Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

ATM FRAUD DETECTION USING DEEP LEARNING

SHAIK DILSHATH,
Department of Computer Science Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
Mail: dilshath08@gmail.com

SANJANA ATHMARAMAN,
Department of Computer
Science Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
Mail: sanjuwilma@gmail.com

PRASANNA LAKSHMI,
Department of Computer Science Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
Mail:prasanna.vlr98@gmail.com

Prof. SIVA SHANMUAGM G,
Department of Computer Science Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
Mail: sivashanmugam.g@vit.ac.in

Abstract

An Automatic Teller Machine is an automated electronic bank machine that helps the customer with monetary transitions without any help of bank officials or intermediaries. Customers can access cash transitions and details through the machine, which is why ATMs carry large amounts of cash, thus prone to attacks. Physical attacks can be attempted in the ATM, by means of thermal or mechanical ways with the goal to break or harm the ATM machine so as to rob the machine by stealing the cash inside it. The techniques which are generally used are explosive attacks, ram-raids and cutting. The money inside the ATM can be stolen when it is being repaired or when the money is being stored. Staff is either held up as they are conveying cash to or from an ATM or when the ATM safe is open and money tapes supplanted. There is an assortment of physical and mechanical components that can restrain assaults to the safe.Thus, in this project, we tried to predict if the attack is happening and thus send the message to the local police station. This project helps in predicting the attack before it has already occurred.

Keywords: Camera, internet connection, CNN, Fast RCNN, FaceNet, haar cascades.

1. Introduction

In the present technically advanced society, various autonomous systems have gained the rapid population. The new technologies for banking has modified the banking rules and their exchanges. One such advancement that has been done in the present days is invention of ATMs (Automated Teller Machines**.** With an ATM, a client can lead various financial exercises, for example, money moves, cash withdrawal, taking care of power and telephone tabs past available time, and record

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

requests. More or less, an ATM gives clients a helpful and snappy approach to get to their records and to lead money related exchanges. A Personal Identification Number (PIN) or secret key is a significant component of the ATM security framework. PIN or secret key is normally used to ensure and makes sure about the monetary data of clients from unapproved get to. However, the crime related to the financial organizations have been increased with the increase in the spread of automation and smart devices. These crimes are gradually increased from 1999 to 2003 and decreased a bit in 2004 and then drastically increased from the year 2005. Thus, robberies have been dramatically increased from the last 12 years. Thus, we have proposed a solution for this problem using deep learning algorithms. This project, warns the police officials prior to the crime or theft happening inside the ATM. Thus, instead of reacting late to the robbery, this model helps to react early and take necessary actions if possible.

Related work

In order to protect ATM robberies, many solutions and techniques have been developed and implemented over many years by many people. Many such solutions have been implemented to trace the attacks happening in ATM using many deep learning and machine learning algorithms. The algorithms used in machine learning to detect the robberies are Multiple Instance Learning(MIL), Support Vector Machines(SVM), Random Forest Classifications. Deep learning algorithms like Convolution Neural Networks(CNN) are also used in some of the existing systems. Not only software, but few systems also used IOT to detect the attack happening inside the ATM. These IOT techniques use sensors like gas detection sensor(to detect any gas in the ATM), thermal sensors(to detect the temperature), sound sensors(to detect any find of sound produced inside the ATM). But if the hardware part is used, the machine has to be attached with an external source(which has sensors in it). But attaching an external source to the machine is not the efficient way to solve the problem and the major drawback of using the hardware part is that this increases the cost of the system. Hence, we have trained our system using machine learning and deep learning algorithms which increased the accuracy of the results.

Existing systems:

Ink and dye stain technology: A passive solution for gas and commercial explosive for Cash Protection Devices. This technique is compatible with all ATM cash cassettes. It is retrofitted with ease. There are no sensors, no triggers, no detection system required in this method. A DNA marker is be added to the ink and it supports paper and polymer notes.
Automated Teller Machines (ATMs) focuses on arrangements which give numerous purposes to insurance against any sort of robbery from ATM and ensuring its establishments. The venture aids to giving constant checking of framework. This

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

uses different types of sensors with the help of which they will recognize the issue and will give the arrangement right away. The technique utilized to peruse the card ceaselessly. At that point the outcome is quickly refreshed to administrator and the message is sent to the closest higher officials headquarters.

IOT based systems[1] that has been proposed has many levels of protecting the machine against physical as well as electronic attacks. The system that has been developed is on the Arduino for securing the inputs by using many sensors like GSM modem[9], vibration sensors, temperature sensors, sound sensors. This system works on a simple formula which is if the sensor crosses its threshold level, then the alarm sound comes into play and this alerts the higher officials indicating that there is something wrong happening inside the ATM. But this proposed system is not accurate as it doesn't work efficiently on temporal values and also has the risk of false alarms. The other system that is based on IOT[7][8] is with the use of image processing with IOT. Here, the primary step is to identify the person and obtain the outline of the person. Once the outline is extracted, the motion of the person is recorded using MHI, which helps in obtaining the motion of the image. Now, the features are extracted from MHI using Hu moment function. Then the outline is made more accurate using PCA(principal component analysis). Here, this obtained a 72% accuracy on single normal, 69.89% for multiple normal. But this accuracy obtained is very low as this system is dealt with security.

Proposed system:

In this project, we have proposed a way to provide the security to the ATM by using deep learning algorithms. Proposed "Physical Security of ATM" ought to encourage the efficient usage of cameras inside the ATM in order to reduce the attacks on the ATM machine. The cameras detect the person who is trying to cover his/her face with the help of helmet or sunglasses and warns the user to remove them. The cameras also identify any specific weapon carried by the user inside the ATM machine. And if the person is trying to attack the machine, then the system identifies the motion of the user and if there is some attack happening, then the alarm gets activated. In this proposed system, deep learning algorithms like CNN and LSTM[2][3][4] are used to make the system more accurate. In addition to these algorithms, the Facenet algorithm which is used in detecting the face gives accurate results and doesn't require more time to train the dataset. RCNN and haarcascases used help in detecting and identifying the objects carried by the person, are also accurate in producing the results. Thus the proposed system, is accurate and gives higher accuracy results as it has used advanced algorithms to train the model.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

Methods

In this paper, we have used various deep learning algorithms which helps in detecting the face of the person, the objects he is carrying and the motion of the person once he enters the ATM.

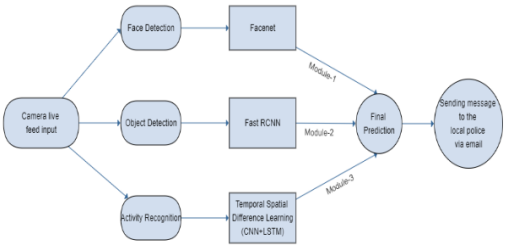

Fig 1: architectural diagram

This figure shows the proposed work implemented to secure the ATM when an unauthorized person enters and tries to attack the machine. This uses Facenet, Fast RCNN, LSTM algorithms to detect the person, identify the objects he is carrying, track the motion of the person who entered the ATM and notify to the nearest local police station if there is some attack happening. This project mainly consists of three modules.

Module-1: To identify the user and detect if he is wearing a helmet or sunglasses. In this module, if the person is trying to cover his/her face, then the system warns the user by displaying a message to remove the sunglasses and the helmet. This is done using FaceNet and haar cascade. This module has two parts.

i. To apply the face detection[5] so as to detect the presence and location of the face in an image but doesn't identify it. This is called the training phase.
ii. To extract the 128D feature vectors which is called embedding, that quantify each face in an image. This is the testing phase.

The architecture diagram used in this module is as follows:

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

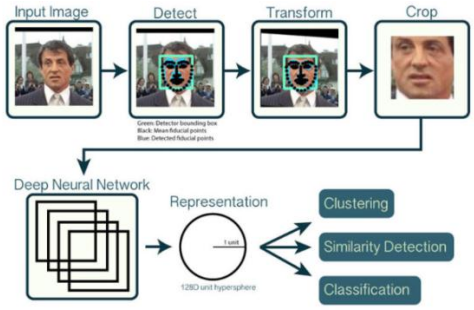

Fig 2.

In this module, when the face is detected, the input image is transformed, and the unwanted pixels are removed from the image. This phase is called pre-processing. After pre-processing, embedding of the image is done. Here, it represents the face in a multi-dimensional space where the distance corresponds to the measure of face similarity. The final step is classification which uses information given by the embedding process to separate distinct faces.

Module-2: Weapon, helmet, and sunglasses detection. Here, in this module, if a person is carrying any kind of weapon, then the system sends a message stating that the user is carrying weapons with him. This is done using Fast RCNN and haar cascade.

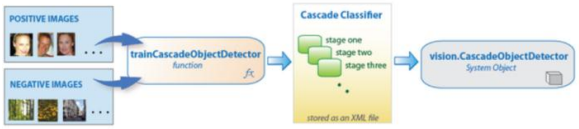

Fig 3.

The algorithm used in this module is haar cascade. This is a machine learning algorithm and helps in detecting the objects. In the first step of haar feature extraction. In this, the calculation thinks about the adjoining rectangular locales of a specific area in a discovery window, summarizes the pixel forces an incentive in those districts and computes the distinction between these entireties. Adaboost helps in calculating the most important features that contributes the maximum to the correct output. Thus, once the classifier is applied, the objects can be detected after the training phase.

Module-3: The person's activity is traced in this module and if the person is trying to attack the machine, then the alarm gets activated. This is done using LSTM and CNN algorithm.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

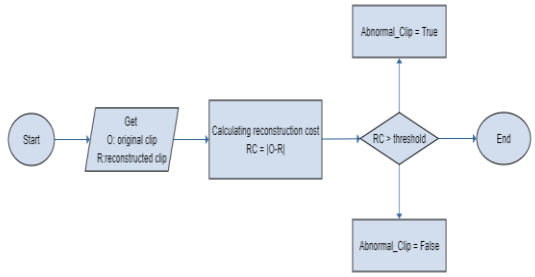

Fig 4: flow chart

In this module, CNN uses a mathematical operation called convolution to identity and extract only the most relevant pixels. CNN divides the image pixels into small matrix and computes the mathematical operation using filters to extract only the relevant pixels and finally classify the object in the image. Now once the objects are classified, we use LSTM algorithm for motion classification.

I. Experimental results and discussions:

In this project, the dataset is used to train the algorithms used and then it is tested. Once the algorithm is implemented, the sample is tested, and the respective results are obtained. The system starts scanning the person as soon as he enters and helps in detecting the face of the person.

Fig 5.

Once the face of the person who entered the ATM is detected, the camera then tries to identify if there is some object present. This object is basically a helmet or sunglasses. If these objects are present, the system that is trained using haar

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

cascade algorithm will identify these objects and then test with the dataset that is already loaded. If this matches with the dataset, then the warning message will be popped on the screen asking the person to remove the glasses and helmet. This algorithm doesn't send any warning message if the person wears normal glasses (as the normal glasses doesn't cover the face of the person).

Fig 6.

Now, if the person carries some weapon like gun, hammer, screwdriver, or a knife so as to attack the machine, then the weapon detection code gets activated. Once the weapon is identified, the warning message is popped and the video of the ATM which the camera is capturing will be informed to the authorities. If the person tries to attack the machine, using the motion detection code, the alarm starts ringing and message will be sent to the police.

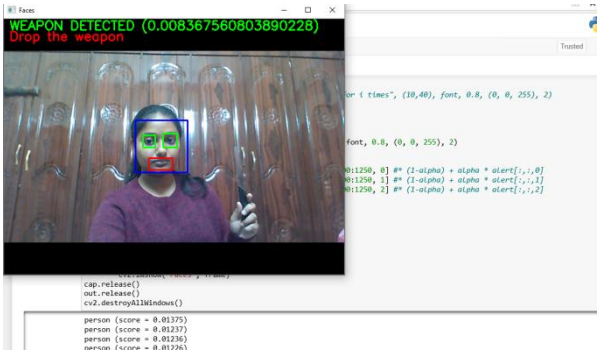

Fig 7.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

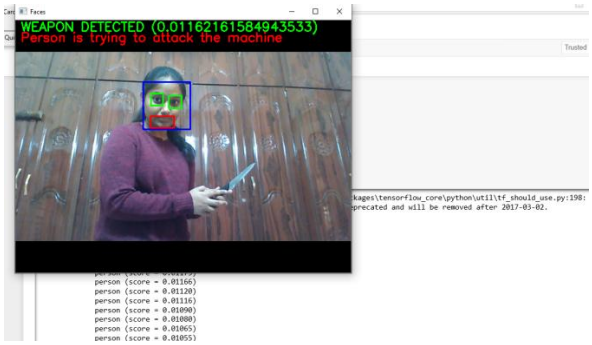

Fig 8.

Conclusion

In this project, we discussed different types of risks that can happen inside the machine. ATM owners should ensure to follow ATM best practices of rapid development of banking technology. The deep learning model that we have proposed provides the highest accuracy of detecting any wrong intensions of the customers towards the ATM machine and the money in it. It successfully identifies and gives an alert/warning messages if a person's face is hidden by sunglasses or caps, if a person is carrying any weapon and if a person is standing in an abnormal position that creates an idea of suspicion. Based upon these messages, necessary actions could be taken immediately to avoid further big problems in the future. The proposed controls should be validated by implementing them on the ATM and then performing a penetration test. This should be done in different geographical regions to ensure the controls work in all regions of the world. Thus, with the help of deep learning algorithms, we have developed a model which warns and alerts the police before some theft or robbery takes place. This proposed algorithm is hence useful for all the ATMs which have undergone severe loss due to the theft.

Future scope

In this world full of highly secured technologies, ATM has been one of the most vulnerable places for the robbers and thieves to get the money directly or to trace other's card information and use that information to get the money indirectly by covering their faces.

This could be avoided with the help of deep learning algorithms for human and object detection. This could be the stepped stone of a big revolution of a new system that enables us to deposit, withdraw and do various other operations in a safer and more secured manner without having any vulnerabilities.

Tianjin DaxueXuebao (ZiranKexueyuGongchengJishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:54 Issue:11:2021
DOI 10.17605/OSF.IO/M3YTH

References

1. Jacintha. V, J. Nagarajan, K. Thanga, " An IOT Based Surveillance System," IEEE International Conrefenre on Computational Intelligence and Computing Research, Chennai, India 2017

2. H. Gammulle, S. Denman, S. Sridharan, C. Fookes, "Two Stream LSTM : A Deep Fusion Framework for Human Action Recognition." IEEE Winter Conference on Applications of Computer Vision, 2017, pp. 177-186.

3. S. Arif , J. Wang, Tehseen Ul H and Z. Fei "3D-CNN-Based Fused Feature Maps with LSTM Applied to Action Recognition" Future Internet, 2019.

4. A. Ullah, J. Ahmad, Khan M, Muhhamad S "Action Recognition in Video Sequences using Deep Bi-Directional LSTM With CNN Features" Digital Object Identifier 10.1109/ACCESS.2017.2778011

5. A. Ullah, J. Ahmad, Khan M, Muhhamad S "Action Recognition in Video Sequences using Deep Bi-Directional LSTM With CNN Features" Digital Object Identifier 10.1109/ACCESS.2017.2778011

6. W. Sultani, C. Chen, M. Shah, "Real-world Anomaly Detection in Surveillance Videos", IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018

7. C. Rajmohan, M. Raghavi, E. Malavika, "ATM Theft Detection And Prevention Using Advanced IOT Techniques".

8. Jamuna Ranii S, Glory Beula J, Jeba Johnsly J, Jacintha V M.E, "An Extensive Resolution Of ATM Security Systems," third international conference on science technology engineering and management, 2017.

9. Bharati M Nelligani, N V Uma Reddy, Nithin Awasti, "Smart ATM Security System Using FPR, GSM, GPS."