Graphical Password Authentication Using Neural Style Transfer

Burre Chandu (411613)
Kaza Phani Rohitha (411634)
Umesh Yadav (411675)

18 November 2019

1. Introduction

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). Neural Style Transfer refers to a class of software algorithms that manipulate digital images, or videos, to adopt the appearance or visual style of another image. NST algorithms are characterized by their use of deep neural networks in order to perform the image transformation.

2. Approach To solve Problem

Neural Style Transfer is applied to user images and those images are displayed to user in two steps for authentication.The motivation to apply style is drawn from idea of blurring images for preventing hidden camera attacks.

Initially we have created a webpage which have following :
- User Registration
- User Login

2.1. User Registration

1. During sign up user has to enter the username and upload the images of his choice limited upto three.

2. The user is also asked to select the style image in the next step.

3. After selecting the style the user is redirected to check how the images appear after applying the selected style so that user can remember them for future login.

4. The username of the user and the three pictures and style image, selected by user is stored in the database.

5. Username is the unique key to identify user and no two users can have same username.

2.2. User Login

1.The user in the first step is displayed 3x3 grid of random images.

2.The images are in such a way that random style (same for all images) among available styles in the database is applied to them.

3.The user has to select the correct image among those 9 images

4.In second step user is given with 4x4 image grid with random styles applied to random images and images may repeat with different styles.

5.The user has to select the remaining (one image already selected in step 1) two correct styled images from them.

6.The style acts as a key here as user only knows what the style image is.

2.3. Verification Procedure

If the user clicks on correct image in step1 the database is looked up if selected image exist in one of three images selected by user then the user is verified and the user is redirected to second step.

In second step the database is looked for remaining two images and also the style image if the images are correct the login is successful.

If the user clicks on the wrong image the whole login process should be repeated and there is only single attempt.The user is redirected to the initial login/signup page if the user clicks on wrong image.

3. Merits

It prevents following attacks:

1.Hidden Camera Attack

2.Phishing Attack

3.Shoulder Surfing Attack

4. Drawbacks

1. API calls take some time to load the images.
2. Options for style to be given such that no conflict occurs

5. Conclusion

The blurred approach for graphical password authentication is extended to use style transfer so that style acts as a key and many combinations are possible to attack the password. The images in step 1 and step 2 are not same every time user log in they change randomly for every login and usage of styling concept makes the system more efficient.