algorithm for graphical password and alphanumeric (Text) password. Then the amount of security that provide for the user can be enhanced. This paper along with test results illustrate that user password input is converted into probabilistic values and giving to BAM improves the security of the system. [4]

ASN Chakravarthy and P S Avadhani (2011), in this paper proposed Brain-State -In-A Box for graphical password and textual password, the password will be converted into probabilistic values. And observe how to get password authentication Probabilistic values for Graphical image and Text. In comparison to existing layered neural network techniques, the proposed method provides better accuracy and quicker response time to registration and password changes.[5]

III. MODIFY BIDIRECTIONAL ASSOCIATIVE MEMORY (MBAM) [2]

The Modify Bidirectional associative memory is heteroassociative memory. MBAM consist of a small architecture using the smallest size of the network, a steps that can be done by implement the MBAM to a small number of neuron, which makes the process of computation for MBAM (i.e., learning and convergence processes) very fast and possible process in the real time. And by using MBAM avoids most limitation of BAM, except two which it the scaling and shifting problem. In additional it is increase ability for noise robust.

Similar to the BAM, the MBAM is a two layer neural network, which uses hetero-association tasks and work in two phases (learning and convergence phases). The number of node in BAM (size of network) based on the pattern length used by the network (i.e., pattern with length ten requires a BAM network of size ten), while the size of the MBAM is small and fixed (i.e., two node), the pattern divided to set of vectors with length two. Thus, MBAM will deal with each part of the pattern individually, rather of the whole pattern as one vector. This will lead to benefits of working with a small size of the network, whatever size of the pattern. MBAM architecture allow to avoid learn the same part of the pattern several times.

With a bipolar pattern representation, the elements will be either 1 or -1. The reason for choosing this length of vector is the shortest even length of any vector is two. However, just as in the traditional BAM neural network, each node is connected to every other node but not to itself. These connections represent the corresponding weight of each vector in the pattern. Although the expected number of vectors is, the number of connections will be just four, an advantage that helps deal with the smallest network size regardless of the pattern length. Technically, as with traditional BAM nets, this adapted net has two phases (learning and convergence phases) Figure 1 show MBAM architecture.

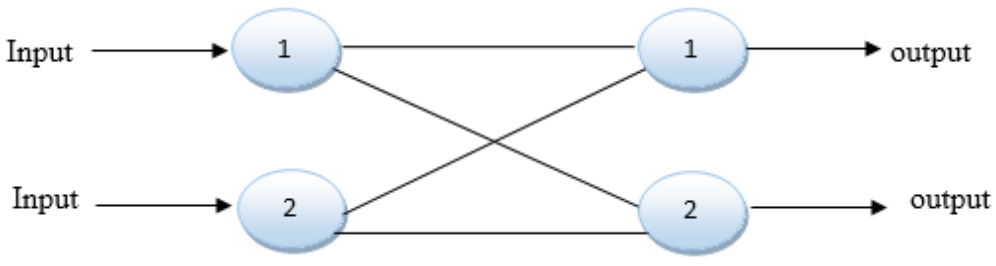

Figure 1: The Modified bidirectional associative memory (MBAM).

The next subsection present learning and convergence phase algorithm for MBAM.

3.1 Learning Phase [2]

In this section explain the learning algorithm as shown in Figure 2. The results of the learning process is the output of this phase, which is stored the result in a lookup table.

Algorithm 2: Learning phase for MBAM

Input: training patterns p with code c.
Output: lookup table for all n corresponding stored patterns.
Step1: Repeat steps 1.1 and 1.2 to the end of training pattern p with code c:
Step 1.1: Divide the training pattern p to n vectors v with length two.
Step 1.2: For each vector v, repeat steps 1.2.1, 1.2.2 and 1.2.3:
Step 1.2.1: Assign the weight for each n vectors v, weights matrix svw as follows:

$$svw_i = v_i * c$$

Where: c is code
Step 1.2.2: Assign the stored vector's weight svw as follow:

$$svw = f(Dcode(v)) \begin{cases} 0 & \{meansw0 \\ 1 & \{meansw1 \\ 2 & \{meansw2 \\ 3 & \{meansw3 \end{cases}$$

Where: Decode is a function to convert the binary number to decimal number.
Step 1.2.3: Save svw for this vector in the lookup table.
Step 2: End.

Figure 2: The Algorithm of the learning phase.

3.2 Convergence Phase [2]

The output of this phase is dependent on the learning phase. Figure 3 and Figure 4 shows MBAM Convergence phase (code to pattern and pattern to code).

3.2.1 Convergence code Phase

Input: n of unknown patterns p.
Output: Convergence code c.
Step 1: Repeat steps 1.1 and 1.2 until the unknown pattern p is ended:
Step 1.1: Divide the unknown pattern p to n vectors v with length two.
Step 1.2: Sum up the energy function for all n vectors v in the unknown pattern each with its corresponding vector in the stored patterns:

$$ep = -0.5 \sum_{i=1}^{n} v_i * svw_i * y_i$$

Where y_i is :

$$y_i = v_i * svw_i$$

Step 2: Determine the stored code number $minc$ with the minimum energy function to converge the unknown pattern towards it:

$$minc = \min(ep)$$

Where the min function is to determine the minimum energy function in ep array.
Step 3: End.

Figure 3: Convergence code Algorithm

4.2.2 Convergence pattern phase

Input: n of unknown codes c.
Output: Convergence pattern CP.

Step 1: Repeat steps 1.1 until the lookup table is ended:
Step 1.1: Find energy function ep:

$$ep = -0.5 * \sum x_i . c$$

Where x_i :

$$x_i = y_i * svw_i$$

Where y_i :

$$y_i = c * svw_i$$

Where c: is unknown code.
svw: is matrix weights stored in lookup table.

Step 2: Determine the stored pattern number $minp$ with the minimum energy function to converge the unknown code towards it:

$$minp = \min(ep)$$

Where the min function is to determine the minimum energy function in ep array.
Step 3: Build the final converge pattern cp:

$$cp = svw_{minp} * c$$

Step 4: End.

Figure 4: Convergence pattern Algorithm

IV. 4. PROPOSED METHOD USING MODIFY BIDIRECTIONAL ASSOCIATIVE MEMORY

The general flowchart of password authentication using MBAM as shown in Figure 5. This method can use either graphical or textual password as input.

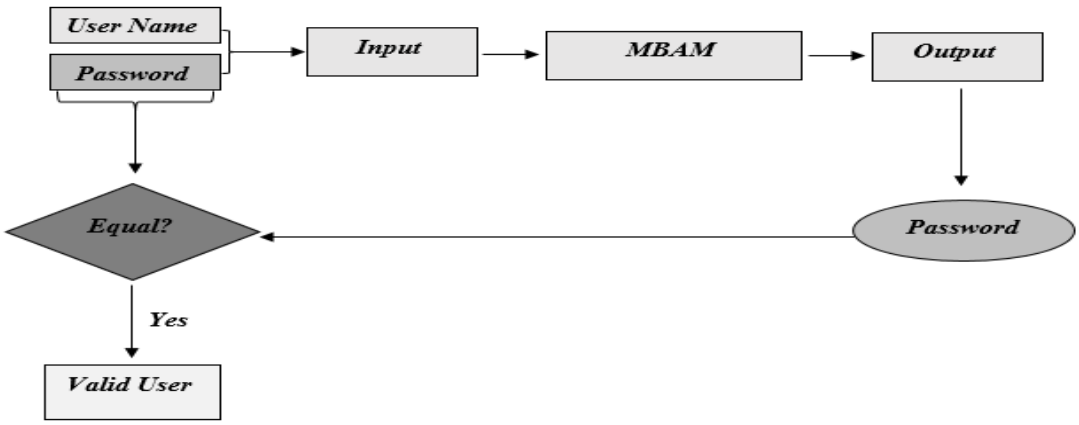

Figure 5: Password Authentication using MBAM.

The method for textual and graphical password is converts the username and password to the binary values with bipolar representation and uses these values as training samples, which can be performed by the following steps as shown in Figure 6.

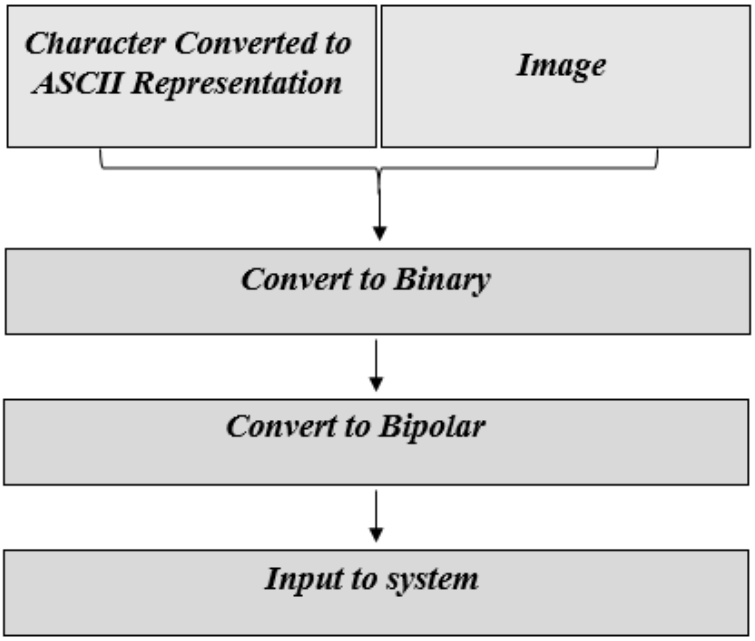

Figure 6: steps Authentication Process.

Once the training has been completed very soon the network will be stored in each server. When the user wants to use an application from a server, the user connects to the server and inserts username and password in that application, then server loads the MBAM and generates output by giving username as input. If the output matches with the password submitted by the user then server allows working with that application.

V. RESULT

The accuracy result for 100 user is 100% for textual password to authenticate a user and for graphical password the accuracy result for 100 user is 100% if the image without noise. But if the image have some noise (rate of noise less than 15%, the noise come from different format or through transformation), in this case the server will send message to email to authenticate the user. The process time to authenticate each user is 2.3 second for textual password and for graphical password is 15 second with image size 32*32.

Additional, it is useful to compare with other work because has a similar target with the proposed method. This comparison focused on compare with the training time and capacity of the neural network is measured in terms of number of stored patterns, the same number of training set was used in this comparison,

Figure 7 shows training time for different networks (see Appendix A). Figure 8 shows percentage number of pattern stored by different training sets. This capacity is different from number of patterns used for training. In many situations neural networks cannot remember (store) all the patterns which are used in training (see Appendix B).

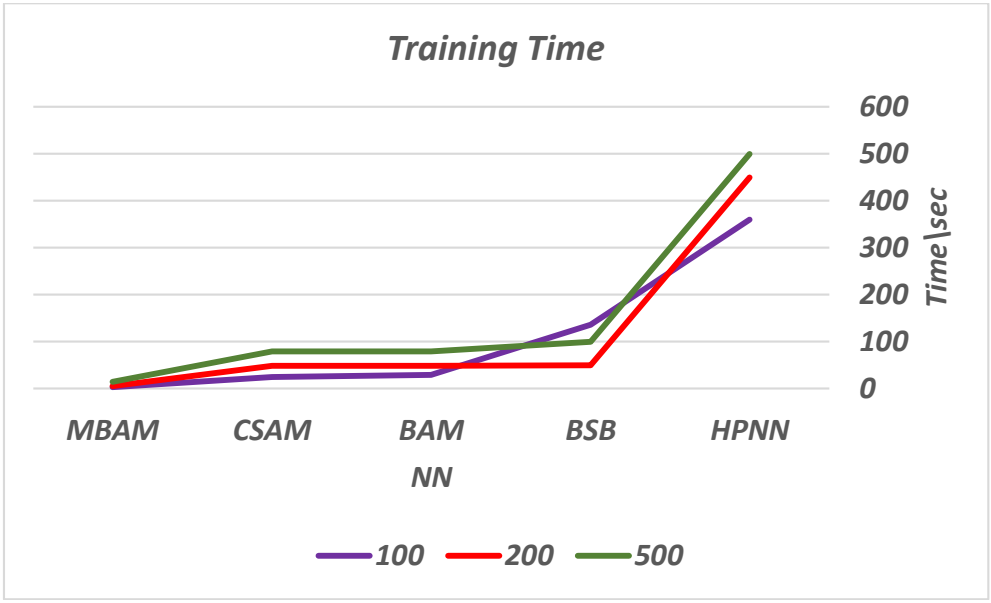

Figure 7: Training time.

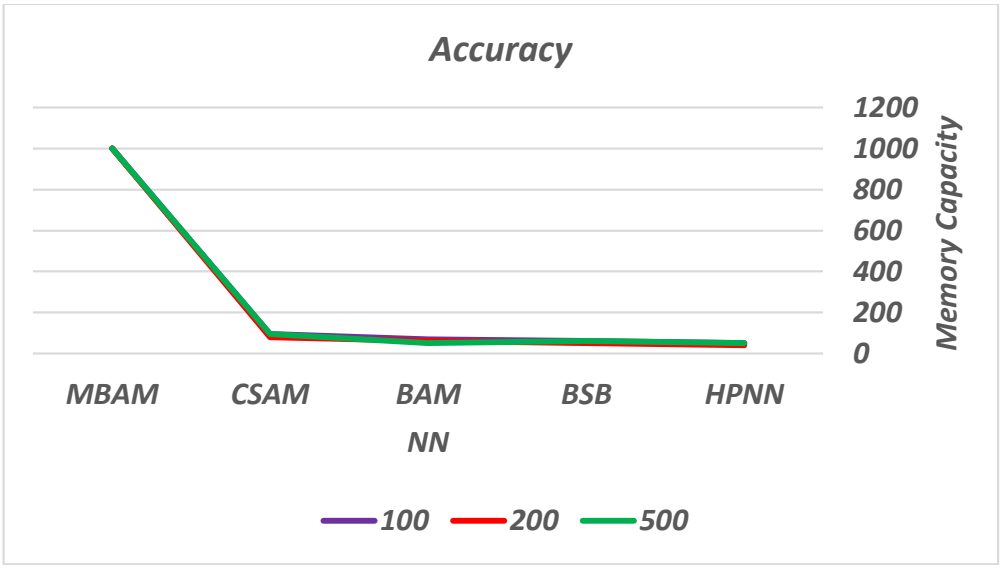

Figure 8: Accuracy result.

Figure 7 show the training time and the MBAM spends less amount of time compare with all other networks. And the Figure 8 shows that MBAM is more accuracy compare with other work, it will return all stored pattern.

VI. CONCLUSION

Results analysis and discussion and show that the proposed password authentication by using MBAM the average accuracy was 100% for graphical and textual password. This work focused on the development of password authentication via using MBAM, which is develop more efficient password authentication in speed and accuracy. But this approach may have some limitations that various usernames may have the same password. In order to solve this problem can take password plus unique key for identifying the username.

REFERENCES

i. ASN Chakravarthy, 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.

ii. Nisreen Abd Alhadi Jabrand Emad I Abdul Kareem (2015), ***"Modify Bidirectional Associative Memory (MBAM)***", International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 02, Issue 08, ISSN (Online):2349–9745; ISSN (Print):2393-8161.

iii. 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.

iv. ASN Chakravarthy, P S Avadhani***," A Novel Approach for Pass Word Authentication Using Bidirectional Associative Memory"***, Advanced Computing: An International Journal (ACIJ), Vol.2, No.6, November 2011.

v. ASN Chakravarthy, P S Avadhani, ***"A novel approach for Pass Word Authentication using Brain -State - In -a Box (BSB) Model"***, International Journal of Computer Science and Information Technologies (IJCSIT), Volume 2 Issue 5 September-October 2011.

vi. Khalil Shihab,***" A Back propagation Neural Network for Computer Network Security"***, Journal of Computer Science 2 (9): 710-715, 2006.

vii. Li-Hua Li, Iuon-Chang Lin, and Min-Shiang Hwang,***" A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks"***, IEEE Transactions On Neural Networks, VOL. 12, NO. 6, November 2001.

viii. G. Horng, ***"Password authentication without using password table"*** Inform. Processing Lett. vol. 55, pp. 247–250, 1995.

ix. M. Udi, ***"A simple scheme to make passwords based on one-way function much harder to crack"*** Computer Security, vol. 15, no. 2, pp. 171–176, 1996.

x. P.E.S.N. Krishna Prasasd and et al, ***"Performance Evaluation of Password Authentication using Associative Neural Memory Models"***, International Journal of Advanced Information Technology (IJAIT) Vol. 2, No.1, February 2012.

APPENDIXES

Appendix A

Training Time

Training Time			
Training set	100	200	500
HPNN	360	450	500
BSB	136	50	100
BAM	30	49	80
CSAM	25	49	80
MBAM	3	6	15

Appendix B

Accuracy

Accuracy			
Memory Capacity in term (No. of pattern)			
	100	200	500
HPNN	50	40	50
BSB	60	50	60
BAM	70	60	50
CSAM	95	80	95
MBAM	Return all stored pattern		

