



KALEIDOSCOPIC EXHIBIT KEYPAD: A HUMAN-MACHINE INTERFACE FOR PIN ENTRY SECURITY

¹M.Sangeetha, ²R.Vidhya.

Department of Information Technology
Vel Tech Multi Tech Dr.RR Dr.SR Engineering
College,
Chennai, Tamilnadu
{sangeethait1997@gmail.com, vidhyaraja1396@gmail.com}

³Ms.A.Mary Judith, M.Tech,

Assistant professor,
Department of Information Technology
Vel Tech Multi Tech Dr.RR Dr.SR Engineering
College,
Chennai, Tamilnadu.
maryjudith@veltechmultitech.org

ABSTRACT:

An individual ID number (PIN) is a numerical code utilized as a part of numerous electronic money related exchanges. They are additionally typically required when utilizing bank charge or mastercards, and most banks or money related foundations issue PINs independently from the cards through the mail. They play the most important part in authentication process. We face a major drawback while performing transactions by having Disguise Camcorder which may lead to reveal of the four digit code. In our

proposed system we implement two methods to prevent these kind of problems, Kaleidoscopic Exhibit keypad method and Enigma pin method by displaying shuffled keypad by generating aOTP (One Time Password).

Keywords: Enigma pin, Kaleidoscopic exhibit, one time pin, color keypad

I. INTRODUCTION

A pin entry device is required for all kinds of bank and ATM transactions. A unique pin number is provided to every card holder for more secure and safe transactions. The user needs to be authenticated by the bank for availing the services provided. Be that as it may, the right now utilized direct stick passage technique is more at risk to bear surfing, infra-red and disguised camcorder assaults. Shoulder surfing attacks occur when the unique pin is tracked using the amount of heat generated in the keypad using infra-red rays. A concealed camcorder is also placed above the pin entry keypad, so that the hackers come to know the user's secret pin which is mishandled. Hence an indirect pin entry method has to be used to prevent such attacks. SteganoPIN method is one of the indirect pin entry method. This is a framework for secure pin authentication system.

The human-machine interface of Stegano PIN requires two numeric keypads, one reaction (general) and the other test (shuffled). In this technique, the stick passage requires two gadgets which might be troublesome now and again and furthermore causes more issues in regards to vicinity. Thus our proposed system finds a solution to the above problems by using two methods for pin authentication: **Enigma Pin method** and **Kaleidoscopic exhibit keypad method**.

Enigma pin method uses only a single device for pin entry and authentication, reducing the complications with respect to **Proximity**. In Kaleidoscopic display technique, the human-machine interface is through two keypads, one hued and the other for all intents and purposes shaded. The virtually colored keypad prevents shoulder surfing attacks, difficulties regarding proximity and paves the way for more secure transactions.

II. EASE OF USE:

Our system mainly reduces numerous attacks which occur during pin entry and improves authentication and proximity services thereby providing a secure transaction to the user.

III. RELATED SURVEY:

In [1] J. Long and J. Wiles, showed that the Clients regularly reuse same customized recognizable proof numeric system for various sessions. Coordinate numeric sections can be powerless for bear to break assaults and

successfully watch PIN section with covered cameras. Backhanded PIN passage techniques proposed as countermeasures are seldom conveyed on the grounds that they request a heavier subjective workload for clients. To accomplish security and ease of use and display a useful aberrant PIN section technique called SteganoPIN. It has two main numbered systems, first is the secured, the second one is unclosed.

In [2] A. Greenberg demonstrated that the primary target, of this paper is to configuration "Secured ATM exchange utilizing Stegano PIN". Clients need to utilize the same customized ID number (PIN) for numerous frameworks and in different sessions. Coordinate PIN passages are to a great degree in danger of shoulder-surfing assaults as assailants can viably watch PIN section with concealed cameras. To accomplish security and convenience, we show a sensible backhanded PIN section procedure called Stegano PIN, intended to physically piece bear surfing assaults. In the fundamental UI of Stegano PIN, one numeric keypad is a standard keypad in customary design and the other in an arbitrary format called the test keypad. The test keypad changes concurring with the ultrasonic sensor.

In [3] V. Roth et al, demonstrated that another strategy, which disguises data about the secret word however much as could be expected, is proposed. covering the secret word objects and the quantity of watchword protests, the proposed technique permits both secret word and

distracter articles to be utilized as the test set's info. The effectively entered secret word gives off an impression of being arbitrary and must be inferred with the information of the full arrangement of watchword objects. So it would be troublesome for a shoulder-surfing to distinguish the client's real secret word. Recreation comes about demonstrate that the right information question and its area are arbitrary for each test set, in this way avoiding recurrence of event investigation assault. In [6] A. Parti and F. Z. Qureshi depicted that the "Secured ATM exchange utilizing Stegano PIN". So the essential UI of Stegano PIN, one numeric keypad is a standard keypad in consistent format and the other in an arbitrary design called the test keypad. The test keypad shifts concurring with the ultrasonic sensor. A client must utilize this test keypad to determine a crisp OTP, the inferred OTP is then entered on the reaction keypad. For every single PIN section the framework catches the client's picture by utilizing UVC camera and sends it to enrolled mail ID.

In [10] S. Wiedenbeck et al depicted that entering private content, for example, passwords that they enable spectators to make sense of what has been written just by viewing, we show the Spy-Resistant Keyboard, a novel interface that enables clients to enter private content without uncovering the eyewitness. We depict a client think about we hurried to investigate the ease of use of the interface and also extra security gave by it. At last it show that clients took more time to enter their passwords,

utilizing the Spy-Resistant Keyboard as opposed to a standard onscreen delicate console to increment in their capacity to shield their passwords from a careful spectator. In [14] P. Golle and D. Wagner, demonstrated that the assaults against two psychological confirmation plans [9] proposed at the 2006 IEEE Symposium on Security and Privacy. These verification plans are intended to be secure against listening in assaults. it accomplish validation by means of test reaction conventions in view of a mutual mystery set of pictures. Our assaults utilize a SAT solver to recoup a client's mystery enter in almost no time, subsequent to watching few fruitful logins.

In[15] H. Sasamoto, N. Christin, and E. Hayashi, portrayed that as of late logical writing, numerous proposition have been made to expand the protection of secret word frameworks to bear surfing assaults. These passwords are called bear surfing safe realistic passwords (SSRGPs). This paper exhibits a general methodological way to deal with breaking down and assessing the protection of SSRGPs, which can be portrayed as far as the information tables. Recently, in connection with the advent of miniature webcams and the widespread use of smartphones with video recording, the danger of shoulder surfing the password when it is entered by the user at various terminals (ATM, computer keyboard, smartphones, etc.) has increased. To protect against these attacks, many password systems have been proposed, which have received the generalized name of shoulder-surfing resistant graphic passwords (SSRGPs). All of these password systems are certainly

different, but they are based on the principle of not directly entering a password character or a password in general. When performing the authentication procedure, the user does not enter the password character itself (PC), but a character that is somehow associated with it and with other characters.

In [16] A. Bianchi et al, showed that Ubiquitous computing enabled by mobile devices, such as smartphones and tablets, causes more exposure of device users to shoulder-surfing attacks in crowded places, such a subway train. shoulder-surfing resistant mobile authentication scheme based on board games. So the design of Pass Game is based on the popular game of chess. PassGame challenges a user with a random formation of chesspieces on a game board. A successful authentication requires a user to respond to the challenge so that a set of predefined rules are satisfied after adjustments made by the user.

In [17] A. Bianchi, I. Oakley, and D. Kwon, demonstrated that the Authentication in broad daylight spaces is naturally presented to perception assaults in which passwords are stolen by the straightforward demonstration of viewing the information input process. Tending to this issues the safe confirmation input by means of PINs or passwords that depend on sets of generally imperceptible material or sound signals. Nonetheless, secure such frameworks are normally conjure abnormal amounts of load in their clients which verification times and high mistake rates and undoubtedly because of

critical psychological requests regarding handling, mapping or reviewing non visual data.

IV. RELATED CONCEPTS:

A. STEGANOGRAPHY:

Steganography is the act of hiding a document, message, picture, or video inside another record, message, picture, or video. Steganography incorporates the camouflage of data inside PC documents. In computerized steganography, electronic interchanges may incorporate steganographic coding within a vehicle layer, for example, a record document, picture record, program or convention. In our framework, we utilize the idea of steganography to produce a rearranged keypad for steganopin confirmation framework.

B. ONE TIME PASSWORD:

A one-time secret word (OTP) is a watchword that is substantial for just a single login session or exchange, on a PC framework or other advanced gadget. OTPs dodge various deficiencies that are related with conventional (static) watchword based confirmation. In steganopin confirmation framework, the client finds the PIN in normal keypad and along these lines maps the key areas in to the arbitrary rearranged keypad for OTP determination and after that enters the OTP on a general keypad called the response keypad.

C. MATHEMATICAL ALGORITHM:

In the kaleidoscopic exhibit keypad generation, **two** keypads, one **colored** and the other **virtually colored** is used. The virtual coloring to the numeric keypad is achieved according to a probability check using mathematical algorithm.

In the Enigma pin method, **two** numeric keypads, one **response** (regular) and the other **challenge** (shuffled) is used. A unique challenge (shuffled) keypad is generated using a mathematical algorithm.

The achievement likelihood is $m/104$ for m endeavors and $1/104 - m + 1$ for the m th endeavor of speculating, for $1 < m < 104$ in light of the fact that the test keypad and the reaction keypad render a balanced mapping in each verification session.

V. EXISTING SYSTEM:

The typical stick passage strategy is the one in which the stick section is done through a common keypad. At whatever point a client straightforwardly enters a mystery PIN into a frameworks, security is effectively traded off, especially out in the open spots. The camera-based shoulder-surfing assailant is characterized as a more grounded rival helped by a programmed recording instrument, for example, a wearable camera, to record and examine whole exchanges successfully. At the point when a client enters an individual ID number (PIN) as a numeric secret word in versatile including ATM, an immediate perception assault in light of shoulder surfing winds up incredible concern.

The PIN section can be seen by adjacent rival, all the more viably in a swarmed place. Since a similar PIN is typically picked by a client for different purposes and utilized more than once, a bargain of the PIN may cause the client an incredible hazard.

VI. DRAWBACKS IN THE EXISTING SYSTEM:

The normal pin entry method is more liable to shoulder surfing attacks and infrared attacks. In the steganopin method, the pin entry requires two devices which may be difficult at-times and also causes more issues regarding proximity.

VII. PROPOSED SYSTEM:

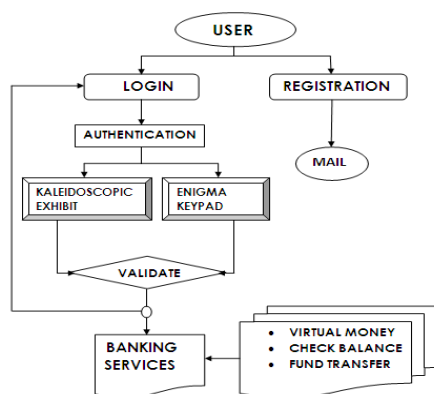
In the proposed system, pin entry can be done by two ways: Enigma pin method and Kaleidoscopic exhibit keypad method.

In Enigma pin method, an enhancement of using only **one device** for pin entry (instead of two) is made, which reduces the complications with respect to **proximity**. In kaleidoscopic exhibit keypad method, we use a randomly generated four digit sent to the user's registered email which must be used by the user whenever a transaction is to be made and the pin entry for transactions is accomplished by a **virtual keypad**. The human-machine interface of this strategy is through two keypads, one shaded and the other for all intents and purposes hued. The virtually colored keypad appears beneath the numeric keypad. There are two options for each numeral either upper half or lower half, so that the user selects either one and uses it throughout

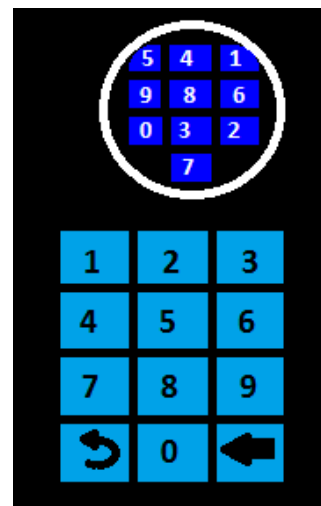
the pin entry. The colors in the virtually colored keypad is shuffled each time when the user makes his pin entry. The user maps the uniquepin with the virtual keypad and types the color option in the colored keypad which appears in the bottom. An enhancement of using striped lines and dotted lines (instead of colors) for color blind people is made.

VIII. RELATED DIAGRAMS:

A.ARCHITECTURE DIAGRAM:



B.ENIGMA PIN KEYPAD (SAMPLE):



C.KALEIDOSCOPIC EXHIBIT KEYPAD (SAMPLE):



IX. CONCLUSION AND FUTURE USE:

In this venture, two secure jumbled PIN verification convention for ATM and other purpose of-benefit terminals utilizing individual cell phones is constructed. An enhancement of using striped lines and dotted lines (instead of colors) for color blind people is made. Our system can be extended by increasing the number of colors in the kaleidoscopic exhibit

method so that pin entry sessions can be reduced.

REFERENCES:

- [1] J. Long and J. Wiles, *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Boston, MA, USA: Syngress, 2008.
- [2] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your pass- code with a glance,” *Wired*. [Online]. Available: 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance /
- [3] V. Roth, K. Richter, and R. Freidinger, “A PIN-entry method resilient against shoulder surfing,” in *Proc. ACM Comput. Commun. Security*, 2004, pp. 236–245.
- [4] T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 6, pp. 716–727, Jun. 2014.
- [5] Q. Yan, J. Han, Y. Li, and R. H. Deng, “On limitations of design- ing leakage-resilient password systems: Attacks, principles and usability,” in *Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp.*, 2012, pp. 1–16.
- [6] A. Parti and F. Z. Qureshi, “Integrating consumer smart cameras into camera networks: Opportunities and obstacles,” *IEEE Comput.*, vol. 47, no. 5, pp. 45–51, May 2014.

- [7] B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-chowdhury, "Distributed camera networks," *IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 20–31, Apr. 2011.
- [8] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security—A field study of real world ATM use," in *Proc. ACM Symp. Usable Privacy Security*, 2010, pp. 1–10.
- [9] T. Matsumoto and H. Imai, "Human identification through insecure channel," in *Proc. Adv. Cryptol.*, 1991, pp. 409–421.
- [10] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proc. ACM Int. Working Conf. Adv. Visual Interfaces*, 2006, pp. 177–184.
- [11] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proc. IEEE Symp. Security Privacy*, 2006, pp. 295–300.
- [12] A. De Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN—Securing PIN entry through indirect input," in *Proc. ACM CHI Conf. Human Factors Comput. Syst.*, 2010, pp. 1103–1106.
- [13] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, "Cryptoanalysis of the convex hull click human identification protocol," in *Proc. 13th Int. Conf. Inf. Security*, 2010, pp. 24–30.
- [14] P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication scheme," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 66–70.
- [15] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of prying eyes," in *Proc. ACM SIGCHI conf. Human Factors Comput. Syst.*, 2008, pp. 183–192.
- [16] A. Bianchi, I. Oakley, V. Kostakos, and D. Kwon, "The Phone Lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in *Proc. 5th Int. Conf. Tangible, Embedded, Embodied Interaction*, 2011, pp. 197–200.
- [17] A. Bianchi, I. Oakley, and D. Kwon, "Spinlock: A single-cue haptic and audio PIN input technique for authentication," in *Proc. Haptic Audio Interaction Design*, 2011, pp. 81–90.

