IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 41-44
www.iosrjournals.org

Graphical Color Code Password and Facial Recognition Using Net Banking System

[1]Mr.Kawade Kiran, [2]Miss.Mahajan Hemlata, [3]Miss.Mandge Yogita,
[4]Miss.Waykar Varsha, [5]Prof.Kandalkar S.A.
(Department Of Computer Engineering/ SVCET,Rajuri)

Abstract: *Now days success of online banking, there remains a reluctance to use it primarily because of uncertainty and security concerns. This study evaluates the potential of biometric authentication for online banking (banking) as a way of improving adoption auto base sms gateway and Graphical Color Base Password use of online banking. The biometric is the study of physical or behavioral characteristics of human being used for the identification of a person. These physical characteristics of a person include the features like fingerprints, face, hand geometry, voice, and iris biometric features. These biometrics features can be used to make computer systems more secure for authentication purpose in computer based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The biometric identification overcomes all the above. Additional security barriers can be provided using those characteristic of a person which are unique in nature. The biometric systems offer several advantages over traditional authentication systems.*

Keywords: *Face Recognition,RGB Color Code, OTP, Color OTP, SMS Gateway,Security, Access controls,SRS*

I. Introduction

Now a-days with the network world, the way for crime is become easier than before. Because of this reason, network security has become one of the biggest concerns facing today's IT departments. We heard a lot about hackers and crackers ways to steal any password or pin code, crimes of ID cards or credit cards fraud or security breaches in any important building and then reach any information or important data from any organization or company. These problems allow us to know the need of strong technology to secure our important data and credentials. This technology is based on a technique called “biometrics". Biometric is a form of bioinformatics that uses biological properties to identify people. Since bio-metric systems identify a person by biological characteristics, they are difficult to fake. Examples of biometrics are iris scanning, signature authentication, voice recognition and hand geometry.

In this system, the color code technique is used. Here, when user’s login takes place successfully he/she is directed to Color Code authentication page. Where the user enters his/her favorite 3 colors in the form of color code generated by system to authenticate whether user is valid or not. If valid then user is redirected to Transaction page where user can carry out his/her own ATM transactions else he/she is directed to login page. In this way by applying the technique of Color Code we are enhancing the security of login for ATM Transactions, as the attacker don’t know the users favorite colors and even if he/she (attacker) does know those colors, it is not possible to unveil the color code combination which is generated dynamically in our system for carrying out final Authentication process as that color code is encrypted and then sent to user’s personal contact number.

II. Indentations and EQUATIONS

- COLOR CODED ENCRYPTION:

converted in ASCII value ASCII is the abbreviation of American standard code for information interchange it typically based on English, the character are converted into ASCII value

- GROUPING THE ASCII VALUE:

The converted ASCII values are grouped in four digits, if the character is sort of four digits zeros are added to the last part

- ASSIGNING THE COLOR CODE

The each grouped part contains four digit numbers these numbers represent the html color codes, the each part is assigned respective color codes.

- CONVERTED INTO BINARY VALUES

After assigning the color codes the each color code is converted into binary values.

- COMPRASSION OF DATA

The converted binary values are too large for transmitting or storing to reduce the size we use XOR to reduce the size of the data

Methodology/ Planning of work:

Let S = { I, O, F, Success, Failure}
Where,
I : Set of inputs,
O : Set of outputs,
F : Set of functions,
Success :
Failure :
I ={ I1, I2, I3 },
O = { O1, O2, O3 },
F = { F1, F2, F3, F4, F5 }
Where,
For I –
I1 : Registration form,
I2 : Login form,
I3 : Face Recognisation
I4 : Color code form

For O –
O1 : Registration message (Success or Failure),
O2 : Login message (Success or Failure),
O3 : Face Compare (Success or Failure),
O4 : Color code received (via SMS),
O5 : Color code verified message (Success or Failure).

For F-
F1 : Store information given from registration form in DB.
F2 : Check that valid username and password is entered in login page and display message.
F3 : Face Recognise (if success).
F4 : Generate Color-Code and encrypt it (if success).
F5 : Send Color-code to user through SMS (if success).
F6 : Authenticate Color-Code entered by user and thendisplay message.
Success : Login successful
Failure : Login failed

III. Figures and Tables

There are plenty of usage scenarios involved which given as follows:

- User login
- Image capture and tracking
- Color code Verification
- Matching
- Authentication
- Validation
- Database storage
- Logout

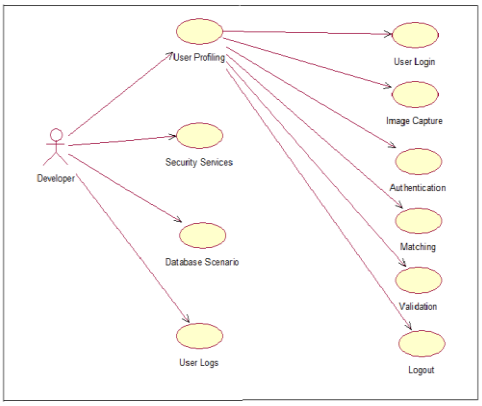


Fig 1 Use case Diagram

IV. System Snaps

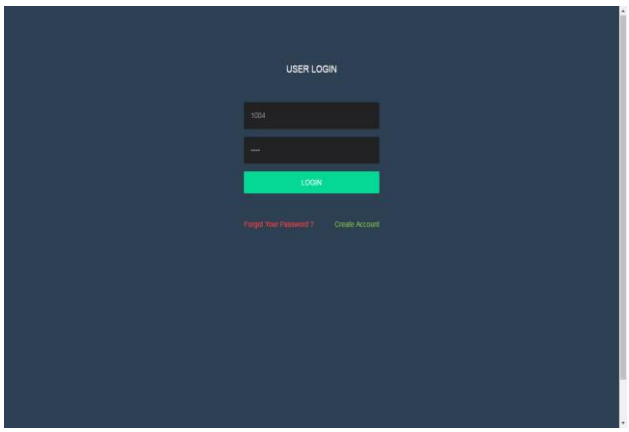


Fig. 2 User Login

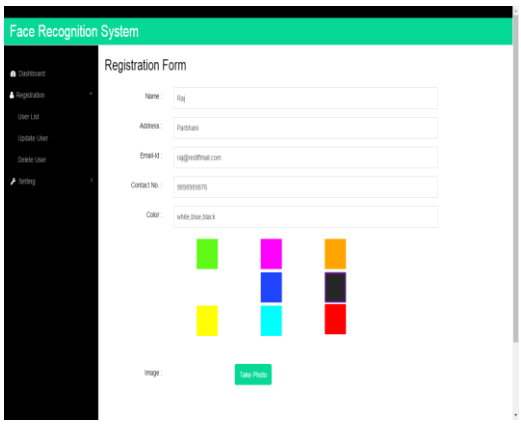
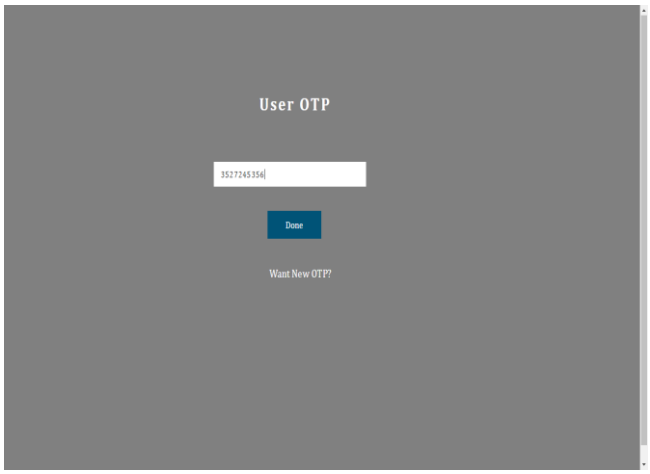


Fig. 3 User Registration



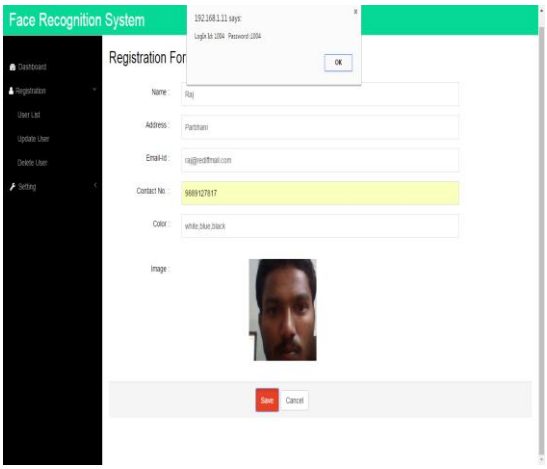


Fig. 4 OTP Page

V. Conclusion

Authentication is crucial for computer security. As the colour matrix password are attack resistant, Facial Recognisation there is a growing interest for them. Presently numerous authentication techniques and models are available. But, each of them have their own pros and cons. In this paper we have proposed a color matrix password scheme that is more resilient to dictionary attacks, shoulder surfing, spyware and phishing attacks. This 2 step random colored matrix password authentication scheme shows promise as a usable and memorable authentication mechanism and also face compare to netbanking login user account.

Acknowledgements

I would like to take this opportunity to thank my internal guide Mrs.Kandalkar S.A. for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful. I am also grateful to Patil H.K. (Head of Computer Engineering Department, Pune) for his indispensable support, suggestions.

References

[1]. Data Compression - DEBRA A. LELEWER and DANIEL S. HIRSCHBERG Department of Information and Computer Science, University of California, Irvine, California 92717 – ACM Journal
[2]. Lossless Data compression techniques - Klaus Holtz, Eric Holtz, Omni Dimensional Networks , San Francisco , CA 94109 – IEEE Research Paper
[3]. RGB Coloured Image Encryption Processes Using Several Colored Keys Images - By Rami El Sawda (IEEE senior member) & Habib Hamam (IEEE senior Member) – IEEE Research Paper
[4]. "Data Can Now Be Stored on Paper" (http:/ / www. arabnews. com/?page=4& section=0& article=88962& d=18& m=11& y=2006.
[5]. "Facial Recognition Applications". Animetrics. Retrieved 2008-06-04

[6]. Airport Facial Recognition Passenger Flow Management". hrsid.com.
[7]. Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
[8]. Smith, Kelly. "Face Recognition" (PDF). Retrieved 2008-06-04.
[9]. R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", IEEE Trans. on PAMI, 1993, (15)10:1042-1052
[10]. Williams, Mark. "Better Face-Recognition Software". Retrieved 2008-06-02.
[11]. Crawford, Mark. "Facial recognition progress report". SPIE Newsroom. Retrieved 2011-10-06.
[12]. Kimmel, Ron. "Three-dimensional face recognition"(PDF). Retrieved 2005-01-01.