Graphical Password by Image Segmentation

A Balamurali, M V R Harsha,V Sai Hitesh, A Sai Chaitanya

Abstract—In our paper we proposed a new method of a password by DES Algorithm, to arrange a picture in the desired manner. This is based on a technique in which coordinates of the segmented image allows the image to be fragmented and store it in different parts.The fragments of the image are converted into a grid and stores each part accordingly in order. The idea of the paper is to give access only if the image is arranged correctly.

Keywords— Graphical password, Image Segmentation

I. INTRODUCTION

A common method of user authentication is through the key which is set by the user in their username and password.This procedure is most commonly used in many authentication methods. This approach may have many cons; such as passwords canbe easily identified and can be remembered. Moreover, the users choose the most certainpassword in other way, passwords that can be easy to memorize and use the most common password.

Graphical password is an alternative solution to text-based. This paper highlights theimages rather than alphabets and numerical. The main advantage is that users are better atmemorizing pictures. Besides this, it is very difficult for hackers to steal pictures.If the sample size of the images are large it provides enhanced security.Image Segmentation is done based on the coordinates. The coordinates of the segmented image allow the system to fragment the image and store it in different partsand jumbled every time.

In our proposed system, graphical image plays a key role in authentication. In this approach, we store an image break it into fragments in grids of the desired size and if the user is successful in arranging the fragments of the image the application can be accessed and if not access is denied.

II. RELATED WORK

The different types of passwords used nowadays are recognition-based and recall based are some of the examples. In recall based,a person is required to regenerate the password, he stored atthe time of registration process. The disadvantage in this process is that it depends on recall of password and if the user does a mistake the authentication is denied.

In the recall based process, there is a chance of someone replicating the same password.Jeermyn,et al. proposed "Draw a Secret " in which users are asked to draw a text or shape on a grid.

On the other side, the recognition based technique, a set of images which consists of a set of pass images is given to the user and they are asked to recognize and identify their pass image was chosen at the time of registration.

The other method of user access is the user must select an imagewith low resolution of the image which was preserved earlier.This was proposed by Hayashi, et al. The oil painting filter is used to decrease the quality of the image of the original image which was selected by the user during the initial registration phase. This process is most useful in the device with a good color display.

'Deja vu' is another method of visualization technique which was proposed by Dhamaija and Perrig. In this method, user is given some random computer generated images and the user has to select the pass image. During the authentication, the user has to select the same pre-registered image to prove his identity.

In general, pictures of nature and animals are memorized easier than computer graphic images. Mostly the memory of nature requires more storage. However, Secure and usable graphical password is desired.

III. PROPOSED SYSTEM

We can use this proposed system for web-based services andapplication in ourmobiles. User want to use the application he/she starts login procedure at their desk his/her co-worker or friend may notice the password when they pass by them. This process tries to minimize such observer's knowing the image. User registers the image in the initial stages of the registration. Then the image is stored and divided into several fragments. When the user wants to use web-based service or application then the stored image fragments are jumbled and then the user has to arrange in proper order so that it forms an image which is same as a registered image then the user will be successfully authenticated. The advantage of this method is only registered user knows the correct position of the objects in the image.

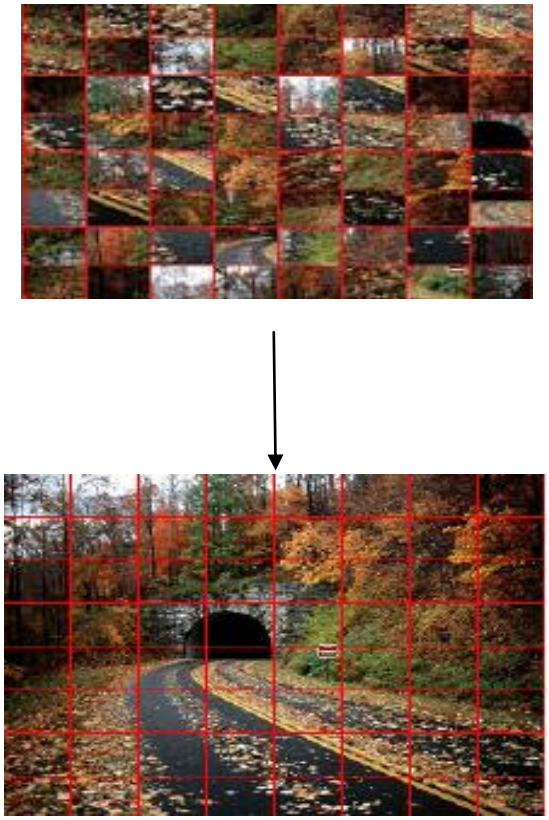
Revised Manuscript Received on April 12, 2019.

A Balamurali, Assistant Proffesor, Department of Cse, Srmist, Chennai., t.n, India.

M V R Harsha, Student, Department of Cse, Srmist, Chennai.T.N, India.

V Sai Hitesh, Student, Department of Cse, Srmist, Chennai.T.N, India.

A Sai Chaitanya, Student, Department of Cse,Srmist, Chennai.T.N, India.



REARRANGED IMAGE

Fig 1: graphical password by segmentation

IV. IV.MODULE DESCRIPTION

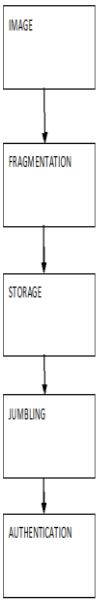


Fig 2: Proposed system

a.IMAGE

The image is to be given as an input for the conversion of the image into the fragment. The input image should be in the form of JPEG, PNG format as its required condition.

b.FRAGMENTATION

The image is now divided into fragments by the system into a grid.

c.STORAGE

The parts of the image are separated and stored.

d.JUMBLING

The image stored is nowprovided to the user in a jumbled order.

e.AUTHENTICATION

If the parts of the image are arrangedin original order then authentication is done or else not.

V. DES ALGORITHM& RESULTS

Data Encryption Standard (DES) is a symmetric-key block cipher uses 16 round Feistel structure. The block size is 64-bit. Though the key length is 64-bit, DES has an effective key length of 56 bits.

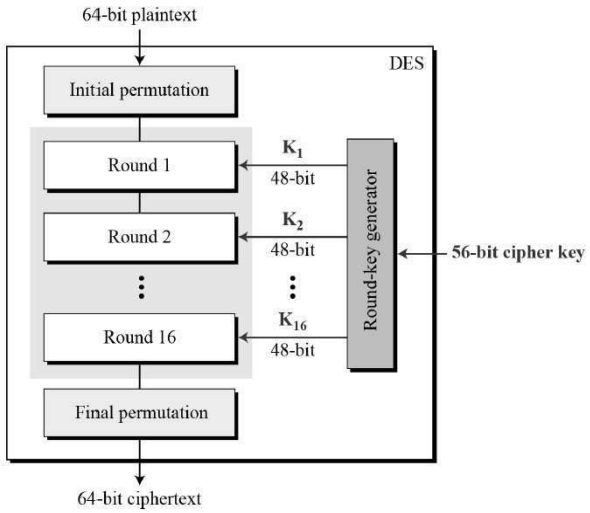


Fig 3: Structure of DES

There are 16 identical stages of processing also known as rounds.The initial and final permutations takeplace which inverses each other.The 64 bit block is divided equally 32 bit on both sides and are processes alternatively.The key role of blocks is to perform encryption and decryption.The encryption siteuses the cipher and the decryption site uses reverse cipher.The input is permutated according to a predefined rules.These keyless permutations and straight permutations that are the inverse ofeach other.

The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.This algorithm is used since it provides large number of keys for permutation.

Security of DES:-

The security of des can be affected by following techniques

1.Brute force attack:-

DES consists of weak short cipher key, it is known that des consists of 2^55 encryptions. The most used keys in des are 3DES with two types of keys or 3DES withthree types of keys, these keys provide strong protection from brute forces.

2.CryptanalysisDifference:-

DES can be broken by using technique of differential cryptanalysis if it consists of 24/7 of chosen plaintexts or 255 of known plaintexts. Though thislooks efficient than compared to brute-force attack, tracing of 247 chosen plaintexts or 255 know plaintexts is one of the toughest task. Hence we can conclude that DES is resistant tothedifferential cryptanalysis. Increasing the number of plaintexts is not allowed in more than 264 is not allowed in DES.

VI. RESULT

In this process we have overcome many disadvantages of present day security issues and there is a sample in the figure 1 how the arrangement is done and if arrangement is successful as shown in the example we can access the application. Now a dayspassword has become common for any application this may lead to new revolution. This also helpful in banks like to open bank lockers.

VII. CONCLUSION

In our project,we have developeda graphical passwordmethod using DES algorithm.Thismethodgives enhanced security to application.Further testing can be done to improve the access time.General traditional attack methods such as bruteforce search and spyware find difficult to break this method. In this process we need notremember the password just we need to rearrange properly to authenticate the application.

REFERENCES

1. HousamKhalifaBashier, Lau Siong Hoe , Pang Ying Han,"Graphical Password: Pass-Images Edge Detection"2013 IEEE 9th International Colloquium on Signal Processing and its Applications
2. Madoka Hasegawa, Yuichi Tanaka and Shigeo Kato,"A Study on an Image Synthesis Methodfor Graphical Passwords"2009 International Symposium on Intelligent Signal Processing and Communication Systems
3. Kar-Ann Toh, Quoc-Long Tran, and DiptiSrinivasan,"Benchmarking a Reduced MultivariatePolynomial patter classifier"IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 26, NO. 6,
4. Yang Hao ,Li Changshun ,Pei Lei,"An improved method of image edge detection based on wavelet transform",2011 IEEEInternational Conference on 10-12 June 2011
5. R. Dhamija and A. Perrig, "Déjà vu: A user study, usingimages for authentication," *Proc. 9th* USENIX SecuritySymposium, August 2000.
6. Duan Qing, Li Feng-xiang, Tian Zhao-lei, " An Improved Method for Wavelet Thresholding Signal Denoising,''ComputerSimulation,vol.26,no.4,pp.348-351,2009.
7. W. Campbell, K. Torkkola, and S. Balakrishnan, "DimensionReduction Techniques for Training Polynomial Networks," Proc.Int'l Conf. Machine Learning, June 2000.
8. SubhradeepBiswas, SudipaBiswas,"Password Security system with 2-way authentication",ThirdInternational Conference Research in Computational Intelligence& Communication Network(ICRCICN).