INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume2, Issue6)
Available online at www.ijarnd.com

One Time Password Generation from Retinal Images

Devendra Kumar
M. Tech Student
Kanpur Institute of Technology, Kanpur, India
devendrakumarnri@gmail.com

ABSTRACT

Authentication is processed in which right user will be given access to the resource. Authentication protects resource to access from the unauthorised user. There various traditional techniques are available for authentication. But these techniques have disadvantages. To overcome this disadvantages multi-factor authentication is used for authentication. In multi-factor authentication, more than one authentication method is combined to perform authentication. One form of authentication that is mostly used with other forms of authentication for multifactor authentication is a one-time password (OTP). One time password is valid for one login session. In this paper, we conduct a survey of existing one-time password generation methods.

Keywords: Authentication, One-time password (OTP), Security, Multi-factor authentication, RGB, Sobel, Dendrogram, Retinal image.

1 INTRODUCTION

Security is a major concern in the web application. Nowadays Attacker uses various type of attacks to break the password of a system. Some well-known attacks are eavesdropping, phishing attack, spoofing, and man in the middle attack, Denial-of-service attack and virus attacks. The security problem is increasing day by day. Several techniques are implemented in the past to secure a system. The password is an important factor while authenticating a user legal or illegal. The static password is used in the past to enter into a system. But they could be broken. One-time password generation technique (OTP) is very helpful to secure a system.

OTP is valid only for a single session. The password is changed every time a user wants to log in the system. Sometimes simple mathematical methods are used to generate the password. So, randomicity of the password is broken at some stage. Randomness of the OTP is the main factor

In this work, random numbers are generated from extracted retinal features. Retinal image feature is a strong biometric factor. Variable length password is created for the security purpose.

1.1Problem Statement

An efficient one-time password (OTP) generation technique from features of the retinal image.

1.2Objective

In this research work, retinal image features are used to generate the OTP. Retinal image features are strong authentication factor. The main objective of this work is to generate a random number (one-time password) of variable length for the higher security of a system.

1.3Application

The proposed technique can be used in a various application where higher security is needed. It is used to authenticate a user whether the user is valid or not. It can be applied to highly secure network like:

1. Online money transaction
2. Accessing of confidential information and data

1.4 Challenges

The main challenge of one-time password generation technique is to generate a random number. The whole security system is dependent upon the randomness of the password.

2 LITERATURE SURVEY

Security problems are major issues in the web application. Nowadays Attacker uses various type of attacks to break the password of a system. Several techniques are used in the past to secure a system. Traditional ID/Password are used in the past to authenticate a user. These passwords are static in nature. So, they could be broken easily. One-time password generation technique (OTP) is very helpful to secure a system. OTP is valid only for a single session. The password is changed every time a user wants to log in the system. The randomness of the password is the important factor in OTP generation technique.

Biometrics factors and tokens are described by the authors in the paper. Biometric features are unique in nature. Therefore, the biometric features are very useful at the time of authentication and identification. Some common biometric factors described by the authors are:

- Palm scan
- Hand geometry
- Iris scan
- Retinal pattern
- Fingerprint
- Voice verification
- Facial recognition
- Signature dynamics
- Keystroke dynamics

Tokens are used to generate a static and dynamic password. Authors described the token devices as four types. They are:

- Static tokens
- Synchronous dynamic password tokens
- Asynchronous dynamic password tokens
- Challenge response tokens

3 BACKGROUND CONCEPTS

3.1 One Time Password

One time password is valid only for a single session. Every time a user wants to enter the system, a new OTP is generated. OTP is basically a random number. Traditional static passwords are vulnerable to replay attacks. OTP is used to remove the shortcomings of static passwords. Some methods are used to generate the OTP. They are:

- Time synchronized method
- Mathematical algorithms

3.2 Security Attacks

Security is a major concern in the web application. Nowadays attacker uses various techniques to break the password of a system. Some well-known attacks are:

- Eavesdropping
- Phishing attack
- Spoofing
- Man in the middle attack
- Denial of service attack
- Virus attacks

3.3 Digital Image

The mathematical representation of an image is called digital image. The digital image is shown in a matrix format. Information present in row and column (x,y) of the matrix represents a point in the image. The value stored in the matrix describes the brightness of an image corresponds to the point (x,y). This point is known as a pixel.

3.4 Color Image

Color information of each and every pixel of the image is contained by a color image. There are three types of color model i.e RGB, HSV, and CMYK. RGB is the most popular color model. Three bands are present in an RGB image. Each band contained a different color. The colors are Red, green and blue. 24-bit data (each color has 8-bit data) is present in an RGB image.

3.5 Binary Image

The binary image is a digital image representing the data 0 and 1. Black and white images are known as a binary image. 0 refers to black and 1 refers to white.

3.6 Gray Scale Image

Grayscale images have 8-bit data. Each pixel has only the intensity information. Grayscale images are made of gray shades. Black refers to the minimum intensity and white refers to the maximum intensity.

3.7 Dendrogram

A dendrogram is a hierarchical binary cluster tree. The function H = dendrogram (Z) is used to create the cluster tree of the matrix Z. Z is an (m-1) by 3 matrices. Linkage function is used to generate the matrix Z. _m‘is the number of objects in the original data set. Each object is connected with another object by the U-shaped lines in a dendrogram. These U-shaped lines show the distance between two connected objects.

3.8 Edge Extraction with Sobel Method

Various edge detection method is used in the image feature extraction process. Sobel operator is one of the popular edge detection methods in image processing. Sobel approximation to the derivative is used to select the edges from an image. Edges are selected if the gradient of I(input image) is maximum.

The simple Sobel method:

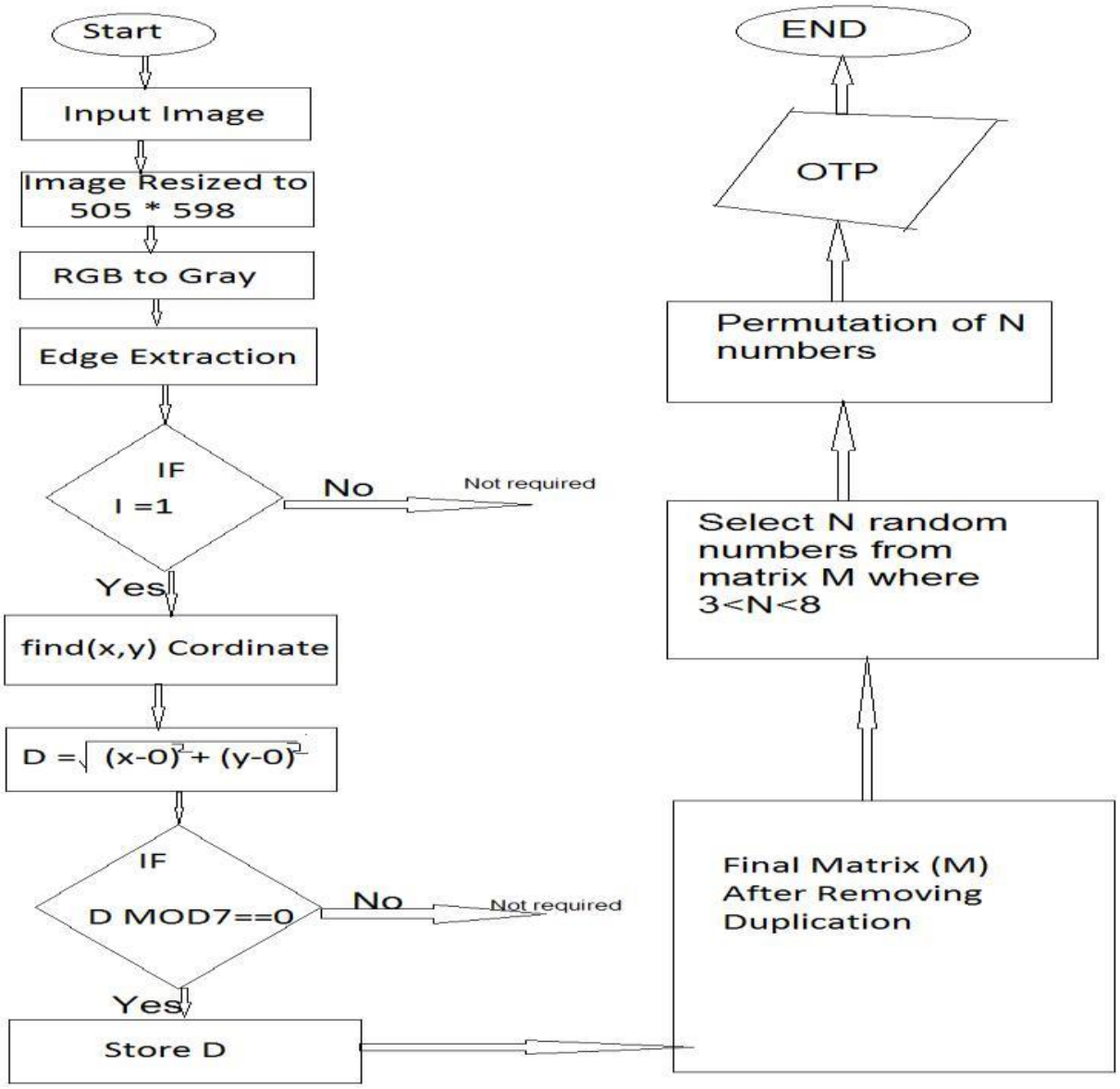
BW = edge (I,'sobel')

Sobel method with threshold value:

BW = edge(I,'sobel',thresh)

The edges which are stronger than thresh value is selected by this method. If the thresh value is null then the value is automatically chosen by the edges.

FLOW CHART



4 THE PROPOSED ALGORITHM

Step i. Read the input image (RGB) file.
Step ii. Resized the image to 505×598.
Step iii. Convert RGB image to grayscale.
Step iv. Edge extraction using ‗sobel' method.
Step v. Find the (x,y)coordinates where intensity(I)=1.
Step vi. Measure distance (D) from (0,0) to each coordinate.
Step vii. Select D if (D MOD 7 == 0)
Step viii. Remove duplicate number to get final matrix (M).
Step ix. Select a random number (N) where 3<N<8.
Step x. N numbers are selected randomly from the final matrix (M).
Step xi. Permutation of N numbers to get the one-time password (OTP).

5 EXPERIMENTATIONS AND RESULTS

5.1 Dataset STARE dataset is used as a source file of retinal images. STARE dataset contained 20 images of the retina. Retinal images file format is changed to BMP format for use. Retinal images are resized to 505×598. OTP generation system is implemented in MATLAB platform.

5.2 Source images

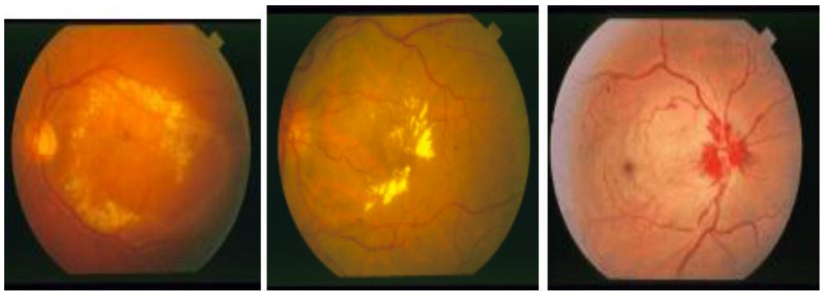


Image 1 Image 2 Image 3

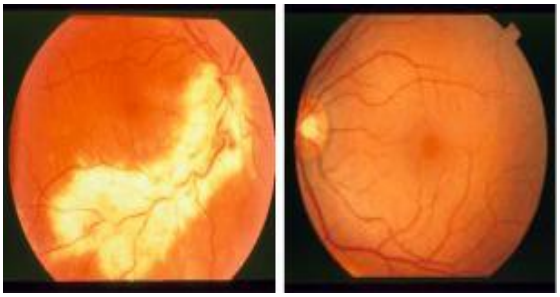


Image 4 Image 5

Fig. 5.1: Retinal Image

5.3 Execution of algorithm

Step i. Read the input image (RGB) file.

Image 3 is used as the input image.

Step ii. Resized the image to 505×598.
The image is resized into (505×598).

Fig. 5.3: Image 3 with dimension (505×598).

Step iii. Convert RGB image to gray scale.
The RGB image is converted to gray scale image.

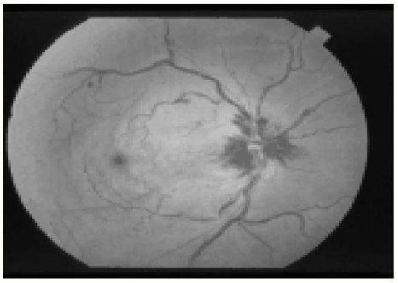


Fig. 5.4: Gray scale image of image 3.

Step IV. Edge extraction using 'sobel' method.
Only the edges are present after the sobel method

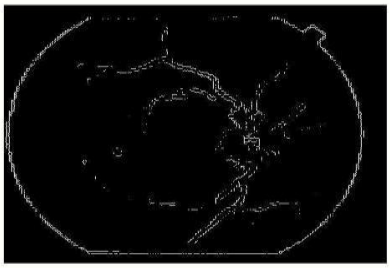


Fig. 5.5: Edges of image 3.

Step v. Find the (x,y)coordinates where intensity(I)=1.
5071 coordinates(x,y) are selected and stored in coords (5071×2) matrix.
Step VI. Measure distance (D) from (0,0) to each coordinate.
5071 distance values stored in dist(5071×1) matrix.
Step vii. Select D if (D MOD 7 == 0)
1033 distance values stored in D (1033×1) matrix.
Step viii. Remove duplicate number to get final matrix (M).
Matrix M (1×80) contained 80 numbers.
Columns 1 through 9
364 140 147 154 161 168 175 182 189
Columns 10 through 18
196 203 210 217 224 231 238 245 252
Columns 19 through 27
259 266 273 280 287 294 301 308 315
Columns 28 through 36
322 329 336 343 350 357 371 378 385
Columns 37 through 45
392 399 406 413 420 427 133 434 126
Columns 46 through 54
441 455 483 119 490 476 112 462 497
Columns 55 through 63

469 504 105 511 518 525 532 539 546
Columns 64 through 72
553 448 560 567 574 581 588 595 602
Columns 73 through 80
609 616 623 630 637 644 651 658

Step ix. Select a random number (N) where 3<N<8.

7
7 is selected randomly.

Step x. N numbers are selected randomly from the final matrix (M).

259 119 406 602 532 392 140
7 numbers are selected randomly from the final matrix (M).

Step xi. Permutation of N numbers to get One-time password (OTP).

119 140 406 532 259 602 392
This is the final OTP.

RESULTS

5 Retinal images are used in the testing phase. 30 passwords (OTP) are generated from each image. The dendrogram is drawn to show the randomness of the password. A different password is generated every time of execution of the algorithm for a single image.

REFERENCE

[1] James Michael Stewart, Ed Tittle, and Mike Chapple, ―CISSP: Certified Information Systems Security Professional Study guide‖, 3rd Edition, SYBEX Inc, 2005, pp. 16-20.
[2] Young Sil Lee, HyoTaek Lirn and Hoon Jae Lee, ―A Study on Efficient OTP Generation using Stream Cipher with Random Digit‖, vol 2**,** The 12th International Conference on Advanced Communication Technology, ICACT, Feb 2010, pp. 1670 – 1675.
[3] Yu tao, Fan and Gui ping, Su, ―Design of Two-Way One-Time-Password Authentication Scheme Based On True Random Numbers‖**,** vol. 1, Second International Workshop on Computer Science and Engineering, IEEE, Oct 2009, pp. 11-14.
[4] Mohammad Saleh Miri and Ali Mahloojifar, ―A Comparison Study to Evaluate Retinal Image Enhancement Techniques‖, International Conference on Signal and Image Processing Applications, IEEE, Nov 2009, pp. 90-94.
[5] Paras Babu Tiwari and Shashidhar Ram Joshi, ―Single Sign-on with One Time Password‖, First Asian Himalayas International Conference on Internet 2009, IEEE, Nov 2009, pp. 1-4.
[6] Foon Chi Francis Chui, Raymond Williams, Ivan Bindoff and Byeong Ho Kang, ―Feature Extraction for Classification from Images: A Look at the Retina‖, International Symposium on Ubiquitous Multimedia Computing, IEEE, Oct 2008, pp. 93-98.
[7] Feng-ying Cui, Li-jun Zou and Bei Song, ―Edge Feature Extraction Based on Digital Image Processing Techniques‖, Proceedings of the IEEE International Conference on Automation and Logistics Qingdao, China, September 2008, pp. 2320 – 2324.
[8] ByungRae Cha and Chul Won Kim, ―Password Generation of OTP System using Fingerprint Features‖, International Conference on Information Security and Assurance, IEEE, April 2008, pp. 243

