12. Return Visually encoded **vOTP**
13. Server forwards the generated visual OTP to client/user via SMS/MMS/Other-App.
14. Client/User submits the OTP on web portal, wherever it is required or requested.
15. Server receives the reply as OTP submitted by client/user
16. Server verifies the OTP reply.
17. Returns the decision logic

6. Result Analysis

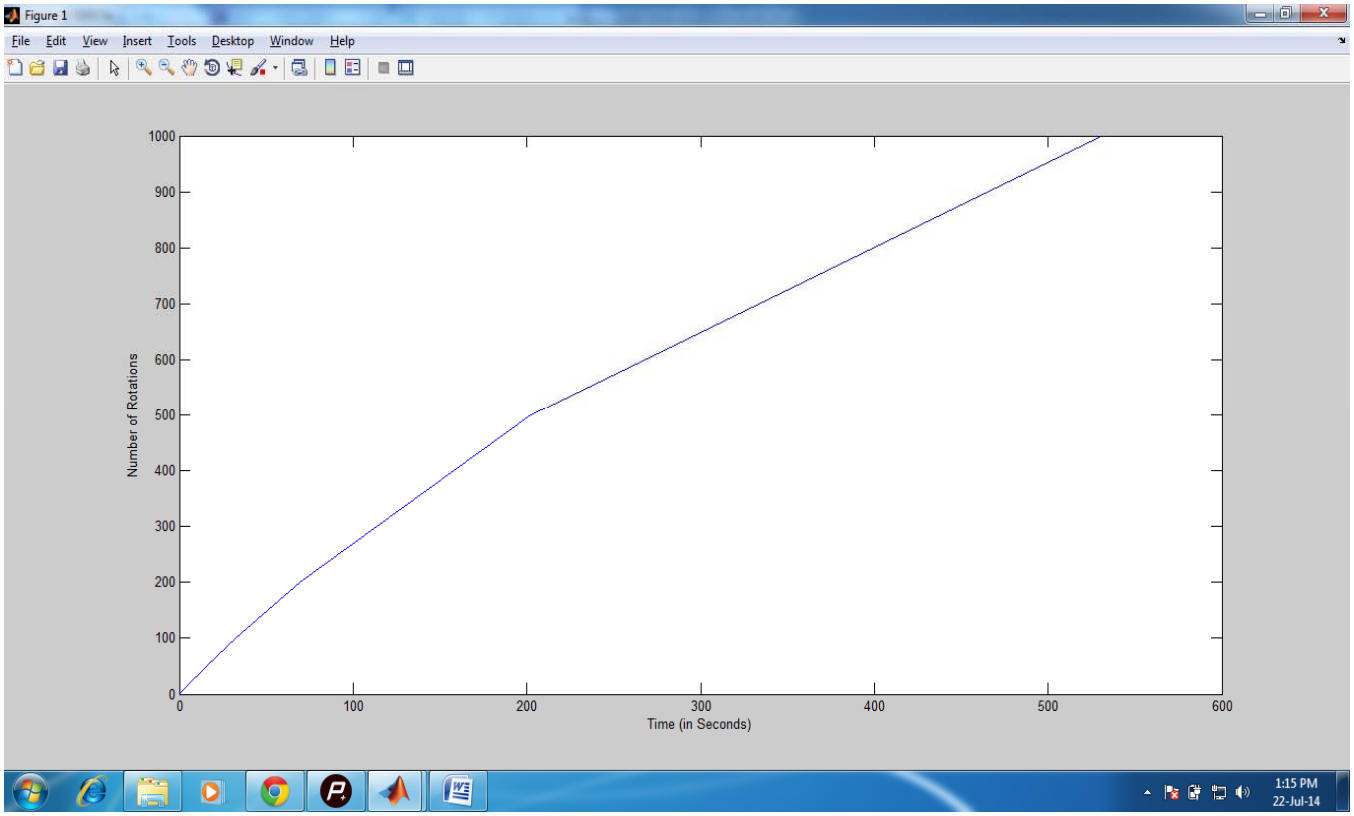
The experimental design has been developed using MATLAB simulator and the results have been observed and analyzed deeply. The OTP generation procedure is using multi-level random value generation from the sphere, and further concatenated in uneven fashion to produce the unique one time password every-time. One time password generation process is flexible and unique to produce the unique one time passwords at one point of time to reduce the possibility of two users receiving the same password at one point of time. This random one time password generation framework can used with medium or smaller sized web or utility based portals. This sequence will be able to handle thousands to tens of thousands of users at one point of time. The uniqueness calculation has shown that this OTP framework is capable of handing flexible number of unique OTP at one point of time with minor changes in the program sequence. The framework simulation is designed to generate the one time password which is followed by visual encoding to produce one time image password (OTIP). OTIP is then forwarded to the client side, where client enters the password the

Table 1: The uniqueness of one-time passwords shown for 5 rotations

Sr. No.	Rotation 1	Rotation 2	Rotation 3	Rotation 4	Rotation 5
1	25286222	209279231	248264273	289234261	238292210
2	27422498	287294297	283218245	107271247	263180221
3	256159207	202283285	294244194	136262282	270171123
4	138292287	115206291	102187199	296264253	184291160
5	165252216	264273278	229227134	205258277	284232255
6	152262204	151261283	289260210	43249272	128251226
7	273265151	250202227	230254287	255200256	292149276
8	286269237	287245139	297240197	213295190	291227266
9	286162191	184223227	218244197	300273282	20116962
10	259299293	264220274	156246276	263216188	193295229

Table 2: The Time (in seconds) to Rotations size comparison table

Rotation Size	1	10	50	100	200	500	1000
Time in seconds	0.3484	3.1416	15.6925	32.6291	69.2329	201.9823	530.5974



Graph 1: The time (in seconds) to Rotation size graph

OTP input box and submit the information to the server side. The server then verifies the original OTP with the generated OTP and returns the decision logic, which is further used to take the programmed action in the software architecture according to the decision logic. The OTP send by the Client to Server is compared with the OTP generated and saved at the Server. If the both OTPs are same, then the OTP is verified and the access is granted.

Figure 1: The Server Graphical Interface

Figure 2: Generate One Time Password

Figure 3: Convert Integers into Image

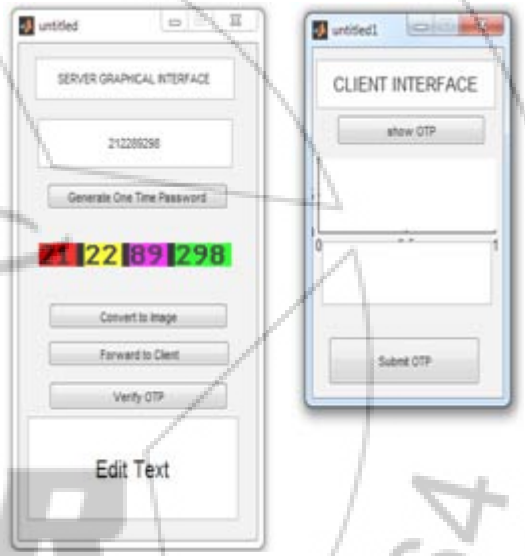


Figure 4: Forward the Image Based Password to the Client

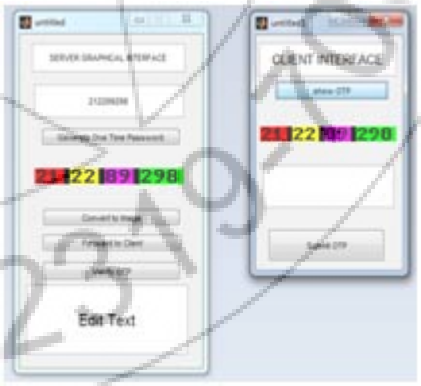


Figure 5: Client Interface receives Image Based Password.

Figure 6: The user or client reads and Fill the image password.

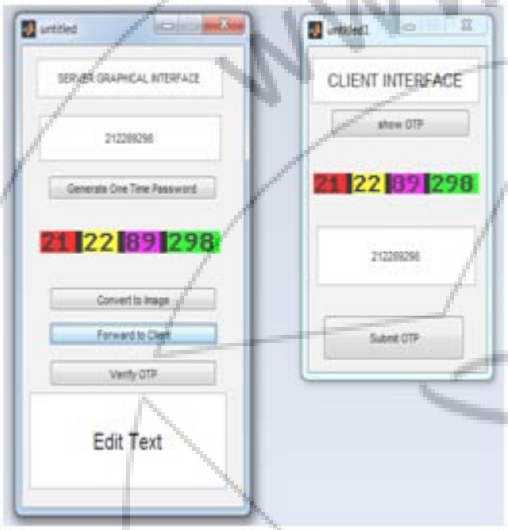


Figure 7: The user submit the OTP to the server.

Figure 8: The OTP Verification and decision Logic

7. Conclusion

OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are used in real-time systems. Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time), Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order) or Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter. The purpose of a **one-time password** (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced. But the text based one time passwords are not being proved to be strong enough to protect against the bots accessing the online portals. Hence, there has to be an strong and secure alternative to the text based one time passwords. By taking the above research gap in account, the new one time password authentication system is proposed in this research. The proposed one time password scheme is a scheme which can be widely accepted over the internet applications. This scheme generates the password using the sphere random function, which carries a heavier amount of numbers and can produce many unique combinations. Spherical random function is capable of generating more unique combinations of integers than any other mathematical random function. Then the random is uniquely selected among the sphere matrix, which creates more unique passwords. The conversion of the integer based password into image hardens the security layer of the mobile/SMS based authentication environments. Also, sphere random function generates the passwords very quickly, which means it is perfectly adaptable to the internet application scenarios with millions or billions of users.

8. Future Work

In future this scheme can be enhanced using the dizzy images scheme, which also protect against the botnets/autobots with image processing or optical character recognition capability. Also this scheme can be enhanced to produce alphanumeric passwords and can be used with existing or improved visual encoding scheme. Some new scheme can proposed in future to generate the passwords in larger number than the proposed system to meet the requirements of the large online enterprise applications. Also the new one time password scheme can be used along with the SSL or other innovative encryption layer to produce the more secure one time password authentication system.

References

[1] R.R.Karthiga, 2013.“One-time Password: A Survey”, International Journal of Emerging Trends in Engineering and Development Issue 3, Vol.1, pp. 613-623.
[2] Ahmad Alamgir Khan, 2013. “Preventing Phishing Attacks using One Time Password and User Machine Identification”, International Journal of Computer Applications (0975 – 8887) Volume 68– No.3.
[3] Indu S., Sathya T.N., Saravana Kumar V., 2013“ A Stsnd-alone and SMS-Based approach for

Authentication using Mobile Phone", IEEE-International Conference on Information Communication and Embedded.
[4] Andrew Y. Lindell, 2007."Time versus Event Based One-Time Passwords", Aladdin Knowledge Systems.
[5] Soonduck Yoo1 , Seung-jung Shin1, Dae-hyun Ryu1, 2013. "An effective Two Factor Authentication Method using QR code", ISA 2013, ASTL Vol. 21, pp. 106-109, © SERSC 2013.
[6] S. Behal, A. S. Brar, and K. Kumar, "Signature based Botnet Detection and Prevention", ISCET, pp. 122-127, 2010.
[7] Bin Li, Shaohai Hu, Yunyan Liu, 2006."A Practical One-Time Password Authentication Implement on Internet", ICWMMN Proceedings.
[8] Ping Wang, Lei Wu, Baber Aslam and Cliff C. Zou, 2009. " A Systematic Study on Peer-To-Botnets", International Conference on Computer Communications and Networks, 2009. ICCCN 2009. San Francisco, CA, IEEE.
[9] Yu tao, Fan, Gui ping, Su, 2009."Design of Two-Way One-Time-Password Authentication Scheme Based On True Random Numbers", Second International Workshop on Computer Science and Engineering, pp. 611-614.
[10] Jivika Govil, 2007. "Examining the Criminology of Bot Zoo", IEEE.
[11] Mihai Ordean, 2012. "Secure Authentication Using One Time Visual Password", Ph.D. Dissertation, The technical university of Cluj-Napoca.
[12] Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, and Jingyuan Zhang, 2009." Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures", Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2009,11 pages doi:10.1155/2009/692654
[13] Julian B. Grizzard, Vikram Sharma, Chris Nunnery,and Brent Byung Hoon Kang, David Dagon, 2007, "Peer-To-Peer Botnets: Overview and Case Study". HotBots'07 Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets. USENIX Association Berkeley, CA, USA.
[14] Abebe Tesfahun and D.Lalitha Bhaskari, 2013. "Botnet Detection and Countermeasures- A Survey", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, ISSN 2278-6856.
[15] Takasuke TSUJI, 2003. "A One-Time Password Authentication Method", Kochi University of Technology.
[16] Márk Jelasity, Vilmos Bilicki, 2009. "Towards Automated Detection of Peer-To-Peer Botnets: On the Limits of Local Approach", Hungary, www.usenix.org