V.D. Ambeth Kumar et al. (Eds.)

doi:10.3233/APC210067

Personalized CAPTCHA Using Cognitive Cryptography

Radhika[a,1], Somasundaram.S K[b] and Sivakumar.P [b]
[a,1] *PG Scholar, Dept of IT, PSG College of Technology, Coimbatore, India*
[b]*Assistant Professor, Dept of IT , PSG College of Technology, Coimbatore, India*

Abstract. Cognitive Cryptography is used to improve personal verification process using the individual's characteristics. The personal information contained can be biometrics because it is the unique information that identifies the owner. In advanced cryptographic protocol oriented for authentication of user, there is a possibility of using personal characteristics and perception abilities are required to create a new authentication procedure. This paper presents a new approach for creation of advanced multilevel user authentication protocol by using Image grid CAPTCHA codes. Here the user needs the special skills or knowledge while verifying, this is because of cognitive CAPTCHA's. Instead of generating some random numbers or text while authentication procedure these CAPTCHA's can be used. In multilevel authentication code the user verification can be realized in several iterations, in which the user attention can be oriented on different visual elements, region of interest or semantic content. This cognitive code will able to identify the recognition abilities of the user. Cognitive codes are having high security feature similar to traditional CAPTCHA's because of understanding or recognizing the blurred or distorted patterns and also requires background knowledge to experience the connection with evaluated patterns. This feature guarantees the high level of security and allows to get succeeded in authentication process because the user possess specific skill that or not available for computers or answering systems. The traditional authentication protocols are to be involved with human mental capability is the vital idea of the proposed solution.

Keywords. Cognitive Cryptography, Multi-level authentication, CAPTCHA codes, human mental capability.

1. Introduction

Personal cryptography refers to classifying information in the protocols of data sharing by means of labeling information conducted in accordance to the personal features of the secret holders. Every part of information is subjected to the labeling process executed at the stage of shadow allocation and the identification process conducted at the stage of information reproduction. Based on the biometric features contained in personal information, it is possible to specify clearly that person and whose biometric allocate personal features to right person based on analysis of DNA code, fingerprint, facial, eye, palm, speech, walking manner and characteristics feature of human body organ.

[a,1]Radhika, PG Scholar, Dept of IT, PSG College of Technology, Coimbatore, Tamil Nadu, India.
Email: s.radhika.meenakshi@gmail.com

The personalized cryptography is used to enhance the security while it is being compared to traditional cryptography and which is the main objective of cognitive cryptography. The difference between cryptography and cognitive cryptography is, Cryptography encryption does not depend on cryptographer's personal information or semantic meaning of information. Cognitive Cryptography is based on cryptographers personal data, semantic meaning of information and context of procedure. The semantic information of information or resources is based upon on UBIAS and E-UBIAS cognitive system. The cognitive systems may also use semantic data, by analysing it from the information that is to be secured. It produces a semantic description of the examined information. And then use this description to apply a specific cryptographic procedure aimed at encrypting this information, secretly sharing it or encrypting it.

2. Related Works

A new computational model called semantic data evaluation for cryptographic applications. The semantic meaning of encrypted messages is taken into account. Cryptography procedures and Cognitive approaches are combined to derive new computational model. All such techniques are related to crypto-biometrics techniques and also cognitive and semantic procedures [1]. [2] Introduces a new set of CAPTCHA codes called CATCHA. These codes are very popular and it is used in many applications or website for providing remote services of data accessing Authentication using CAPTCHA ensures that the responses comes from the human or bot. It guarantees confidentiality of data using personal and perceptual characteristics

Multi stages of verification can be done using several iterations. These features guarantee the appropriate level of security and allow to successfully passing verification procedure only for high-qualified users, who possess specific and expertise information, which are not available for computer or answering systems[3].

[4] Introduces a algorithm for maintaining usability in optimizer. The Distortion methods used are: 1) Crowding characters together, 2) random arcs, 3) overlapping characters, 4) Random connected line. Usability is based on following parameters such as learning, efficiency, errors, memorizing and satisfaction [5]. CAPTCHA'S are generated based on face images. The distorted face images will be given, we need to identify the face correctly while there will be non-human images also. And if all responses are correct then test is solved [6].

Development of two new face recognition CAPTCHAS using Farett-Gender and Farett-Gender& Age. The security analysis of both procedures is performed [7]. Process of information sharing usually refers to classified information. The personal verification method is used to reproduce the information[8]. In [9], if users biometric are compromised, it might be impossible or highly difficult to replace it in a particular system. It can be achieved through, combining multiple biometric traits, selecting different feature set from some source of biometric. A new model is designed where a keyword is selected based on lexical chains. The semantic feature of the keyword is used. Trustworthiness is detected using registration stage and detection stage.

3. Proposed Methodologies

Cognitive Cryptography is combination of cognitive skills with traditional cryptography. In traditional cryptography authentication can be done through CAPTCHA's where recognition abilities and noisy patterns makes the system more secure for authentication. Based on iterations users skill can be recognized and ensures confidentiality. The overview of the project is given as a flowchart in figure 1.

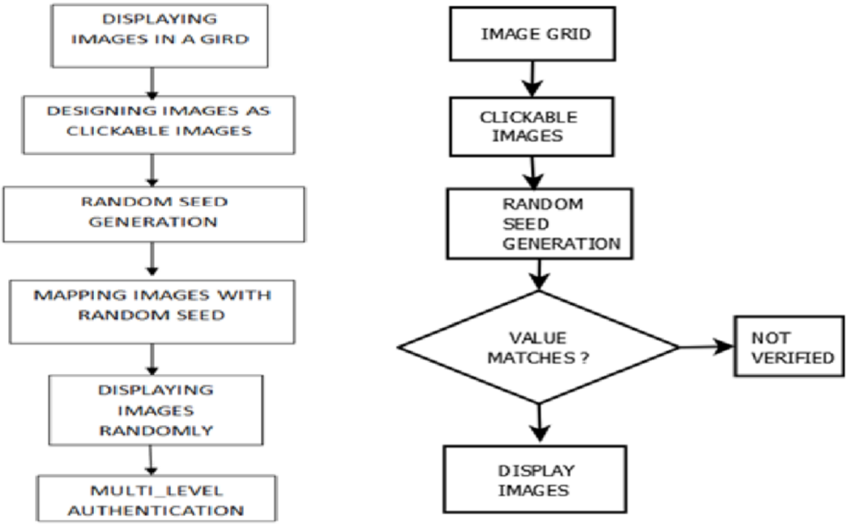
DISPLAYING IMAGES IN A GIRD
DESIGNING IMAGES AS CLICKABLE IMAGES
RANDOM SEED GENERATION
MAPPING IMAGES WITH RANDOM SEED
DISPLAYING IMAGES RANDOMLY
MULTI_LEVEL AUTHENTICATION
IMAGE GRID
CLICKABLE IMAGES
RANDOM SEED GENERATION
VALUE MATCHES ?
NOT VERIFIED
DISPLAY IMAGES

Figure 1. Overall process to be carried out

Modules Description: This project creates a new set of authentication codes based on are verified in multiple stages of verification. Workflow or overall module flow is explained using the figure 2.

3.1 Dataset Description

Dataset consist of images. Images in folders are named in numbers and folders are named using user id. The dataset is taken as sample images. Initially the dataset will have 6 images named as 1.jpg to 6.jpg, three folders named a, b and c. Each folder has 6 images named as 1.jpg to 6.jpg.

3.2 CAPTCHA Generation

Image based CAPTCHA'S are generated as grid, for example I created 4 images in a 2*2 grid. Then images are created as clickable images using Tkinter library. Buttons are created using Tkinter, and are displayed as grid. While displaying images, selection of images is done using random function. Now this list value is separately stored in a variable and it is being compared with the filename. If the filename and variable value matches then function will be called and images will be verified. Multi-level Authentication: Here authentication is done using comparison of values. If first iteration is verified successfully, then another set of verification process is initiated.

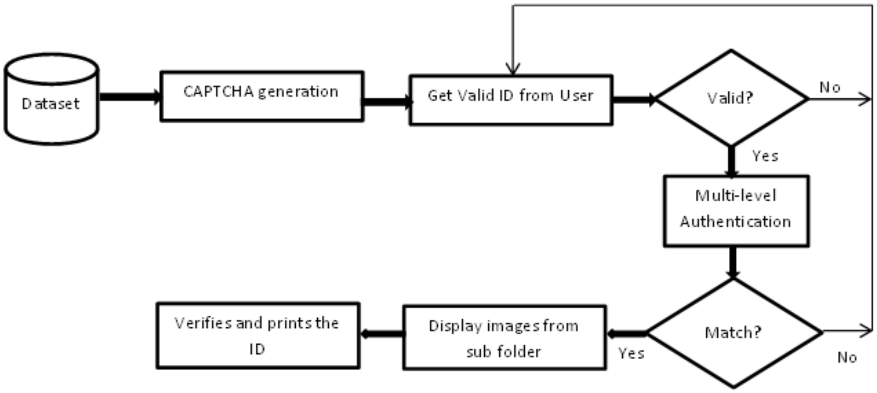
Dataset
CAPTCHA generation
Get Valid ID from User
Valid?
No
Yes
Multi-level Authentication
Match?
Yes
No
Display images from sub folder
Verifies and prints the ID

Figure 2. System Architecture

3.3 CAPTCHA Generation

Grid Formation: Initially, in grid formation using matplotlib grid axes is created. With the help of axesgrid module grid can be created. Then using for loop grid axes of image is displayed. The images are displayed with the help of file directory with image open command. Clickable Images: Tkinter module is used to display the image as clickable image. The title for root window can also be declared using root. title() command. Random Seed Generation: Random can be imported for using random seed function. For example, if the random seed value that is stored is 3 then it will be printed as “verified” else “Not verified”. Selecting Images Randomly From Subfolder: The images from subfolders are to be displayed for first iteration. For example, if we try to click the correct image then it’s based on user-id another set of iteration will happen.

3.4 Validation of CAPTCHA

Validation of CAPTCHA can be done using the def() function. The function can be called in the button command. The button command is used to have an argument command which is used to call the def() function. This is used for validation of images.

3.5 Multi-Level Authentication

Multi-level authentication can be done after the first iteration. The master window is the main window which is used to display the first iteration of images. The second set of images can be titled as multi-level authentication and it is used to display the images randomly. For verification, we can compare the value with the id or subfolder**.**

4. Result Analysis

Initially, a random list is created and is displayed in the command console. The random lists are mapped with string variables for displaying the images accordingly to the list generated. Then for multi-level authentication, based on the id of the user another set of random list is taken and are mapped with string variables. Finally, multilevel authentication is completely processed andthis can be shown in figure 3. Here initially, a random list is generated and got user-is from the user then verifying in first iteration.

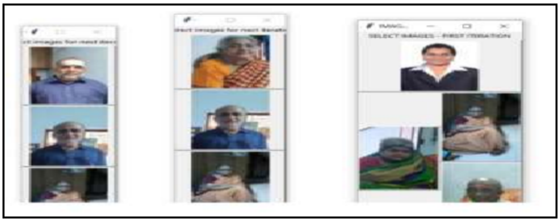

Figure 3. Multi-level authentication

5. Conclusion and Future Work

Thus, the personalized CAPTCHA is created for single user. It is also validated based on his/her special skills. Normally CAPTCHA'S is created for group of user, to overcome this personalized CAPTCHA is introduced. To ensure confidentiality verification is done at each step. For authentication, multi stages verification or set of iterations is used. Cognitive Cryptography follows traditional method and also provides enhanced security for the system. This project can be implemented in banking system for authentication or verification of a user while he or she is trying to login to the application. User's knowledge is being tested in all the iteration so that bypassing the credentials will be impossible. In future work, protecting dataset and the scalability issue of maintaining such a large image based dataset have to be addressed as well.

References

[1] Marek R. Ogiela, Lidia Ogiela. On Using Cognitive models in Cryptography. 2016 IEEE 30th International Conference on Advanced Information Networking andApplications.

[2] Marek R. Ogiela, Lidia Ogiela. Multi-level Authentication Protocols Using Scientific Expertise Approach. Springer Nature Switzerland AG 2020 L. Barolli et al. (Eds.): AINA 2019, AISC 926, pp. 176–180,2020.

[3] Suliman A. Alsuhibany. Evaluating the Usability of Optimizing Text-based CAPTCHA Generation. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 8,2016.

[4] DonghuiHu,JuanZhang,XuegangHu,LianWang,WenjieMiao,ZhengfengHou.Textssource trustworthiness detection based on cognitive hash.

[5] Rui Zhang, Yu-Jie Hao, Wei-Hua Zhang, Qiao-Ling Han, Zhi-Peng-Lu. MultiBiometric Feature Identification Technologies Based On Visual Perceptionand Cognitive Mechanism. 978-1-4244-3425-1/08/$25.00 ©2008 IEEE.

[6] Marcin Piekarczyk, Marek.R.Ogiela. The touch-less person authentication using gesture type emulation of handwritten signature templates. 2015 10th International Conference on Broadband and Wireless Computing, Communication andApplications.

[7] Gaurav Goswami, Brain M.Powell, Mayank Vatsa, Richa Singh, Afzel Noore. FaceDCAPTCHA: Face detection based color image CAPTCHA. Future Generation Computer Systems Volume 31, February 2014, Pages 59- 68.

[8] Guido Schryen, Gerit Wagner, Alexander Schlege. Development of two novel facerecognition CAPTCHAs: A security and usability study. Computers & Security, Vol. 60, July 2016, Pages95-116.

[9] Lidia Ogiela, Marek R. Ogiela. Bio-Inspired Cryptographic Techniques in Information Management Applications,2016.