Performance Evaluation of Password Authentication using Associative Neural Memory Models

P.E.S.N. Krishna Prasasd[1], A.S.N. Chakravarthy[2], B. D. C. N. Prasad[3]

[1]Dept. of Computer Applications, P V P Siddhartha Institute of Technology, India.

surya125@gmail.com

[2]Department of Electronics & Computer Eng., K.L.University, India.

asnchakravarthy@yahoo.com

[3]Dept. of Computer Applications, P V P Siddhartha Institute of Technology, India.

bdcnprasad@gmail.com

Abstract

They are many ways of providing security to user resources. Password authentication is a very important system security procedure to secure user resources. In order to solve the problems with traditional password authentication several methods have been introduced to provide password authentication using Associative Memories like Back Propagation Neural Network (BPNN),Hopfield Neural Network(HPNN),Bidirectional Associative Memories(BAM),Brain-State-in-a Box(BSB). Later Password authentication has been provided using Context-Sensitive Associative Memory Method (CSAM). Here in this paper we proposed performance analysis of password authentication schemes using Associative memories and CSAM using graphical Images. We observe that in comparison to existing layered and associative neural network techniques for graphical images as password, the CSAM method provides better accuracy and quicker response time to registration and password changes.

Keywords –

Authentication; Cryptography; Password;

1. 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. Authentication is the act of confirming the truth of an attribute of a datum or entity. Password authentication is a common approach to the system security and it is also a very important procedure to gain access to user resources. In the conventional password authentication methods a server has to authenticate the legitimate user [1].

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, we proposed authentication methods that use pictures as passwords.

Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood [1]. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption . Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text- based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

2. RELATED WORK

To overcome the disadvantages of traditional password authentication schemes, a novel technique for password authentication was introduced using BPNN [1]. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption [1].Before giving the image as password the image should be converted in to its RGB values and these values will be normalized using our normalization function. We can't give image directly as input to the neural network. So here we converted image into matrix (or text). In back propagation method we will calculate error at the output layer and it will be propagated to the previous hidden layers and then to the input layer. Basing on the error at all the layers weights will be adjusted to get the correct output or to decrease the error rate. Dictionary attacks are infeasible, partly because of the large password space, but mainly because there are no pre-existing searchable dictionaries for graphical information. It is also difficult to devise automated attacks. Whereas we can recognize a person's face in less than a second, computers spend a considerable amount of time processing millions of bytes of information regardless of whether the image is a face, a landscape, or a meaningless shape.

3. COMPARITIVE STUDY

Since the output of this BPNN [2] method is in the form of probabilistic values, the system can introduces noise, due which we may not do the efficient authentication. Training time for BPNN is extremely large. Easy to remember passwords are vulnerable to password guessing attacks. The system users can freely choose their password and the server is required to retain only the pair user ID and password. Server only stores the weights of the network [1]. When all the networks are given with same training set, each one spends different amount of times to adjust their weight values.

This password authentication using graphical images is introduced using other associative memories like Hopfield Networks Bidirectional memories, Brain in state Box.

The password authentication using Hopfield method may use any one of the Textual or Graphical password as password and can train network so that it can authenticate users [3]. This scheme reads colour of each pixel of the selected image and converts the colour into red, green and blue (RGB) parts as any colour can be produced using these three primary colours as
Shown

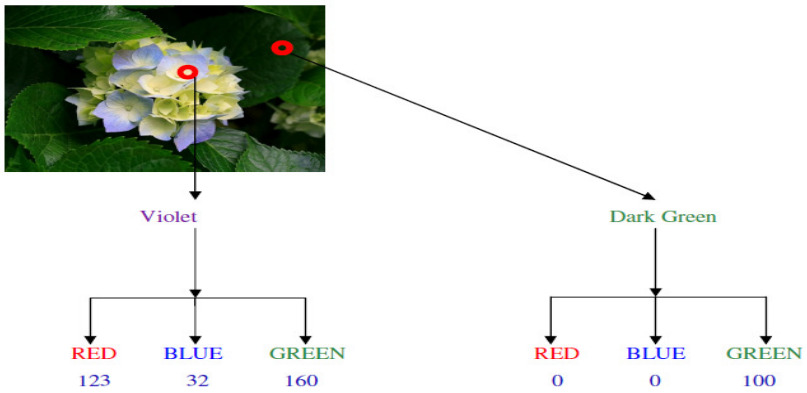


Fig. 1 Converting Image in to Binary Values

By practicing the above custom we can convert any image into a matrix enduring of set of numbers representing all the pixels of the image.

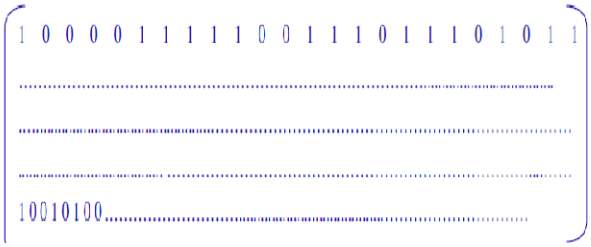
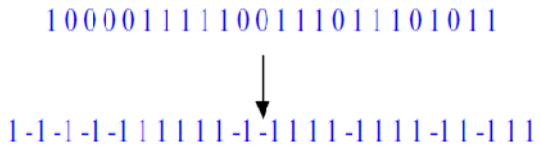


Fig. 2 Converting Binary Values to Matrix Representation

3. 1CONVERTING IMAGE TO BIPOLAR VALUES

In all the cases bidirectional associative memory spends less amount of time comparing with all other networks and feed forward network spends huge amount of time as it uses back propagation. The above procedure first converts the image into a matrix representing binary values and then converts the binary values into bipolar values by replacing 0 with -1 and represent in the form of a matrix.



HPNN-based authentication scheme can effectively be used for access authentication in the open computing environment. An HPNN, with large capacity, can store authentication information using marginal training time. The authentication scheme incorporating the use of HNN can

recall information for a legal user's ID and password instantly and accurately. Our experiments have demonstrated the usefulness and robustness of the authentication scheme using HPNN.

Recognizing the Pattern uisng HPNN:

The pattern which we want to use for testing the network will be endowed as input to the application and then application stores the pattern in the corresponding variable.

This is implemented as follows

```
private void toolStripButton4_Click(object sender, EventArgs e)
{
   try
   {
      int[,] pattern = CreateMatrix(tableLayoutPanel2);
      int[,] result = MatrixMath.Multiply(Weight, pattern);
      result = MatrixMath.GetBipolar(result);
      MessageBox.Show(MatrixMath.GetString(result));
   }
   catch (Exception ee) { MessageBox.Show(ee.Message); }
}
```

3.2 PASSWORD AUTHENTICATION USING BIDIRECTIONAL ASSOCIATIVE MEMORY

The password authentication using HPNN takes the input and the output pattern together to the network. There is a chance of wrong user validation. In order to eliminate the limitations in Password Authentication Scheme (PAS) using HPNN new technique for password authentication using bidirectional associative memory has been introduced [4]. In this approach of password authentication using BAM we need not give input and output together to train the network. Since BAM is bidirectional in nature we can further improve this method for an application which can give username if the password is given. But this method may have some limitations that different usernames may have the same password. In order to solve this we can take password plus any unique image as input for identifying the username, if the same

Combination was given as input while training network.

Recognizing the Pattern using BAM:

The pattern which we want to use for testing the network will be supplied as input to the application and then application stores the pattern in the corresponding variable.

The Methods and the Equations for Retrieve are:

Start with an initial condition which can be any given pattern pair (α , β).Determine a finite sequence of pattern pairs

(α^1 , β^1), $(\alpha^{11} , \beta^{11})$, until an equilibrium point (α_f , β_f) is reached, where

$$B = \phi (A M) \quad \text{and} \quad A^1 = \phi (B^1 M^T)$$

$$B^{11} = \phi (A^1 M) \text{ and } A^{11} = \phi (B^{11} M^T)$$

$$\emptyset (F) = G = g_1,g_2,\ldots,g_r$$

$$F = (f_1,f_2,\ldots\ldots,f_r)$$

M is correlation matrix

$$g_i = \begin{cases} 1 & \text{if } f_i > 0 \\ \begin{cases} 0 \text{ (binary)} \\ -1 \text{ (bipolar)} \end{cases} & , \quad f_i < 0 \\ \text{Prevous } g_i & , \quad f_i = 0 \end{cases}$$

Pattern Recognization Implementation using BAM:

```
private int[,] Recognize()
{
                    // pa -->  Previous alpha
  int[,] a =null, pb = null, b = null ;
  a = test;
  do{
     pb = Phi(MatrixMul(a, Weight));
     a = Phi(MatrixMul(pb, Transpose(Weight)));
     b = Phi(MatrixMul(a, Weight));
  }while(!areEqual(pb,b));
  ShowMatrix(pb);
  return pb;
}
```

3.3 PASSWORD AUTHENTICATION USING BRAIN-STATE-IN-A-BOX (BSB)

The "Brain-State-In-A-Box" [5](BSB) model is one of the earliest Dynamic Associative Memories (DAM) models. It is a discrete-time continuous-state parallel updated DAM. The BSB model extends the Linear Associator model and is similar to the Hopfield Model in that it is an Auto-associative model with its connection matrix computed using outer products in the usual way. The operation of both models is also very similar, with differences arising primarily in the way activations are computed in each iteration, and in the signal function used. The BSB model stands apart from other models in its use of the linear threshold signal function.

In this chapter an algorithm for constructing the interconnection matrix W and vector b is proposed and implemented. This chapter also provides a heuristic explanation for yielding an interconnection matrix with desired properties. The desired properties include the asymmetry of W. The algorithm ensures that the negatives of the desired patterns are not automatically stored as asymptotically stable equilibrium points of the network, and it has provisions to minimize the number of spurious states. Digital computer simulations verified that our design algorithm yielded a network which stored all of the desired patterns as asymptotically stable equilibrium points with very few spurious states. The network has one main shortcoming: the network is not guaranteed to be globally stable.

Recognizing the Pattern using BSB

Here the pattern which is used for testing the network will be supplied as input to the application and then application stores the pattern in the corresponding variable. The equation 6.3 is used to calculate the output of the network.

$$X_{[n+1]} = f(\gamma X_n + \eta W X_{[n]} + \delta X)$$

Wher f(x) is defined as follows.

$$f(x) = \begin{cases} -1, & for \quad x < -1 \\ x, & for \quad -1 \leq x \leq 1 \\ +1, & for \quad x > +1 \end{cases}$$

This is implemented as follows

```
private void Recognize()
{
   try
   {
      int[,] pattern = CreateMatrix(tableLayoutPanel2);
      int[,] temp1 = MatrixMath.ScalarMultiply(gama,pattern);
                  int[,] temp2 = MatrixMath.ScalarMultiply(lr,Weight);
      int[,] temp3 = MatrixMath.ScalarMultiply(delta,pattern);
      result = MatrixMath.Add(temp1+temp2+temp3);
                  result = f(result);
      MessageBox.Show(MatrixMath.GetString(result));
   }
   catch (Exception ee) { MessageBox.Show(ee.Message);
   }
}
```

3.4 CONTEXT-SENSITIVE ASSOCIATIVE MEMORY MODEL (CSAM)

Context-sensitive associative memories are models that allow the retrieval of different vectorial responses given a same vectorial stimulus, depending on the context presented to the memory [6]. The contextualization is obtained by doing the Kronecker product between two vectorial entries to the associative memory: the key stimulus and the context. These memories are able to display a wide variety of behaviors that range from all the basic operations of the logical calculus (including fuzzy logics) to the selective extraction of features from complex vectorial patterns. In the present contribution, we show that a context-dependent memory matrix stores a large amount of possible virtual associative memories that awaken in the presence of a context. A system of networks consisting of first net which constructs the Kronecker product between two vectors and then sends it to a second net that sustains a correlation memory, defines a context-dependent associative memory.

Simple Associative memories are static and very low memory so that they cannot be applied in the applications where high memory is required. A simple model describing context-dependent associative memories generates a good vectorial representation of basic logical calculus. One of the powers of this vectorial representation is the very natural way in which binary matrix operators are capable to compute ambiguous situations. This fact presents a biological interest because of the very natural way in which the human mind is able to take decisions in the presence of uncertainties. Also these memories could be used to develop expert agents to the recent problem domain

4.RESULT ANALYSIS

Training Time:

When all methods are given with same training set, each one spends different amount of times to adjust their weight values. In all the cases bidirectional associative memory spends less amount of

time comparing with all other networks and feed forward network spends huge amount of time as it uses back propagation for learning. Compared to the associative memories CSAMM takes less time to authenticate a user.

Table 1 Training Times

Training Time			
HPNN	360	450	500
BSB	136	50	100
BAM	30	49	80
CSAM	25	49	70

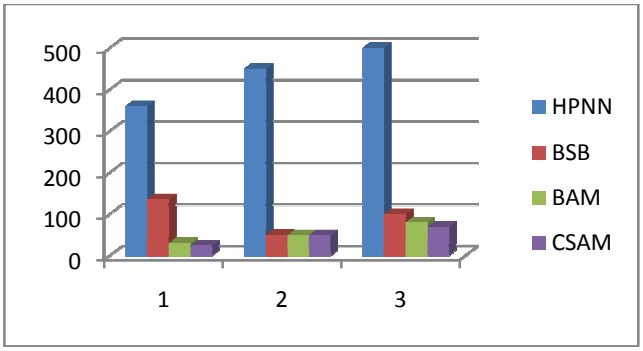


Fig. 3 Bar Chart Showing Training Time

X – Axis → *Different training sets*
Y – Axis → *Time taken for training*

In general capacity of the neural network is measured in terms of number of patterns stored. 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. Table 2 shows percentage of number of patterns stored by different networks when they are trained with same training sets. Following figure shows these issues more clearly that CSAMM is having more accuracy compared to associative memories.

Table 2 Accuracy

Accuracy			
	Memory Capacity(In terms of no of Patterns)		
	100	200	500
HPNN	50	40	50
BSB	60	50	50
BAM	70	60	50
CSAM	95	80	95

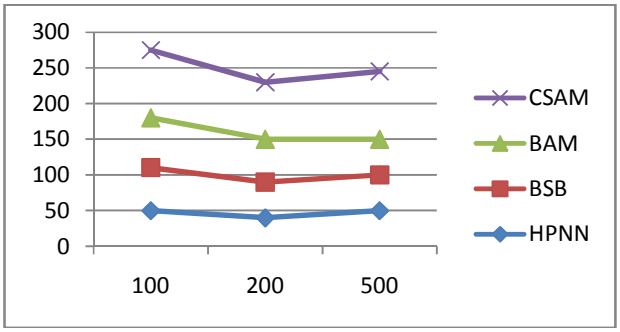


Fig. 4 Line Graph Showing Accuracy

False Positive Rate (FPR):

- False positive(FP): Authorized people incorrectly identified as Un authorized
- True negative(TN): Authorized people correctly identified as Authorized

False positive rate (α) = FP / (FP + TN)

Table 3 False Positive Rate

False Positive Rate			
	Memory Capacity(In terms of no of Patterns)		
	100	200	500
HPNN	30	30	50
BSB	20	25	45
BAM	15	15	30
CSAM	1	5	10

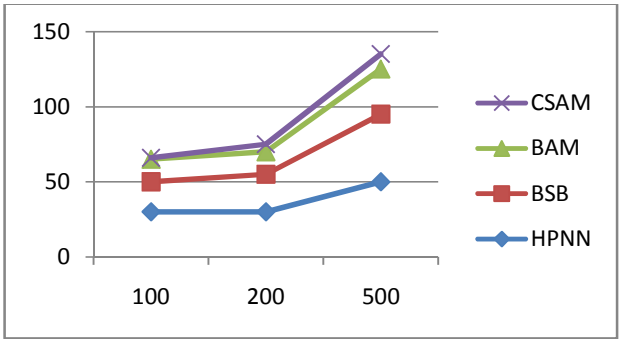


Fig.5 Line Graph Showing False Positive Rate

False Negative Rate (FNR):

- False negative (FN): Unauthorized people incorrectly identified as Authorized.
- True positive(TP) : Unauthorized people correctly identified as Unauthorized

False negative rate (β) = FN / (TP + FN)

Table 3 False negative Rate

False Negative Rate			
	Memory Capacity(In terms of no of Patterns)		
	100	200	500
HPNN	10	30	50
BSB	8	25	45
BAM	7	15	30
CSAM	1	5	10

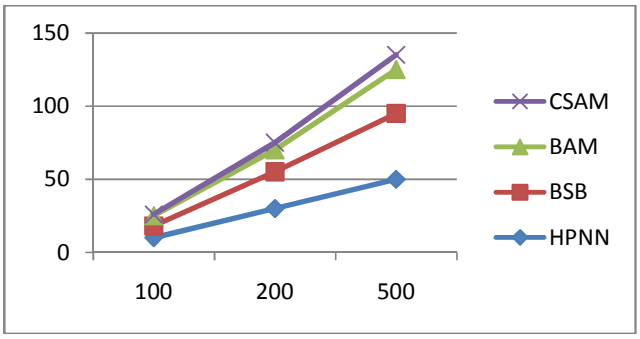


Fig.5 Line Graph Showing False Negative Rate

5.CONCLUSIONS

The PAS using CSAMM is having more PPR and FNR. Memory is not just a passive store for holding ideas without changing them; it may transform those ideas when they are being retrieved. There are many examples showing that what is retrieved is different from what was initially stored. A simple model describing context-dependent associative memories generates a good vectorial representation of basic logical calculus. One of the powers of this vectorial representation is the very natural way in which binary matrix operators are capable to compute ambiguous situations. This fact presents a biological interest because of the very natural way in which the human mind is able to take decisions in the presence of uncertainties. Also these memories could be used to develop expert agents to the recent problem domain. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this scheme, the server does not store or maintain password or verification table. The server only stores the weights of the classification network. Also we want to enhance the BPNN method for hand written Graphical passwords and hand written signatures. For graphical passwords we can draw images or symbols on the virtual screen and can use those images as passwords.

Enhancement can be provided for the authentication by using alternate active functions like Hyperbolic Tangent, Linear, SoftMax, Tangential, Sin Wave, Bipolar and Gaussian etc. For graphical passwords we can draw images or symbols on the virtual screen and can use those images as passwords. We want to enhance the method for other Intrusion detection using associative memories like bidirectional memories, Hopfield Networks and brain in state Box. The same Probabilistic approach can be applied for authentication Schemes which may use

Boltzmann machines, Godelization Theorem, Pell's Equation, Helbert Matrix, Key Stroke frequencies, Sound as Password. Neural Network approach can be used for SPAM mails, designing S-box concept and replacing SHA-1 and RSA algorithms in cryptography.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation.

References

1. 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.
2. B.D.C.N.Prasad, P E S N Krishna Prasad, ASN Chakravarthy, "A Study on Back Propagation Models through Hidden Units" ,Advances in Computational Sciences and Technology, ISSN 0973-6107 Volume 4 Number 2 (2011) pp. 213-227.
3. 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
4. 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.
5. 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.
6. B.D.C.N.Prasad, P E S N Krishna Prasad,ASN Chakravarthy," Password Authentication using Context-Sensitive Associative Memory Neural Networks: A Novel Approach", Proceedings of Springer Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST) Series, at the CCSIT 2012 in Bangalore, India .
7. ASN Chakravarthy, P S Avadhani ,"Handwritten Text Image Authentication Using Back Propagation.", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
8. Shouhong Wang and Hai Wang," Password Authentication Using Hopfield Neural Networks", IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 38, No. 2, March 2008.
9. T. Schmidt, H. Rahnama, A. Sadeghian, "A Review Of Applications Of Artificial Neural Networks In Cryptosystems", Seventh International Symposium on Neural Networks, June 6-9, 2010 Shanghai, China.
10. Yash Pal Singh, V.S.Yadav, Amit Gupta, Abhilash Khare," Bi Directional Associative Memory Neural Network Method in the Character Recognition", Journal of Theoretical and Applied Information Technology,2009.
11. B.D.C.N.Prasad, P E S N Krishna Prasad, Sagar Yeruva,"A Study on Associative Neural Memories", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 6, December 2010.

AUTHORS PROFILE

P. E. S. N. Krishna Prasad, currently a Researcher in the area of Machine Intelligence and Neural Networks. He is working as Associate Professor in the Department of Computer Applications at Prasad V. Potluri Siddhartha Institute of Science and Technology, Vijayawada, Andhra Pradesh, India..He is a member of ACM, ISTE. He has presented and published papers in several International Conferences and Journals. His areas of interest are Artificial Intelligence, Neural Networks and Machine Intelligence, Information security Applications.

Dr. A. S .N. Chakravarthy, Currently is working as Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He received Ph.D. in Computer Science & Engineering from Acharya Nagarjuna University, Guntur, India in 2011. He has 13 papers published in various National / International journals and conferences. He is a Life member of CSI, ISCA and reviewer for various International Journals. His research areas include Security & Cryptography, , Biometrics, and Digital Forensics and Cyber Security, Neural networks.

Dr. B D C N Prasad, currently is a Professor & Head of Department of Computer Applications at Prasad V. Potluri Siddhartha Institute of Science and Technology, Vijayawada, Andhra Pradesh, India. He received Ph.D. in Applied Mathematics from Andhra University, Visakhapatnam, India in 1984. His research interests include Machine Intelligence, Data Mining, Rough Sets and Information Security in Computer Science and Boundary value problems and Fluid Dynamics in Mathematics. He has several publications in mathematics and computer science in reputed national and international journals. He is a member of ACM, ISTAM, ISTE and also he is Technical Committee member on Soft Computing in IEEE SMCS and National Executive member of Indian Society for Rough Sets.