Invention Journal of Research Technology in Engineering & Management (IJRTEM)
ISSN: 2455-3689
www.ijrtem.com Volume 2 Issue 1 ǁ January. 2018 ǁ PP 05-10

Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks in ATM

S. Preema ,
Department of Computer Science, VLB Janakiammal College of Arts & Science, Coimbatore, Tamilnadu

ABSTRACT : *The scope of this work extends to system components (for example service providers, networks, servers, hosts, applications, processes and personnel) which are used to exchange PIN-related data. The PIN Guidelines in this document encompass PIN security within any one system or sub-system and between systems. This process designs 10 digit keypad with random RGB color SCHEME using a Fast Finite-State Algorithm for Generating RGB Palettes of Color. In this work, we propose a color finite-state LBG (CFSLBG) algorithm that reduces the computation time by exploiting the correlations of palette entries between the current and previous iterations.*

KEYWORDS: *Palettes , Color quantization, LBG algorithm, finite-state algorithm,*

I. INTRODUCTION

This work is designed to provide PIN security guidelines for all payment accounts that use a PIN, including those associated with magnetic stripe cards, chip cards, 'hybrid' cards that incorporate both a magnetic stripe and a chip or any other cardholder payment device form factor The scope of this work extends to system components (for example service providers, networks, servers, hosts, applications, processes and personnel) which are used to exchange PIN-related data. The PIN Guidelines in this document encompass PIN security within any one system or sub-system and between systems. These guidelines are targeted at PIN protection during PIN processing in the issuer security domain. PIN processing of interchange transactions is covered by the PCI PIN Security Requirements. A PIN (Personal Identification Number) is a four to twelve digit number known by a cardholder and used to authenticate the cardholder to the card-issuing bank (or to the cardholder's ICC). The transaction PIN is the PIN entered by the cardholder during a payment transaction. The online PIN is the transaction PIN used to verify the cardholder online. The offline PIN is the transaction PIN used with an ICC to verify the cardholder offline. The reference PIN is a stored or derived PIN value used by the issuer to verify the transaction PIN.

If stored in an ICC it may or may not be equal to the online PIN. The PIN management guidelines in this document refer to the following processes. The primary objective of this research paper is to provide a complete knowledge of ATM and a solution to its pin entry process. To access the funds which are kept in the bank at any time is not an easy task but today it is not at all difficult. A person just has to tell his bank that he wants an ATM card. The bank issues him an ATM card which is pass coded and could be used by him alone. ATM card is called by different names like bank card, MAC(Money access card), client card, key card or cash card, etc. In most cases even debit and credit card could be used. The ATM card helps the customer to be identified by a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip. The security is provided by the customer entering a personal identification number (PIN). Now the person who needs funds when he is taking his family out of shopping or when he requires funds for an outing it is easily done. If someone falls very seriously ill the person can remove the funds in the middle of the night too. The ATM machine helps the customer to make his / her life much easier. It does most The ATM card is slowly replacing cheque, the personal attendance of various customers, has increased banking hours and reduced the holidays. They do not require any paper based verification. Due to heavier computing demands and the falling price of personal computer–like architectures, ATMs have moved away from custom hardware architectures using microcontrollers or application-specific integrated circuits and have adopted the hardware architecture of a personal computer, such as USB connections for peripherals, Ethernet and IP communications, and use personal computer operating systems.

II. NATIONAL / INTERNATIONAL STATUS

Today, the vast majority of ATMs worldwide use a Microsoft Windows operating system, primarily Windows XP Professional or Windows XP Embedded. A small number of deployments may still be running older versions of the Windows OS, such as Windows NT, Windows CE, or Windows 2000. There is a computer
industry security view that general public desktop operating systems(Dos) have greater risks as operating systems for cash dispensing machines than other types of operating systems like (secure) real-time operating systems (RTOS). RISKS Digest has many articles about ATM operating system vulnerabilities.[1]With the onset of

Windows operating systems and XFS on ATMs, the software applications have the ability to become more intelligent. This has created a new breed of ATM applications commonly referred to as programmable applications. These types of applications allows for an entirely new host of applications in which the ATM terminal can do more than only communicate with the ATM switch. It is now empowered to connect to other content servers and video banking systems. Notable ATM software that operates on XFS platforms include Triton PRISM, Diebold Agilis EmPower, NCR APTRA Edge, Absolute Systems AbsoluteINTERACT, KAL Kalignite Software Platform, Phoenix Interactive VISTAatm, Wincor Nixdorf ProTopas, Euronet EFTS and Intertech inter-ATM. With the move of ATMs to industry-standard computing environments, concern has risen about the integrity of the ATM's software stack.Security Experts says that Automatic Teller Machine (ATM) in future will have biometric authentication techniques to verify identities of customer during transaction. In South America, there are companies that have introduced fingerprint technology as a embedded part of ATM systems, where citizens have already started using fingerprint in place of PIN or Password for general identification with their ID cards. Nowadays, there are devices to perform biometric identification and authentication of following: fingerprint, hand, retina, iris, face, and voice. India is still lacking in implementing biometric with smart card as a safety approach. Fingerprint approach for identification given by Oko S. and Oruh J. (2012) not proved efficient as when citizen will move to ATM system, fingers may become dirty from natural environment and will not be able to access his account with ATM system, since fingerprints will not match from the one that was traced during identification. Secondly, a iris and retina approach proposed by Bhosale S. and Sawant B.(2012) as a identification method, but citizens might not want a laser beamed into their eyes for retina scan at every time he wants to access account through ATM. Thus, iris and retina as identification authentication proved inefficient. Vibration detector sensor were also proposed as a security system for ATM machines by Ajaykumar M. And Bharath Kumar N.(2013). Voice was also proposed for security in ATM systems as a biometric with smart card. The cons were there at the same time as two citizens can have same voice and one can easily hack and can fraud with another's account.

Objectives : Our proposed scheme is based on an elegant adaptive black-and-white to coloring of the 10-digit keypad in the standard layout. Proposed method requires many user inputs, so that human guessing pin Entry becomes a difficult process. The new scheme has the remarkable property of resisting camera-based recording attacks over an unlimited number of authentication sessions without leaking any of the PIN digits. In the earlier method user enters a pre-arranged textual, numerical password directly through the user interface of the authentication system. So, the password submission process is prone to direct observational attacks. Entry of a password can easily be observed by nearby adversaries in crowded places, aided by vision enhancing and/or recording devices. Due to its short length and the simplicity of the ten-digit keypad guess of password is easy.

The main features include:

1. Pin security is very high.
2. Tictoc PIN holds two measures that can prevent information leakage.
3. More Efficient so that we can use any Type of pin Entry application.

III. METHODOLOGY

This project, proposes virtualizing Harvard architecture on top of the existing memory architecture of modern computers, including those without non-executable memory page support, so as to prevent the injection of malicious code entirely. Harvard architecture is simply one wherein code and data are stored separately. Data cannot be loaded as code and vice-versa. In essence, we create an environment wherein any code injected by an attacker into a process' address space cannot even be addressed by the processor for execution. In this way, we are attacking the code injection problem at its root by regarding the injected malicious code as data and making it unaddressable to the processor during an instruction fetch. Split memory architecture produces an address space where data cannot be fetched by the processor for execution. For an attacker attempting a code injection, this will prevent him from fetching and executing any injected code. It includes the following process:

PIN LAYOUT DESIGN PROCESS: This process designs 10 digit keypad with random RGB color SCHEME using a Fast Finite-State Algorithm for Generating RGB Palettes of Color. In this work, we propose a color finite-state LBG (CFSLBG) algorithm that reduces the computation time by exploiting the correlations of palette entries between the current and previous iterations. Instead of searching the whole color palette, the
CFSLBG algorithm searches only a small number of colors that are very close to the training vector. Thus, the computation time for color quantization is reduced. The proposed approach generates RGB palettes efficiently. This work describes the implementation of this algorithm and simulation results. Video monitors typically use the three primary color components, red, green, and blue, to specify the color of each pixel in a color image. Each

primary component usually provides 8 bits for specifying the color of each pixel in a full-color digitized image. Color quantization algorithms can be grouped into splitting algorithms and clustering-based algorithms. Clustering-based algorithms extract quantized colors by applying various clustering algorithms. In this paper, we propose an effortless and straightforward clustering algorithm, which is fast and excellent for generating colour palette. Vector quantization (VQ) has been shown to be an efficient method of image coding. The input vectors are individually quantized to the closest codeword in the codebook. The codebook is generated by using some clustering algorithms from a set of digits. The iterative clustering algorithm proposed by Linde, Buzo, and Gray (LBG) is usually used in VQ . A number of methods for generating color palettes using the VQ codebook design techniques were proposed. In view of color image coding, each pixel can be considered as a 3-dimension vector in the RGB color space. These vectors are the input vectors of the color VQ (CVQ) scheme. The LBG algorithm is most popular method used to select a color palette with a limited number of colors from a full-color digitized image. In each iteration of the LBG algorithm, it searches the whole color palette in order to find the corresponding palette entry for each training vector. That is, the LBG algorithm requires a large amount of computation for color quantization. This paper proposes a novel color finite-state LBG (CFSLBG) algorithm that reduces the computation time required to select palettes . Instead of searching the whole color palette, the proposed algorithm searches only a small part of the palette to find the corresponding palette entry for each training vector. In the CFSLBG algorithm, the number of palette entries that need to be searched for a training vector in each iteration is always much smaller than the size of the whole palette. For this reason, the duration of each iteration is greatly reduced.

COLOR FSLBG ALGORITHM : Although the VQ scheme yields acceptable performance for image coding, the finite-state vector quantization (FSVQ) schemes [16-21] improve performance for an ordinary VQ. An FSVQ can be viewed as a finite collection of ordinary VQ's, each with its own codebook associated with a state, which is called the state codebook. The encoding state of the current input vector is decided by a state function F(x). This coding state may be described by a state variable $s \in S = \{si : i = 1, \ldots, M\}$, where M is the total number of states. The FSVQ is defined as a mapping from $Rk \times S$ to a subset of a master codebook $MC = \{xi : i = 1, \ldots, N\}$. For each state si, the FSVQ encoder selects Nf codewords by means of the state function from the master codebook MC as the state codebook SCs. For each input vector x, the encoder decides the current state s and then searches the state codebook SCs to find its corresponding codeword. The codebook size of the state codebook is much smaller than that of the master codebook. Hence, the searching time can be reduced. A fast finite-state algorithm that reduces the computation time for vector quantizer design by exploiting FSVQ techniques shows that the fast finite-state algorithm can reserve the quality of encoding. For each state s, the state palette SPs is the subset of whole palette Pi, and the size of SPs is Nf. The Nf codewords in SPs are the closest codewords to s in the whole palette Pi−1. Thus, the first iteration of the CFSLBG algorithm is the same as that of the ordinary LBG algorithm, in which the full search algorithm is used to select a codeword for each training vector. At the following iteration, i.e. $i \geq 2$, the information in the previous iteration is used to determine the states of the training vectors. The CFSLBG algorithm is described in the following steps.

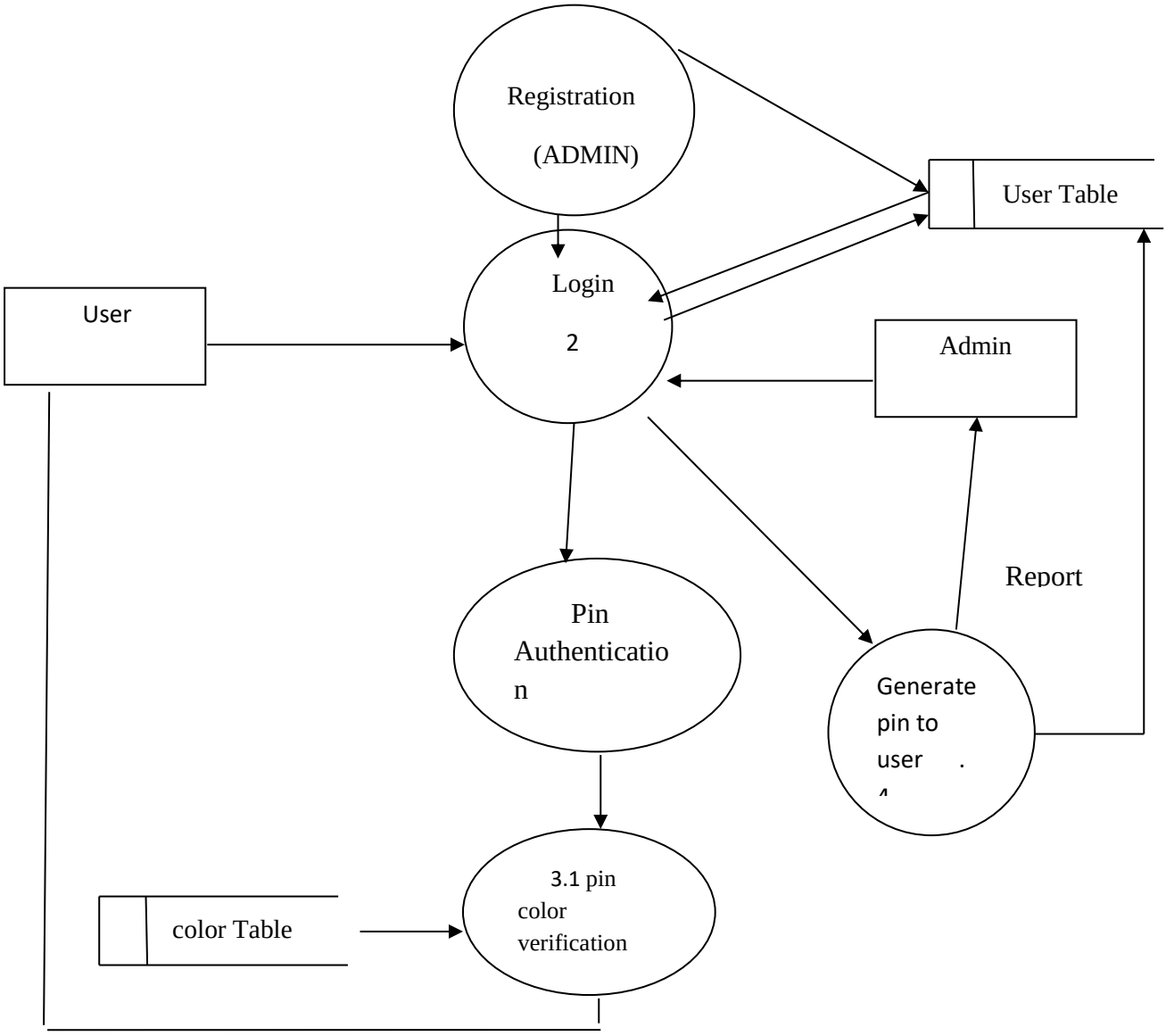
Step 1: Design an initial RGB color palette P0 and set DAVG0 ← ∞.
Step 2: For each training vector x, find the closest palette entry 0 xˆ by searching the whole color palette P0. Compute the average distortion DAVG1 .
Step 3: For each palette entry 0 xˆ in P0, generate a new entry 1 xˆ ← centroid(CS(ˆ)) 0 x and add 1 xˆ into P1. Set i ← 2.
Step 4: Set the state space S = Pi−1.
Step 5: For each state s in S, find the set of the Nf closest codewords in the whole color palette Pi−1 and define this set as the state palette SPs. For each training vector x, use the previous codeword -1 ˆi x as the state s. Find the closest palette entry ˆi x by searching the state palette SPs.
Step 6: Compute the average distortion DAVGi . If | DAVGi-1 − DAVGi | / DAVGi is smaller than ε, then stop.
Step 7: For each entry -1 ˆi x in Pi−1, generate a new entry ˆi x ← centroid(CS(ˆ)) i-1 x and add ˆi x into Pi. Set i ← i + 1 and go to step 4.
Note that the state palette size Nf is much smaller than the whole color palette size N. The Nf codewords for each state are found by an insertion sorting algorithm applied to the entire palette.

ENROLLMENT PROCESS : In Enrollment process user/admin fills their personal details like name, address, phone no, username and submit the user registration form. Automatically 4 digit pin will be generated and send to the corresponding user mail id. And user can change the pin also.

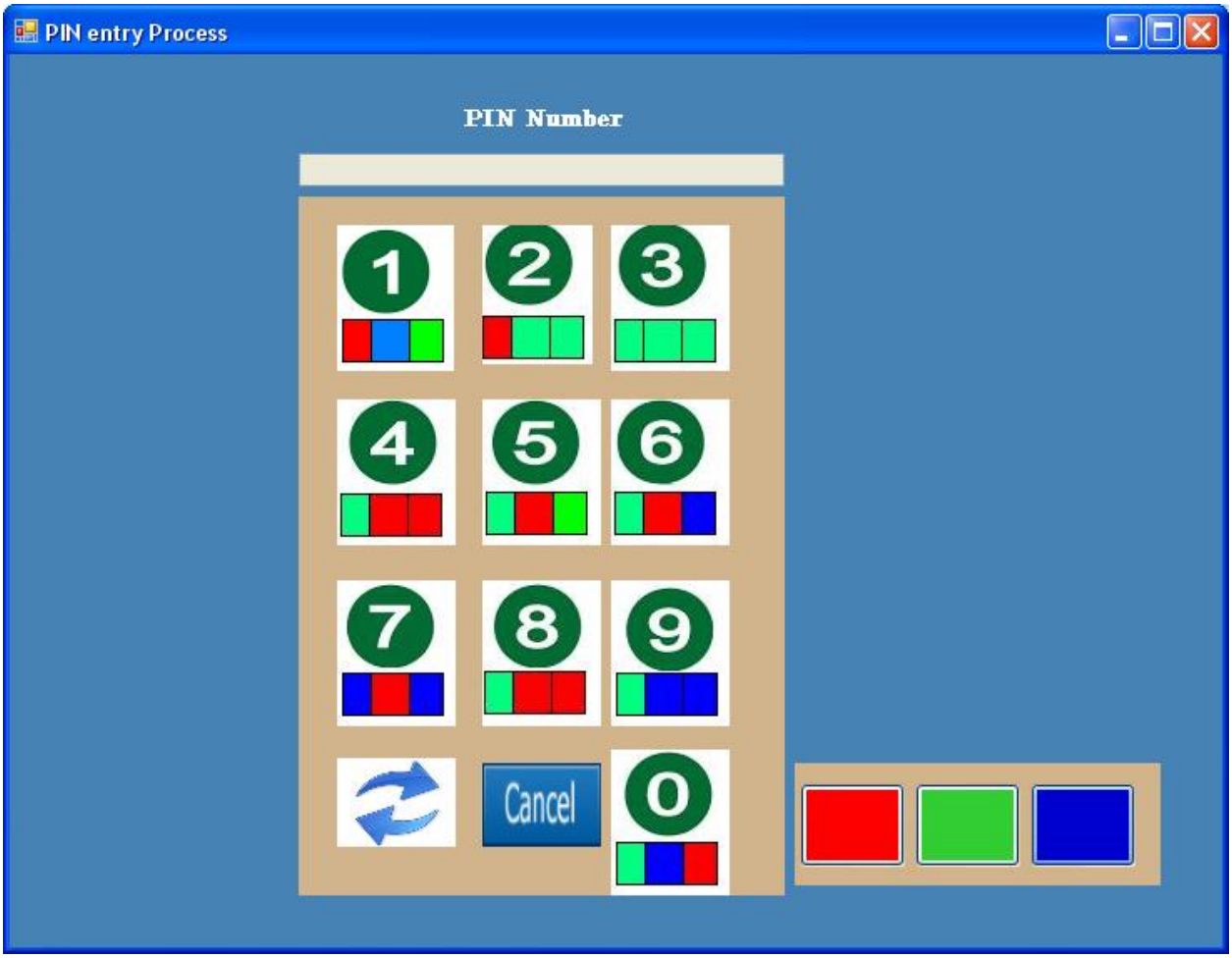
SPLIT AND MERGE SCHEME : This process collects all the colors from GUI after user enters it in the system. The colors are spilt in to four groups and each and every groups consist of three color combination of colors .every group have one user entered pin digit.

PIN IDENTIFICATION AND AUTHENTICATION PROCESS : Finally this process identifies four digit pin. It compares each group with another group and apply random color match scheme for identifying user pin. The color combinations are compared with each and every group and this pin is finally compared with the user's original pin.

TRANSACTION : This process includes the user account details entry process along with the bank ATM transactions. The transaction such as deposit and withdraw will be performed after the successful login. This feature will allow a customer to transfer money from any of their accounts to another account, and also this feature will allow customers to check money transfer information report and balance details.



Modules



IV. CONCLUSION

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding will be mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the system will be immediately blocked while attacks take place. In future all transaction will be processed in a secure manner and can find the intruders activity by getting all relevant details. In future it will capture all actions of the intruder by using screen capturing mechanism. It is concluded that the application will work well and satisfy the needs. It also acts as the sharing of files to the valuable resources.

REFERENCES

1. Y. W. Lim and S. U. Lee, "On the color image segmentation algorithm based on the thresholding and the fuzzy C-means techniques," Pattern Recognition, Vol. 23, 1990, pp. 935-952.
2. Z. Xiang, "Color image quantization by minimizing the maximum intercluster distance," ACM Transactions on Graphics, Vol. 16, 1997, pp. 260-276.
3. I. S. Hsieh and K. C. Fan, "An adaptive clustering algorithm for color quantization," Pattern Recognition Letters, Vol. 21, 2000, pp. 337-346.
4. E. Rendon, L. Salgado, J. M. Menendez, and N. Garcia, "Adaptive palette determination for color images based on Kohonen networks," in Proceedings of the International Conference on Image Processing (ICIP), Vol. 1, 1997, pp. 830-833.
5. J. S. Kirk, D. J. Chang, and J. M. Zurada, "A self-organizing map with dynamic architecture for efficient color quantization," in Proceedings of the International Joint Conference on Neural Networks (IJCNN), Vol. 3, 2001, pp. 2128-2132.
6. J. Foster, R. M. Gray, and M. O. Dunham, "Finite-state vector quantization of waveform coding," IEEE Transaction on Information Theory, Vol. IT-31, 1985, pp. 348- 359.
7. W. T. Chen, R. F. Chang, and J. S. Wang, "Image sequence coding using finite-state vector quantization," IEEE Transaction on Circuits Systems for Video Technology, Vol. 2, 1992, pp. 15-24.

8. M. O. Dunham and R. M. Gray, "An algorithm for the design of label-transition finite state vector quantizers," IEEE Transactions on Communications, Vol. COM-33, 1985.
9. R. Aravind and A. Gersho, "Low-rate image coding with finite-state vector quantization," in Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 1986, pp. 137-140.