Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 04, April -2019

Fingerprint Image Processing and Optimal Control in ATM Banking

Thomas Wetere Tulu[1], Tiande Guo[2], Mohamed Ibrahim[3]

[1]*University of Chinese Academy of Sciences, School of Mathematical Sciences, Beijing, China*
[2]*University of Chinese Academy of Sciences, School of Mathematical Sciences, Beijing, China*
[3]*University of Chinese Academy of Sciences, Academy of Mathematics and System Sciences*

Abstract —*Rapid development of banking industry has changed the way banking activities are dealt with. This is mainly because of using advanced technologies like ATM. Related to the booming of banking technology with ATM banking, there is a great security question as the current ATM banking system uses only numeric password as authentication which is not safe and secured. This study tries to propose the authentication by using both numeric based password (PIN) and fingerprint biometric authentication in the objective to make the industry safe and secured.*

Keywords-*Fingerprints, ATM, optimization problem, matching, image processing*

I. INTRODUCTION

Biometric provides automated method to identify a person based on physiological or behavioral characteristics. The unique features measured are face, fingerprints, hand geometry, handwriting, iris, retina, vein, and voice. Biometric technologies are playing vital role to provide highly secure identification and personal verification methods. As the level of security breaches and transaction fraud increases, the role of highly secure identification is becoming apparent. Every biometric method uses some aspect of an individual's physical or behavioral attributes as a means of authenticating the individual's identity. Today the most pervasive biometric in use is fingerprint, a physical biometric. Fingerprints have a unique pattern of ridges and furrows. One can find that the finger prints rarely use the full print for identification. This pattern is stored in a database either in a remote computer or in the device itself. When a person scans a print, this device compares the pattern generated by the print with one in the database to make a positive identification. There are various phases of fingerprint identification as image loading, image enhancement, normalization, thinning, minutia marking and minutia extraction.

Fingerprint image quality is a vital issue to measure the performance of Fingerprint identification system[1-5]. So quality assessment of fingerprint data leads to identify the fingerprints in a better way. The main purpose of such procedure is to enhance the image by improving the clarity of ridge structure or increasing the consistence of the ridge orientation. In noisy regions, it is difficult to define a common orientation of the ridges. The process of enhancing the image before the feature extraction is also called pre-processing. According to Hong, for identification purpose generally two methods are used. First is normalization; this is a method to improve the image quality by eliminating noise and correcting the deformations of the image intensity caused by non-uniform finger pressure during the image capture.

The idea of normalization consists of changing the intensity of each pixel. The normalization preserves the clarity and contrast of the ridges; however it is not able to connect broken ridges or improve the separation of the parallel ridges. The second is transformation. In particular, for detection of high or low frequencies. As the ridges have structure of repeated and parallel lines, it is possible to determine the frequency and the ridge orientation using transformation. Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. After the fingerprint ridge thinning, marking minutia points is relatively easy. In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending[4-10].

II. PROPOSED SYSTEM

As security is so critical in banking industry, there must be security strength. To increase the current less secured and unsafe system we propose the usage of ATM with both biometric fingerprint security system and numeric password authentication method which makes to meet the customers' needs that many of them have saving account and need to have access to their money during banking and non-banking hours. This method is more secured, reliable and very safe than the current system.

III. WHY BOTH FINGERPRINT AND NUMERIC PASSWORD (PIN)?

Existing ATM system only uses personal identification number as an authentication method. Though it is convenient it is weak in security as it can be easily accessed and easily violated by another causing great damage to the customer as well the bank. Besides, usage of only fingerprint authentication has a problem. If fingerprint information is leaked, all information recognized by computers can be copied and used. All the secrets entered by customers' fingerprint information come to of no use. Moreover, people of the world may have the same fingerprint reader results. That is, it is highly likely to be abused and information should be possible to be changed. Therefore, usage of ATM with fingerprint biometric authentication and personal identification number(pin) is proposed as it is very safe, reliable, inexpensive and accurate.

IV. IMPLEMENTATION

To minimize the current risk of ATM against attackers and to increase customer satisfaction as well profit a strong security method has to be used. In this point of view, this paper proposes the usage of both ATM with biometric fingerprint security system and numeric password authentication method with the following implementation process.

Step 1: Take all the bio data of the customer- This include full name, account type, birth date, fingerprint image for minutiae feature extraction, load the image to the ATM card and other important data of the customer.

Step 2: Identification and Verification steps: This step includes identification of the numeric password (PIN), the biometric data (fingerprint) and matching for authentication with the maximum possible trial times(3 times). If the card holder’s authentication steps are successful then transaction will automatically be carried out. The flow chart for this step is given below:

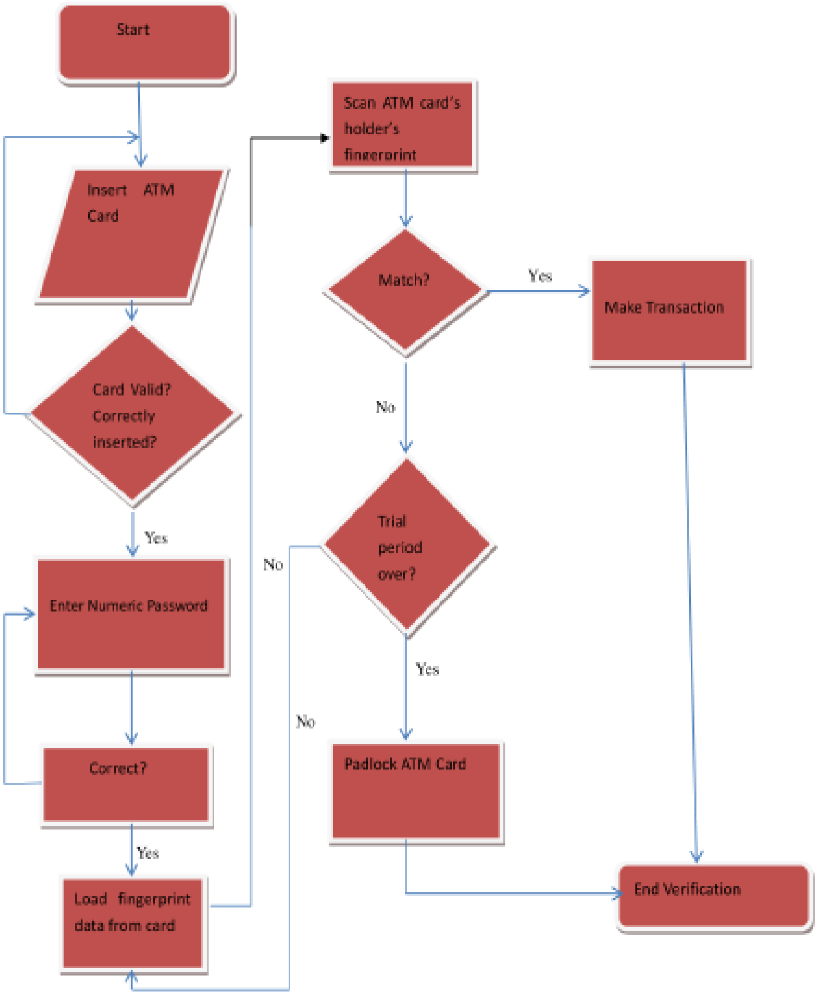

Figure 1: Flowchart for identification and matching process

V. FINGERPRINT RECOGNITION

Fingerprint recognition is a process which is used to compare the given input image with the template fingerprint image that is stored in the database. Fingerprint Recognition comprises of four steps. They are:

1. Image acquisition-which is done by the optical multi spectral sensor.
2. Image enhancement-used to adjust the contrast of the image and also to remove noise.

3. Fingerprint image segmentation- this is used to extract the region of interest, which is further used for feature extraction such as minutiae.
4. Matching-based on the extracted features, the verification of the given image is done with the image in the database and returns the result either as true or false.

VI. IMAGE ENHANCEMENT

This process comprises of two steps:

1. Histogram equalization: it is a normalization method to adjust the images intensity values, such that the contrast of the image is enhanced.
2. Gabor filters: these are used to further enhance the clarity of the image by detecting the edges, i.e., the ridges of the fingerprint. The Gabor filter capture the periodic nature of the fingerprint and its mathematical form is given by:

$$F(x,y;\theta,f) = \exp\left[\frac{-1}{2}\left(\frac{X_0^{\ 2}}{\delta_x^{\ 2}} + \frac{Y_0^{\ 2}}{\delta_y^{\ 2}}\right)\right] Cos(2\pi f X_\theta)$$

$$X_\theta = X\cos\theta + y\sin\theta$$

$$Y_\theta = -X\sin\theta + y\cos\theta$$

where f represents the ridge frequency.

VII. SEGMENTATION

Segmentation is executed for ensuring the focus is only on the foreground regions while the background regions while the background regions. In another words, Segmentation of the image is done to retrieve the region of interest from the image, which alone can be used further in the processing. This process is of three steps they are:

1. Binarization: The gray level enhanced image is converted to a binarized image with 0 as ridges and 1 as valleys.
2. Orientation field estimation: In this, the angle of orientation at each and every pixel is calculated using the x and y gradients of Sobel operator and the orientation field is calculated using the least mean square method implemented by Hong et al.
3. Region of interest extraction: The region of interest is extracted from the image using the morphological operators ’open’ and ’close’.

VIII. MATCHING

Matching of two fingerprints is done based on the features extracted from the fingerprint. In this proposed business model, we use minutiae based matching technique. Minutiae are the most important features of fingerprint; these include ridge bifurcations- ridge dividing into two and ridge terminations abrupt end of a ridge. Before the process of minutiae extraction, thinning of the segmented image is performed. Thinning is done, so that the ridges are only one pixel wide. After thinning, many spurious pixels may be formed, such as H-breaks and spikes. These spurs are removed using morphological operators.

A) Minutiae Extraction

Crossing number method is used to extract minutiae from the fingerprint image. The findings of (Bansal et al, 2007) showed that the minutiae are extracted by using a 3X3 window, which scans the local neighborhood of every pixel.

B). Minutiae based matching

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

The findings of (Bansal et al, 2007) showed that the CN value is computed as: CN = 0:5 $\sum_{i=1}^{8} P((i) - P(i+1)$

Where P(i) : pixel value in the neighborhood of P. After the CN value is computed based on its properties, we find the nature of the pixel. The findings of (Bansal et al, 2007) showed that CN properties are as follows:

CN	Property
0	Isolated point
1	Ridge ending point
2	CONTINUING RIDGE POINT
3	Bifurcation point
4	CROSSING POINT

C). Minutiae based matching

Each and every minutiae of the input image is compared to every minutia in the template image. In each case of input and template, reference points are selected. These reference points are used to convert the remaining minutiae set into polar co-ordinates. For both the input and template, the radial distance, the radial angle and the orientation angle of each minutia is found out.

Once calculated for both input and template, these will be compared and the matching score is found out. The matching score is given by:

$$\mathrm{MS}=\frac{MM}{Max(NI,NT)}$$

where, MS is matching score, MM is the matching minutiae, NI is the number of minutiae in the input image and NT is the number of minutiae in the template image. If the matching score is 1 then the fingerprint is matched exactly and 0 if they mismatch. Therefore, the fingerprint recognition is done in this way.

VIIII. OPTIMIZATION AND OPTIMAL CONTROL

As we are introducing the usage (application) of both fingerprint and numeric password method things must be very affordable in implementing our new system. Hence we built a new model and carry out optimal control strategy to minimize cost related to our new system and to control bank related frauds. Cyber-crime is becoming one of the biggest challenges in banking industry. It is a growing threat for businesses around the world. This is mainly because the tactics used to steal information and money are becoming more sophisticated and involve a high level of technical expertise now a days[11]. In this study a new mathematical (optimization) model with an intervention that solves this problem is given. Briefly, the population is divided into four sub populations: the susceptible individuals (**E**) may become cyber attacker (**U**) after contact with those who are engaged in the attack capable of making others including police officers take part before they give up (**R**) because of different reasons or taken to prison (after they got final decision by court) for cyber attacking and related crimes (**D**). The model with the intervention **V**(usage of fingerprint biometry in banking industry) and **q** that describes our problem is given below: The classical EURD model with the intervention V and q is given below:

$$\frac{dE}{dt}=\gamma_1 R-\frac{\beta_1(1-\beta)EU}{N}-\gamma E$$

$$\frac{dU}{dt}=\frac{\beta_1(1-\beta)EU}{N}-\alpha_1\beta U-\alpha_2(1-\beta)U-\delta_1 U-\delta_2 U$$

$$\frac{dR}{dt}=\alpha_1\beta U+\alpha_2(1-\beta)U+\gamma E-\gamma_1 R$$

$$\frac{dD}{dt}=\delta_1 U+\delta_2 U$$

with parameters as defined below:

Parameter	Description
N	Total number of population
β_1	Rate of applying q(second intervention)
γ_1	Rate of taking part again in crime after punishment
γ	Rate of using fingerprint biometry(first intervention)
α_i	Rate of giving or not giving up because of second intervention
δ_i	Rate of taking action in controlling cyber attackers

The objective functional focuses on minimizing the cost of the intervention V and q on [0, T] and minimizing the attack on banking industry. Here $\gamma = V$ and $\beta = q$. Define the objective functional as:

Minimize $Z(v,q) = \int_0^T [U(t) + \frac{A}{2}v^2(t) + \frac{B}{2}q^2(t)]dt$

Where $A \geq 0$ *and* $B \geq 0$ are the weight on the cost of V and q respectively and Tis the duration of the Program. Moreover, v(t) and q(t) are also measurable functions that : $0 \leq u(t) \leq 1$,$0 \leq q(t) \leq 1$, $t \in [0,T]$.
Here we introduce a control U (t) representing the fraction of people being registered to use our proposed new method.

Minimize $Z(v,q) = \int_0^T [U(t) + \frac{A}{2}v^2(t) + \frac{B}{2}q^2(t)]dt$

Subject to:

$$\begin{cases} \frac{dE}{dt} = \gamma_1 R - \frac{\beta_1(1-\beta)EU}{N} - \gamma E \\ \frac{dU}{dt} = \frac{\beta_1(1-\beta)EU}{N} - \alpha_1 \beta U - \alpha_2(1-\beta)U - \delta_1 U - \delta_2 U \\ \frac{dR}{dt} = \alpha_1 \beta U + \alpha_2(1-\beta)U + \gamma E - \gamma_1 R \\ \frac{dD}{dt} = \delta_1 U + \delta_2 U \end{cases}$$

A). EXISTENCE AND UNIQUENESS OF THE CONTROL

The existence and uniqueness of the optimal control pair for the state system above can be obtained by using a result by Fleming and Rishel. Suppose the minimal objective functional Optimization problem:

$$J(v,q) = \int_0^T [U(t) + \frac{A}{2}v^2(t) + \frac{B}{2}q^2(t)]dt$$

Subject to:

$$\begin{cases} \frac{dE}{dt} = \gamma_1 R - \frac{\beta_1(1-\beta)EU}{N} - \gamma E \\ \frac{dU}{dt} = \frac{\beta_1(1-\beta)EU}{N} - \alpha_1 \beta U - \alpha_2(1-\beta)U - \delta_1 U - \delta_2 U \\ \frac{dR}{dt} = \alpha_1 \beta U + \alpha_2(1-\beta)U + \gamma E - \gamma_1 R \\ \frac{dD}{dt} = \delta_1 U + \delta_2 U \end{cases}$$

with the initial conditions Eo;Uo;Ro and Do. Then, there exists an optimal control J^{*}= (v; q) subject to the system with the initial conditions. To prove the existence of an optimal control, the following conditions must be satisfied:
(a) The set of controls and corresponding state variables are non-negative and non-empty;
(b)The control set (v, q) is convex and closed;
(c)The right hand side of the state system is bounded by a linear function in the state and control variables;
(d)The integrand of the objective functional is convex on (v, q);

(e) The integrand of the objective functional is bounded below by

$$b_1 \,[\,(\frac{v^2}{2})^2 + (\frac{q^2}{2})^2\,]^2 - b_2 \text{ where } b_{1,}\ b2 \text{ and } \beta > 1\ .$$

An existence result by Lukes [Theorem 9.2.1 page 182] was used to give the existence of solutions of ordinary differential equations of our system with bounded coefficients, which gives condition 1. The control set is convex and closed by definition. Since the state system is bilinear in v, the right hand side of the system satisfies condition 3, using the boundedness of the solution. Finally, the integrand in the objective functional:

$[U(t)+\frac{A}{2}V^2(t)+\frac{B}{2}q^2(t)]$ is clearly convex on (v,q). Finally there exists b_1, b_2 and $\beta > 1$ satisfying

$[U(t)+\frac{A}{2}V^2(t)+\frac{B}{2}q^2(t)] \geq b_1 (\frac{v^2}{2})^2 + (\frac{q^2}{2})^2\,]^2 - b_2$ because the state variables are bounded. Therefore, there exists a unique optimal control pair. To find the optimal solution define the Hamiltonian as:

$$H = [U(t)+\frac{A}{2}V^2(t)+\frac{B}{2}q^2(t)] + \lambda_E(\ \gamma_1 R - \frac{\beta_1(1-\beta)EU}{N} - \gamma E\ ) +$$
$$\lambda_U(\frac{\beta_1(1-\beta)EU}{N} - \alpha_1\beta U - \alpha_2(1-\beta)U - \delta_1 U - \delta_2 U) +$$
$$\lambda_R(\alpha_1\beta U + \alpha_2(1-\beta)U + \gamma E - \gamma_1 R) + \lambda_D(\delta_1 U + \delta_2 U)$$

where

$\lambda_E, \lambda_{U,}\lambda_R, \lambda_D$ are the adjoint variables. Moreover, the adjoint equations are defined as follow:

$$\lambda'_E = -\frac{\partial H}{\partial E} = \lambda_E(\frac{\beta_1(1-\beta)U}{N} + \gamma) - \lambda_U(\frac{\beta_1(1-\beta)U}{N} + \gamma) + \lambda_R(\gamma)$$
$$\lambda'_U = -\frac{\partial H}{\partial U} = -1 + \lambda_E(\frac{\beta_1(1-\beta)E}{N} - \lambda_U(\frac{\beta_1(1-\beta)E}{N} - \alpha_1\beta - \alpha_2(1-\beta) - \delta_1 - \delta_2) - \lambda_R(\alpha_1\beta + M)$$
$$\lambda'_R = -\frac{\partial H}{\partial R} = \lambda_R\gamma_1$$
$$\lambda'_D = -\frac{\partial H}{\partial D} = 0$$

Where M= $\alpha_2(1-\beta) + \delta_1 + \delta_2) - \lambda_d(\delta_1 + \delta_2)$

B. Pontryagin's Maximum principle

The necessary first order conditions to find the optimal control were developed by Pontryagin and his co-workers. This result is considered as one of the most important results of Mathematics in the 20th century. Pontryagin introduced the idea of adjoint functions to append the differential equation to the objective functional. Adjoint functions have a similar purpose as Lagrange multipliers in multivariate calculus, which append constraints to the function of several variables to be maximized or minimized[12]. Using Pontryagin's Maximum principle and Solving the optimality conditions

$$\frac{\partial H}{\partial v} = 0 \text{ AND } \frac{\partial H}{\partial q} = 0$$

$$V^* = v = \frac{\lambda_E E - \lambda_R E}{A}$$

$$q^* = q = \frac{\lambda_u U - \lambda_R U}{B}$$

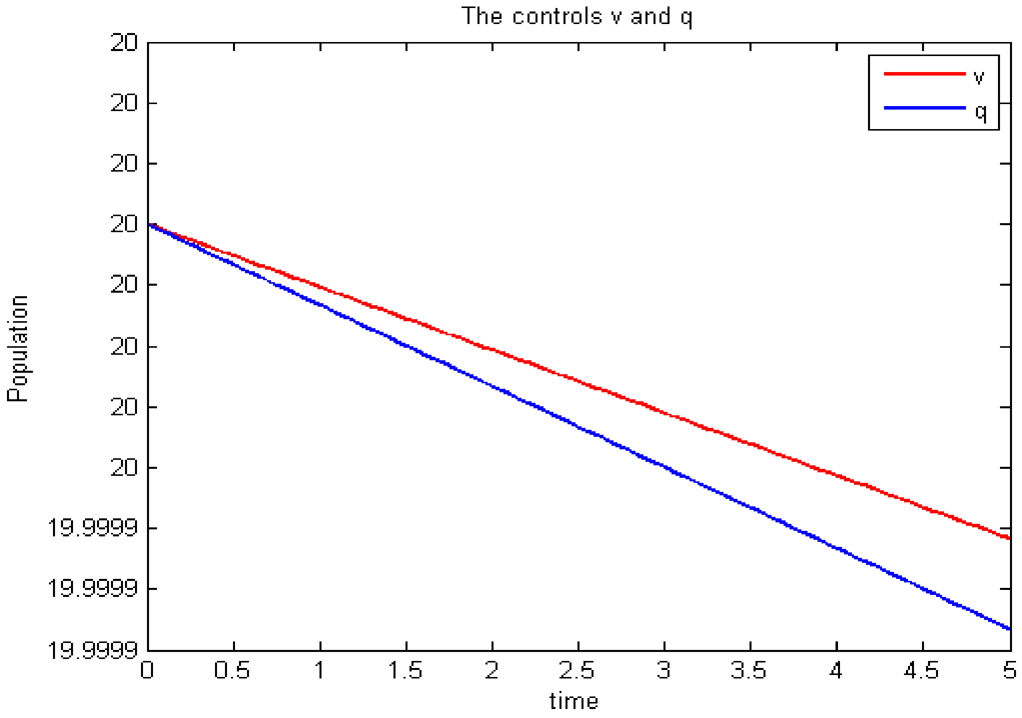

Figure 5.1 The controls V and q.

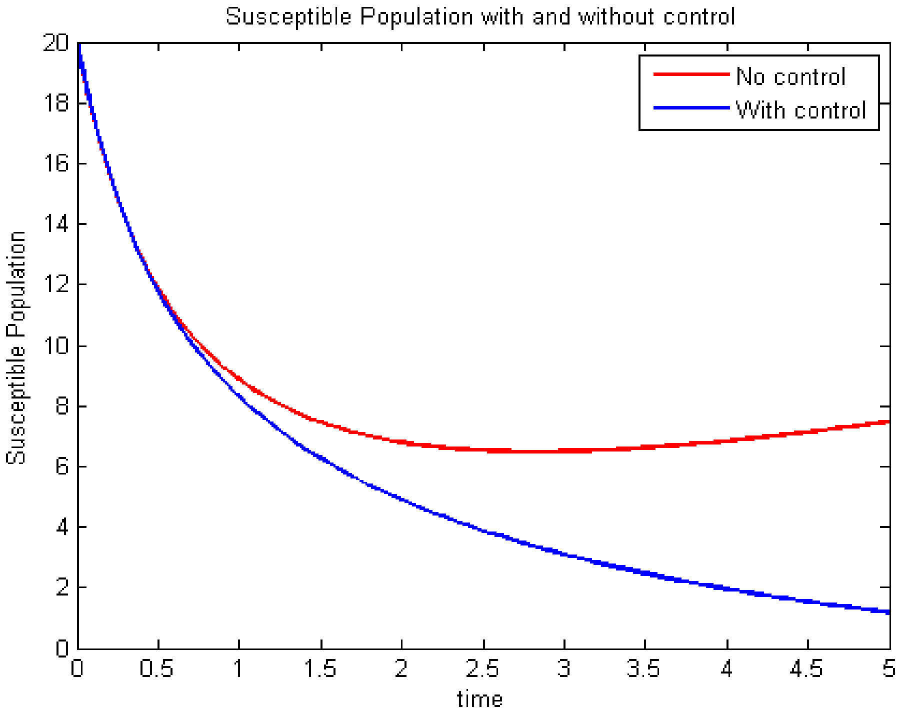

Figure 5.2 The number of susceptible population with and without control.8

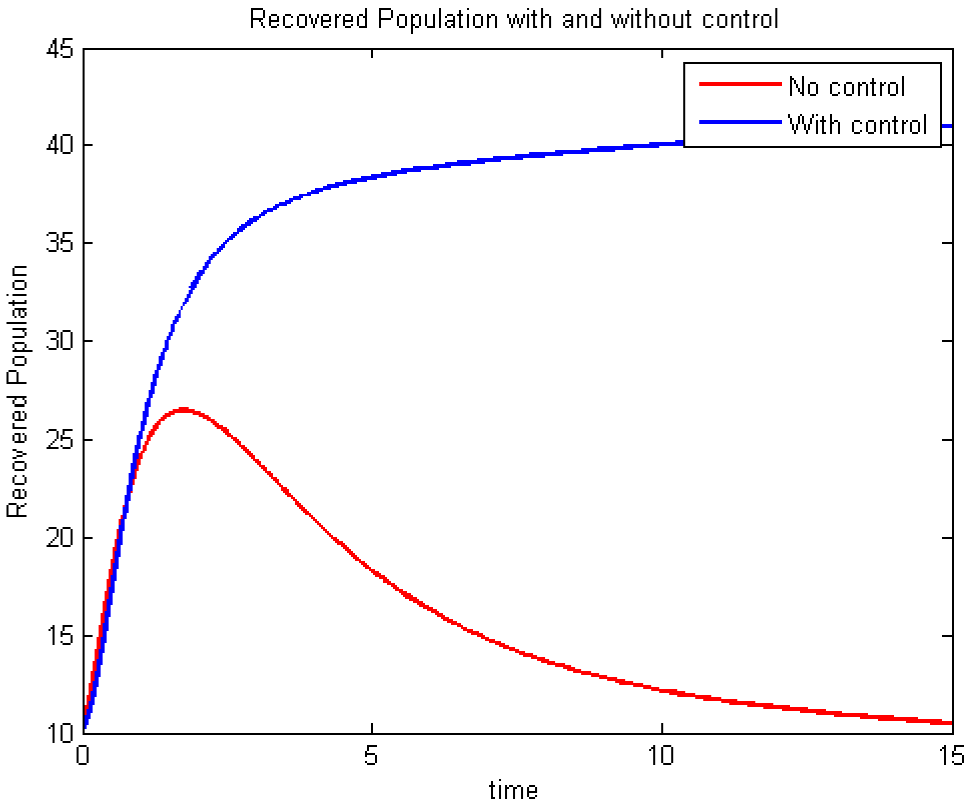

Figure 5.3 The population of R individuals with and without the first intervention, V .

X. CONCLUSION

In this article, we have proposed a new system that uses fingerprint image in ATM banking to overcome the current challenging security issue in banking industry. Besides, as Optimal control method has proven to be a successful tool in understanding ways to curtail optimization problems by devising the optimal intervention strategies, new model with an intervention is built and intensively analyzed. Our result show that usage of intervention strategies like fingerprint image in banking industry has a great role in overcoming the current frauds related to banking industry. However, if they are not carried out at the right time and in the right amount, the problem elimination and securing optimality will remain a very difficult task. So the authentication using both fingerprint and numeric password (PIN) enhances security, fast, easy to use, accurate, reliable and effective.

Finally, we strongly claim that the new system proposed will definitely reduce the rate of fraudulent activities on ATM machines when fully carried out.

XI. ACKNOWLEDGMENTS

This research was supported by CAS-TWAS Presidents PhD Fellowship Programme. Besides, the authors declare no conflicts of interest.

XII. REFERENCES

[1] RouquetP,etal.Wild animal mortality monitoring and human Ebola outbreaks, Gabon and Republic of Congo,2001 2003,Emerging infectious disease 2005 ;11:283-290

[2] Selvaraju, N. and Sekar, G., (2010), A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm, International Journal of Computer Applications (0975 U 8887) Volume 3 U No.6.

[3] Feng, J.,(2008),Combining minutiae descriptors for fingerprint matching, Pattern Recognition 41, 342 U 352.

[4] Jain, A.K., Prabhakar, S., Hong, L., (1999), A multichannel approach to fingerprint classification, IEEE Trans. Pattern Anal. Mach. Intell. 21 (4),348U359.

[5] FVC2002, Second international fingerprint verification competition

[6] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S.,(2009), Handbook of Fingerprint Recognition (2nd Edition). Springer.

[7] Jiang, X. and Yau, W. Y.,(2000),Fingerprint Minutiae Matching Based on the Local and Global Structures, In Proc. of ICPR, volume 2, pages 6038U6041, Barcelona, Spain.

[8] Delac, K. and Grgic, M.,(2004), A Survey of Biometric Recognition Methods, 46th International Symposium Electronics in Marine, ELMAR.

[9] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked SocietyŠ, Kluwer Academic Publications, ISBN 978-0-7923-8345-1.

[10] Bansal, R., Sehgal, P. and Bedi, P.,(2011), Minutiae extraction from fingerprint images- a review, IJCSI, Vol. 8, Issue 5.

[11] https://www.johnsonbank.com/Resources/Articles/2018-07-25-Cyber-and-financial-fraudthreats.

[12] M. Brokate. Pontryagin’s principle for control problems in age-dependent population dynamics. Journal of Mathematical Biology,1985, 23:75–101