International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Login Functionality using Image Pixels Authentication

Mr. Santosh R. Salunkhe[1], Mr. Kishor N. Shedge[2], Mr. Kishor N. Shedge[2] and Mr. Devidas S. Thosar [2]

[1]Department of Computer Engineering Chincholi, Nashik
[2]Department of Computer Engineering, SVIT, Chincholi, Nashik

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

In this century almost of more than 30 to 40 percent India's overall population have owned a smartphone, tablets, laptops, PC's to using multipurpose. They are accessing internet, browsing social medias for entertainment, personal data and electronic communications. All these devices they can access or handle anywhere any places. Now a days CCTV cameras are installed at cafes, parks, shops and offices as well where peoples are using their devices without thinking or taking any kind of security and start to accessed all personal information and data. That time may be they also processed financial transactions or used saved bank details. This all are happened under CCTV surveillance where are easily captured all the information. Mainly, the lock and login details of all the devices like pattern lock in smartphones, simple passwords, complex passwords are easily recorded in CCTV video footage. And that video footage or video film is too sufficient for any hacker to hack any devices and misuse of information. In this paper, we demonstrate a concept which is useful to reduces this kind of risk and prior to the unlike attacks. We are design a login functionality using image processing techniques with optical pixel of random images where images are changing every time while doing login process or accessing their devices. In this functionality, user have to select or click on those areas of image which was selected at the time of signup process. Images could be changing randomly and never repeated within 10 times login process. So, this is very secure and unbreakable login method also attractive or different login process which is never implemented till and very useful to protecting sensitive information.

Keywords: *Video footage, image processing, Optical Pixel authentication.*

Introduction

Peoples are access their mobiles, TABs and laptops anywhere like coffee shops, mall, railway station, banks and those areas which are already in CCTV circumstance. They are totally aware about this environment where their devices easily access and recorded in video footage. that time login information and other personal information recorded. For any hacker this kind of information is enough to hack their devices and miss use it easily without any extra efforts by using CCTV video footage. The purpose of this paper is to avoid this kind of unlike attacks. Here we are giving a login functionality with using image pixels and there are set of images we are used for login process. This process is based on optical image processing techniques. Where system read the image pixels' location and stored into the database. While user access their devices that time all that pixels location should be identify and match. So there will be no chance to hack the devices and personal information's.

Literature Survey

We analyse in our survey, all mobile, laptop and TAB companies are using basic level of authentications to access device. Where they are providing only Login user id and password in laptops. Same in mobile and tabs given a pattern lock, complex password, bio-matrix etc. but users are widely used a pattern lock or complex password methodology to access their devices. Very rear peoples used bio-matrix functionality. The pattern lock and complex password will be easily track or capture into the CCTV cameras or hacker can be easily record it in their high resolutions mobile without knowing that persons. And once password captured then easy to hack their devices with referring recorded video footage and film. So hacker easily access their device and get the all personal information or financial details misuse it. But the all peoples and users are totally aware from this kind of attack.

Proposed Methodology

Before going to proposed system, to check the flexibility of changing current login functionality of all the personal devices which are already used by users. And image processing algorithm where the images pixels are easily read and able to store into the database with its location wise. So whenever user will try to login by using this images the validation work properly and all pixels should be read properly.

A. Architecture

An image consists of a rectangular region of image pixels. Any changes in image in an efficient manner, need convenient access of any pixel anywhere within the particular region or outside the region. In some cases there are image sequence and we required access to any pixels from any regions of any image from the sequence of images. However, there are number of image formats like .jpeg, .jpg, .tiff, .png, .gif, etc. that all are makes it difficult to access pixels from the images on demand. Within these formats we find differences in:

- colorspace (e.g YUV, Lab, sRGB, linear GRAY, CMYK, linear RGB, etc.)
- bit depth (.e.g 1, 4, 8, 12, 16, etc.)
- storage format (e.g. unsigned, signed, float, double, etc.)
- compression (e.g. uncompressed, RLE, Zip, BZip, etc.)
- orientation (i.e. top-to-bottom, right-to-left, etc.),
- layout (.e.g. raw, interspersed with opcodes, etc.)

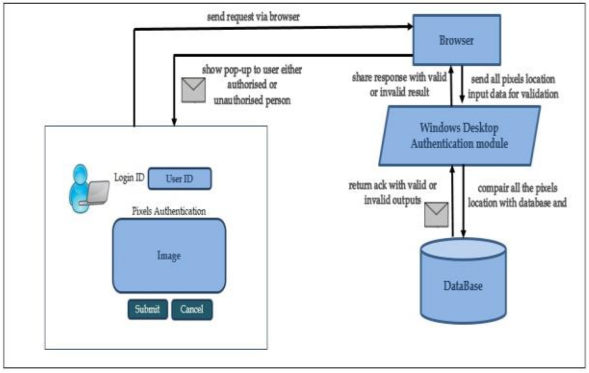

send request via browser
Browser
show pop-up to user either authorised or unauthorised person
share response with valid or invalid result
send all pixels location input data for validation
Windows Desktop Authentication module
Login ID
User ID
Pixels Authentication
Image
Submit
Cancel
return ack with valid or invalid outputs
compair all the pixels location with database and
DataBase

Figure 1. Login functionality architecture

In addition, some image pixels have required attenuation, some formats permit more than one frame, and some formats contain vector graphics that must converted from vector to pixels.

B. Algorithms-

In the implementation of an image processing algorithm required we get or set methodology:

Step1: One pixel a time (e.g. pixel at location 10,3)
Step2: A single scanline (e.g. all pixels from row 4)
Step3: A few scanlines at once (e.g. pixel rows 4-7)
Step4: A single column or columns of pixels (e.g. all pixels from column 11)
Step5: An arbitrary region of pixels from the image (e.g. pixels defined at 10,7 to 10,19)
Step6: A pixel in random order (e.g. pixel at 14,15 and 640,480)
Step7: Pixels from two different images
Step8: Pixels outside the boundaries of the image (e.g. pixel at -1,-3)
Step9: A pixel component that is unsigned (65311) or in a floating-point representation (e.g. 0.17836)
Step10: A high-dynamic range pixel that can include negative values (e.g. -0.00716) as well as values that exceed the quantum depth (e.g. 65931) Step11:
One or more pixels simultaneously in different threads of execution
Step12: All the pixels in memory to take advantage of speed-ups offered by executing in concert across heterogeneous platforms consisting of CPUs, GPUs, and other processors
Step13: Traits associated with each channel to specify whether the pixel channel is copied, updated, or blended
Step14: Masks that define which pixels are eligible to be
Updated
Step15: Extra channels that benefits the user but Otherwise remain untouched by image Processing algorithms

Given the varied image formats and image processing requirements, we implemented the pixel cache to provide convenient sequential or parallel access to any pixel on demand anywhere inside the image region like authentic pixels and any image from in a sequence. In pixel cache permits access to pixels outside of the boundaries which are defined by the images i.e. virtual pixels.

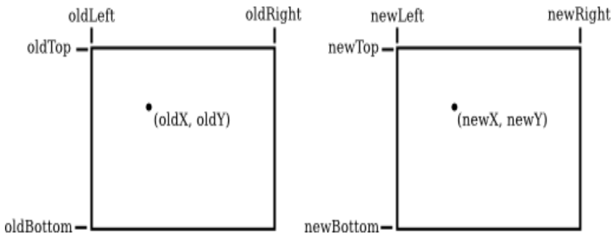
To allow programmers to specify the co-ordinates of pixels in system that they would like to use, it would be good to have a subroutine such as **setCoordinateSystem(left,right,bottom,top)**

C. Function to read pixels -

```
var getImagePixels = function(img){

var canvas = document.createElement('canvas'), ctx =
canvas.getContext('2d'); canvas.width = img.width;
canvas.height = img.height; ctx.drawImage(img, 0, 0);
var imgData = ctx.getImageData(0, 0, img.width,
img.height).data; var nImgData = []; var offWidth =
img.width * 4; var dataRow = (nImgData[0] = new
Uint8Array(offWidth));

for (var x = 0, i = 0; x++ < img.height;)

{
  nImgData[x] = new Uint8Array(offWidth);

    for (var arrI = 0, len = i + offWidth; i < len; i += 4,
arrI += 4)
{ nImgData[x][arrI] = imgData[i];
nImgData[x][arrI + 1] = imgData[i + 1];
nImgData[x][arrI + 2] = imgData[i + 2];
nImgData[x][arrI + 3] = imgData[i + 3];
     }
  }

  return nImgData;
};
```

Mathematical Modules

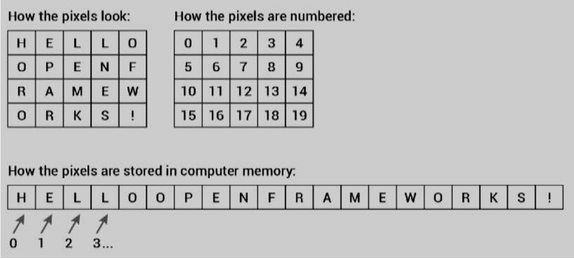
The graphical system would be responsible for automatically transforming the co-ordinates from the specified co-ordinates system into pixel co-ordinates. Subroutine might not available, so it is useful to see how the transformation is done by hand. Let's consider the general case. Given co-ordinates for a point in one coordinate system, we want to find the co-ordinates for the same point in a second co-ordinate system. (Remember that a co-ordinate system is just a way of assigning numbers to points. It's the points that are real!) Suppose horizontal and vertical limits are oldLeft, oldRight, oldTop, and oldBottom for the first coordinate system, and are newLeft, newRight, newTop, and newBottom for the second. Suppose points has co-ordinates (oldX, oldY) in the first co-ordinate system. Need to find the co-ordinates (newX,newY) of the point in the second coordinate system.



Formulas for newX and newY are then given by,

$newX = newLeft + ((oldX - oldLeft) / (oldRight - oldLeft)) * (newRight - newLeft))$ $newY = newTop + ((oldY - oldTop) / (oldBottom - oldTop)) * (newBotom - newTop)$

Each pixel is sample of original image and more pixels samples provide more accurate representations of the original. Intensity of each pixel is variable or dynamic. In color image systems, a color is typically represent by 3 or 4 components intensity such as red, green, and blue, or cyan, magenta, yellow, and black.



How the pixels look:

H	E	L	L	O
O	P	E	N	F
R	A	M	E	W
O	R	K	S	!

How the pixels are numbered:

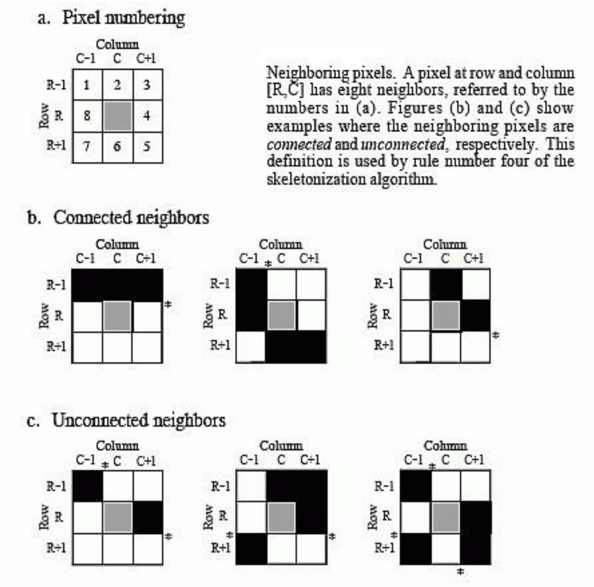
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19

How the pixels are stored in computer memory:

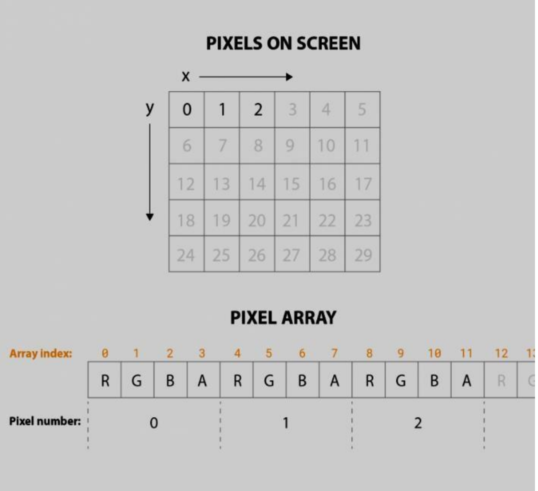
H	E	L	L	O	O	P	E	N	F	R	A	M	E	W	O	R	K	S	!
0	1	2	3...																

Figure 2. Pixels stored into device memory

Digital images is made up of rows and columns of pixels with unique value. Pixel in an image can specified or declared by saying which column and row contains it with which co-ordinate location. In terms of coordinates, pixel can identified by a pair or combination of integers give by the column numbers and the row numbers. For example, pixel with coordinates (8,10) would lie in column number 8 and row number 10. Conventionally, columns are numbered from left to right, starting with zero. Most graphics systems, including the ones we will study in this chapter, number rows from top to bottom, starting from zero. Including OpenGL command, number of the rows from bottom(down) to top(up) instead.



Neighboring pixels. A pixel at row and column [R,C] has eight neighbors, referred to by the numbers in (a). Figures (b) and (c) show examples where the neighboring pixels are *connected* and *unconnected*, respectively. This definition is used by rule number four of the skeletonization algorithm.



PIXELS ON SCREEN

0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	26	27	28	29

PIXEL ARRAY

Array index:	0	1	2	3	4	5	6	7	8	9	10	11	12	1
	R	G	B	A	R	G	B	A	R	G	B	A	R	G
Pixel number:	0				1				2					

Figure 3. Array representation of Pixels

System Description

This is a new concept to secure unlike attacks and avoid the misuse of personal information. In this system we are given a signup functionality to user with login id and password which will be 10 images. User will be select a 5 pixels from all the images as a password. And at the time of login user should be select correct pixels location as he selected at the time of signup process for that particular image. And this images will be change every time whenever user will be login. Hence there is number of combinations of password, so no chance to hack personal devices and misuse of the data. If user unable to login and want to reset the password then he will get the OTP on his register mobile number. If OTP matched the user can change the pixels of images or set new image with new pixels location.

Result and Discussions

Unknown person or hacker theft your personal devices and doing attacked based on CCTV camera or video filmed which will taken from 2 meters away from target device using mobile camera. If user lock their device by using pattern lock then hacker will only follow the finger movements to crack the password. This system will helpful to avoid the unlike attacks on personal devices. Also helpful in the personal data leakage and misuse of it. This functionality will be used in all the devices where login functionality and device access process has follow like mobile, tab, laptops, personal computers etc. If login functionality is unbreakable then your whole system and device will be secure and be a rest assured about any kind of unknown attacks.

References

[1]. Refer “Graphical User Authentication(GUA) : Graphical Password Algorithms and Analysis” , Arash Habibi Lakshkari Ngu Nguyen,Stephan Sigg Aalto University,"Personalized Image-based User Authentication using Wearable

[2]. Camera",arXiv:1612.06209v2 [cs.CR] 29 Mar 2017

[3]. Guixin, Ye, University of Bath, UK. IEEE paper, title is “Cracking Android Pattern Lock in Five Attempts”

[4]. Introduction to Computer Graphics. Section 2.1, Pixels, Coordinates, and Colors. Author: David J. Eck (eck@hws.edu).

[5]. Graphical Passwords Fabian Monrose and Michael K. Reiter A graphical password is a secret that a human user inputs to a computer published paper in IJIES

[6]. Refer Wazir Zada Khan1, Mohammed Y Aalsalem2 and Yang Xiang3 ,A Graphical Password Based System for Small Mobile Devices" IJCSI

[7]. International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011 ISSN (Online): 1694-0814

[8]. Refer Dr. Nagabhushana Department of Computer Science & Engineering, S.J.M.I.T Chitradurga,

[9]. Karnataka-577501” User Authentication Using Image Processing Techniques”, Int. J. Advanced Networking and Applications Volume: 10 Issue: 02 Pages: 3770-3775 (2018) ISSN: 0975-0290

[10]. Refer Muhammad Ahsan1, Yugang Li2,"Graphical Password Authentication using Images Sequence", International Research Journal of Engineering and Technology (IRJET),Volume: 04 Issue: 11 | Nov - 2017