IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Multi-Factor Secure Atm Access With Face Recognition Using Deep Learning

[1]Dr.S.Subashini, [2]S.A.Nanthitha Sri, [3]S.Ponsree, [4]R.R.Riduvarshini

[1]Associate Professor Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, Tamil Nadu, India.

[2,3,4]Final Year Students, Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, Tamil Nadu, India.

Abstract: Automatic Teller Machine (ATM) is widely accessible for users and procedure the ability to carry-out financial transactions and Banking functions in continuous time basis at any time. It made banking transactions effortless for customers current ATM's have access card and pin authentication for unique information. This explains ATMs to lot of financial theft like card theft, pin theft and stealing account holder information. It will make the multilevel high- end security to find the authorized user in the ATM machine and make secured and more safety for transaction. OpenCV library to analyze the person authorized identification by capturing the human face initially it begins with the entering the pin number if entered pin is correct then the process continues with the face recognition. If the entered pin is incorrect then it sends OTP on the registered Outlook mail. Then, if the entered OTP is correct the process continues or otherwise the transaction is declined. If the person is authorized it keeps continuing if the person is unauthorized, it sends alert mail and SMS to the registered user using the fast2sms messaging platform. It will forward the persons image which was taken at the time of withdrawal in the ATM to the mail registered with the user itself after the completion of the transaction.

Index Terms **-** ATM Security, PIN Authentication, Face Recognition, OpenCV, OTP, User Authentication, Real-Time Alerts.

I. INTRODUCTION

ATMs have really revolutionized the landscape of banking and personal finance since it was introduced way back in the late 20th century. Essentially, it is an electronic device allowing one to make many kinds of financial transactions without human intervention. Primarily, ATMs allow one to withdraw cash and check account balances; deposit money into his/her account and transfer funds between accounts. This has changed the game of managing finances. The first ATM was installed in 1967 at Barclays Bank in Enfield, London. Since its invention, the evolution of ATMs has been remarkable. One significant advantage of ATMs is their accessibility. They work on an around the clock system where they enable users to perform their activities even after the close of the banking hours. This is highly valued especially among people with very strict schedules of work or people living in remote settings with access to the bank services that are minimal. Digitalization makes fraud sophisticated. The banks have incorporated other security mechanisms to safeguard money belonging to the account holder such as encryption technology, anti-skimming devices, and multi-factor authentication processes. Users, therefore are also supposed to be on the lookout and, for example, cover the keypad while keying their PIN and to be fully aware of who is around when using an ATM. More tangibly, beyond this, ATMs have furthered the convenience of individuals to open doors; they have also propelled efficiency in financial institutions. By freeing the bank tellers from usual tasks, banks can make their resources more accurately aligned with customer service and more complex financial products. The actual outcome of this shift has been to decrease operational costs while delivering better services. ATMs transformed the banking

sector with regards to 24/7 access to services that entail more than just money withdrawals and balance checks. Instead, it has expanded the services to include complex deposit transactions and cardless ones. With multi-language capabilities and biometric authentication features, ATMs increase accessibility.

II. Deep Learning

Deep learning, a subset of machine learning, involves using neural networks with multiple layers to model complex patterns in data. Inspired by the structure of the human brain, these networks, often called deep neural networks, can automatically learn hierarchical features from large datasets, making them highly effective for tasks like image and speech recognition, natural language processing, and predictive analytics. Each layer in a deep neural network extracts progressively more abstract features from the data, enabling the model to achieve impressive accuracy and generalize to new examples. Key to deep learning's recent success are advances in computational power, large datasets, and techniques such as convolutional neural networks (CNNs) for images and recurrent neural networks (RNNs) for sequential data. Deep learning has transformed fields from healthcare and autonomous driving to entertainment, offering unprecedented capabilities in understanding and interacting with complex data.

2.1 Existing system

In existing system, RFID card is being used as ATM card, IR sensor is utilized to sense the existence of cardholders and Fan and Light is turned ON, if someone tampers with the ATM then an SMS is sent to the two main stations through GSM, biometrics such as finger print and eye ball authentication are prone for easy spoofing and SVM classification is used for face recognition.

2.1.1 Support Vector Machine

Support Vector Machines (SVMs) are supervised learning algorithms used for classification and regression tasks, particularly effective in high-dimensional spaces. The key objective of SVMs is to find a hyperplane that best separates two classes by maximizing the margin between the closest points, or support vectors, from each class, improving generalization on unseen data. While linear SVMs directly compute a best-fit hyperplane, real-world data is often non-linear, prompting the use of kernel functions like linear, polynomial, and radial basis function (RBF) kernels to map data to higher dimensions.

SVMs excel in high-dimensional spaces and are memory-efficient, relying only on support vectors, making them ideal for text classification, where feature count often exceeds sample size. However, SVMs face challenges with large, noisy, or overlapping datasets, raising computational costs and impacting scalability. Key applications include bioinformatics, facial recognition, financial forecasting, and sentiment analysis, where SVMs remain a foundational benchmark for advanced machine learning algorithms.

2.1.2 Linear SVM

A Linear Support Vector Machine (SVM) is a supervised machine learning algorithm used for classification tasks. It works by finding the optimal hyperplane a straight line in two dimensions or a flat surface in higher dimensions that separates data points of different classes with the maximum margin. This margin is the distance between the hyperplane and the closest data points from each class, known as support vectors. By maximizing this margin, the Linear SVM minimizes classification errors and improves generalization to new data.

Linear SVMs are especially effective for linearly separable data, where classes can be distinctly divided by a straight line (or plane). They are computationally efficient, even for high-dimensional spaces, making them suitable for text classification and other large-scale tasks. Linear SVMs are also less prone to overfitting compared to other classifiers, especially in scenarios with fewer data points but a high number of features.

2.1.3 Non-Linear SVM

A Non-Linear Support Vector Machine (SVM) is a supervised learning model used for classification when data is not linearly separable, meaning it cannot be split by a straight line or plane. To handle complex patterns, a non-linear SVM uses a technique called the "kernel trick," which transforms the original input space into a higher-dimensional space. By mapping data points to this new space, it becomes possible to find a hyperplane that effectively separates classes, even if the boundaries are curved or more intricate.

Common kernel functions include the polynomial, radial basis function (RBF), and sigmoid kernels. Each kernel function defines a different way to calculate similarity between data points, allowing the model to capture a variety of patterns in the data. Non-linear SVMs are powerful for tasks like image and speech

recognition where the data exhibits complex structures. However, they are computationally intensive, especially with large datasets, and may require careful tuning for optimal performance.

3.1 Proposed system

The proposed system enhances security in online money transfers and ATM transactions by integrating face recognition and OTP (One-Time Password) verification, creating a robust, multi-layered defense against unauthorized access and fraud. By combining password authentication, facial recognition, and OTP, the system establishes strong protection against hacking and fraudulent activities. When a user initiates a transaction, the system first uses face recognition to verify identity. If the face matches the stored dataset, the transaction proceeds; if not, an OTP is sent to the registered mail for additional verification. This dual-layer approach ensures that only authorized users can complete transactions. Even in cases of attempted fraud or unauthorized access, the system sends alerts, providing real-time defense and a powerful deterrent against potential breaches. This layered security model enhances reliability and strengthens user confidence by safeguarding against identity theft and fraudulent activity.

3.1.1 Image capturing

To create the database, an image of each user's face is captured using a webcam. This image serves as a primary data point within the database, essential for efficient face recognition during verification. When a user initiates a transaction, the system references this stored image to compare with the live image captured. By using facial images as the main identifier, the database allows quick and accurate identity verification, ensuring only authorized individuals can access the system. This approach strengthens security by integrating biometric data, providing a reliable foundation for the face recognition verification process.

3.1.2 Pre-processing

The system employs pre-processing techniques to enhance the quality of images for effective face recognition. Image acquisition captures high-quality images, while image resizing standardizes dimensions and speeds up processing. Histogram equalization improves image clarity, and normalization adjusts pixel intensity levels for consistency. Additionally, grayscale conversion transforms colour images into shades of grey, simplifying the data by focusing on intensity rather than colour. Together, these techniques refine the captured images, ensuring uniformity and clarity before analysis. This pre-processing stage is crucial for reliable and accurate face recognition, as it provides standardized inputs that improve the recognition model's performance.

3.1.3 Liveness detection

Liveness detection is actually a biometric security feature meant to confirm that the biometric sample is from the live person instead of one displaying a photograph or video or with respect to the fake person. It uses liveness detection techniques such as blinking in the eyes or reflection in the eyes or head movement detection to confirm that it is indeed the user there and not trying to play a trick on the system.

3.1.4 Face recognition

Face recognition identifies and verifies individuals based on facial features such as unique geometry of a person's face-geometry, that is to say, measures the space between eyes, shape of their nose and jawline-to create what is usually called a faceprint that's accurate in identification and verification of a face. It uses OpenCV to recognize the user's registered face and compare it with the detected face. OpenCV is an open-source library in python designed for real-time computer vision applications.

3.1.5 Haar Cascade Classifier

Haar Cascade Classifier is an object detection algorithm designed to identify faces in real-time images. Primarily used for face detection, it can also identify other objects like eyes or specific patterns within images. The classifier works by calculating features over rectangular regions of an image, enabling it to detect distinct patterns associated with faces and other objects. Known for its efficiency, this algorithm is widely applied in computer vision tasks because of its speed and accuracy, particularly in real-time scenarios. Its ability to quickly process and identify faces makes it ideal for applications needing instant object recognition.

4.1 System architecture

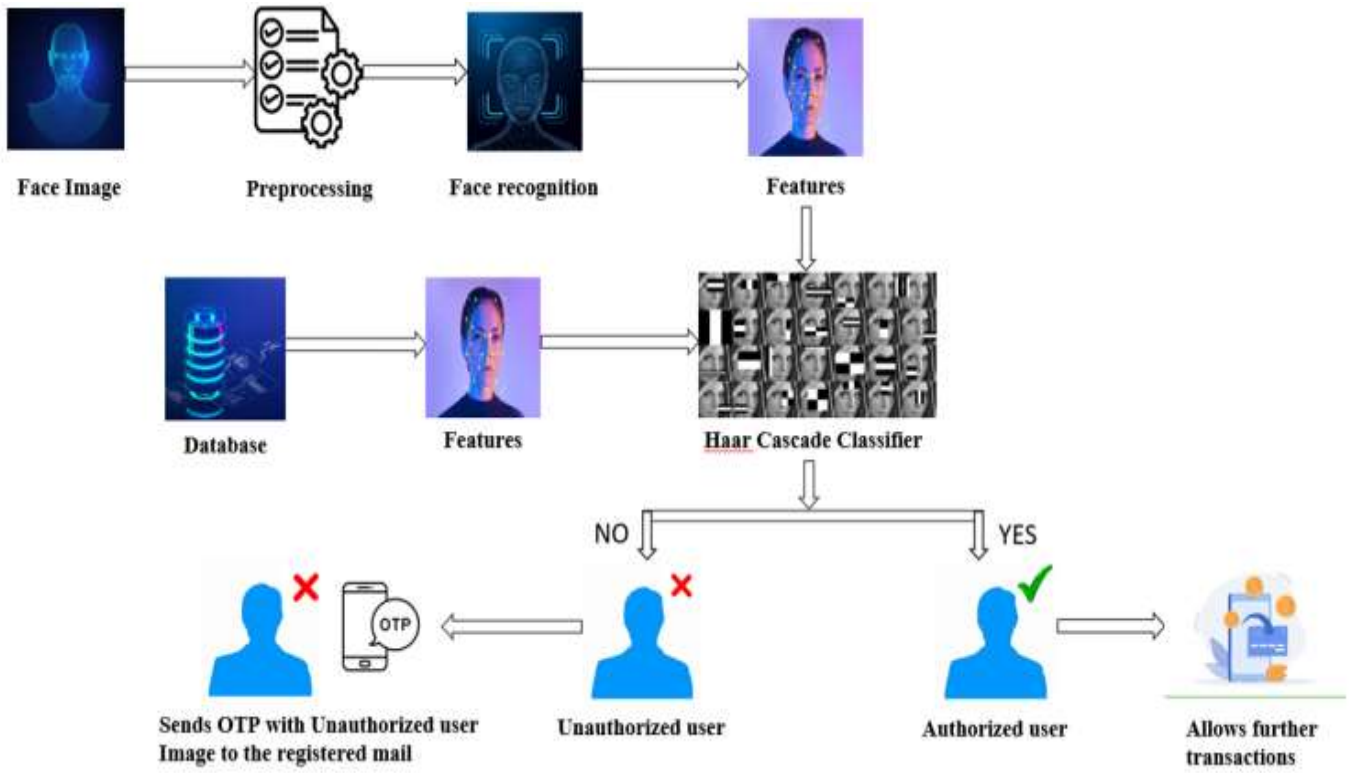

Figure 4.1 Architecture of the system

The architecture diagram depicts the workflow of a face recognition system. Face images are captured by a webcam from any user. That image is mainly used in all of the following processing and verification. A raw image preprocessed applies enhancements such as improvement of image quality and facial alignment to raise the recognition phase's accuracy and speed. This is done by taking some facial attributes, such as eye distance, nose shape, and jawline, and creating faceprint that can be used for identification or verification. The feature extraction aspect is also supported by OpenCV - the open-source computer vision library. These facial features are then stored as unique identifiers, which represent the face of the user that further compared to an array of stored records in a database to check if the user is authorized. The function for recognizing the face is performed by a machine learning algorithm, namely, the Haar Cascade Classifier, trained on facial images, showing accuracy in detecting the face from other objects. In case it does not match with anything in the database detected from the face, the system flags that user as unauthorized and sends an OTP along with the unauthorized user's photo to the registered user's e-mail address. This further gives the account owner more security by giving him a chance to verify an access attempt. When a matched face exists in the database, the system confirms the authenticity of the user and permits them to continue with further processing. After successful face recognition and OTP matching, access to process transactions is granted. This multi-layer check will ensure that authorized users who can pass through both security stages will be allowed to go further. The diagram shows a fusion of deep learning and machine learning. The image of the person is provided by the Haar Cascade algorithm and helps in face detection, while the data processing and feature matching will serve for robust authentication.

III. RESULTS AND DISCUSSION

The system enhances security for online transfers and ATM transactions through a multi-layered authentication approach, combining facial recognition, OTP verification, and liveness detection. Facial recognition with OpenCV and Haar Cascade Classifier authenticates users based on stored facial features, while liveness detection prevents spoofing via photos or videos. If no match is found, an OTP and the image of the unauthorized person are sent to the registered user's mail, alerting them to suspicious attempts. OTP verification adds dynamic security, ensuring transactions proceed only with correct input. This multi-layered approach improves ATM security, reduces fraud, and makes transactions safer and more user-friendly, offering a reliable, effective defense against unauthorized access.

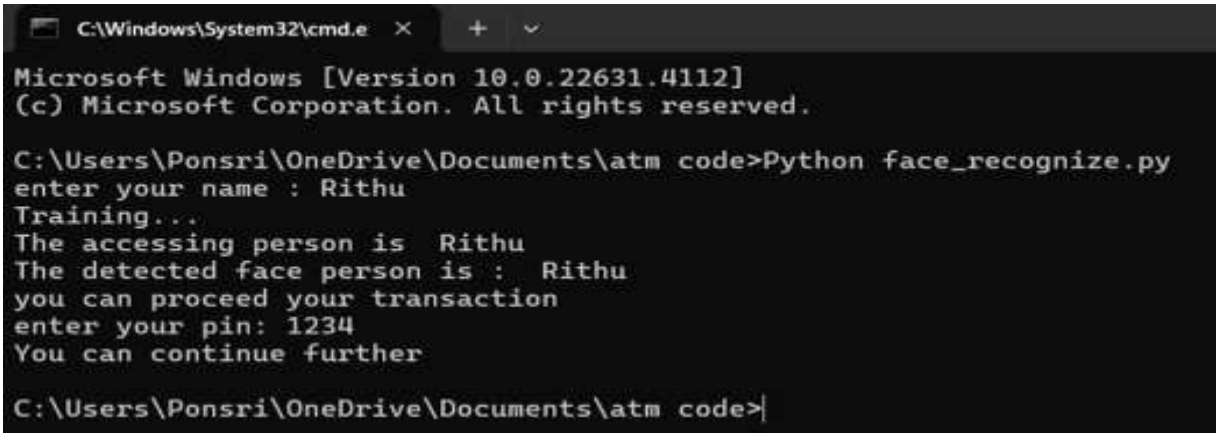

Figure 5.1 Authorized user

In the above figure, if the detected face matches the user's registered face, the accessing person is an authorized user and they are allowed to enter their PIN to proceed with further transactions and the transaction proceeds only when the PIN is correct.

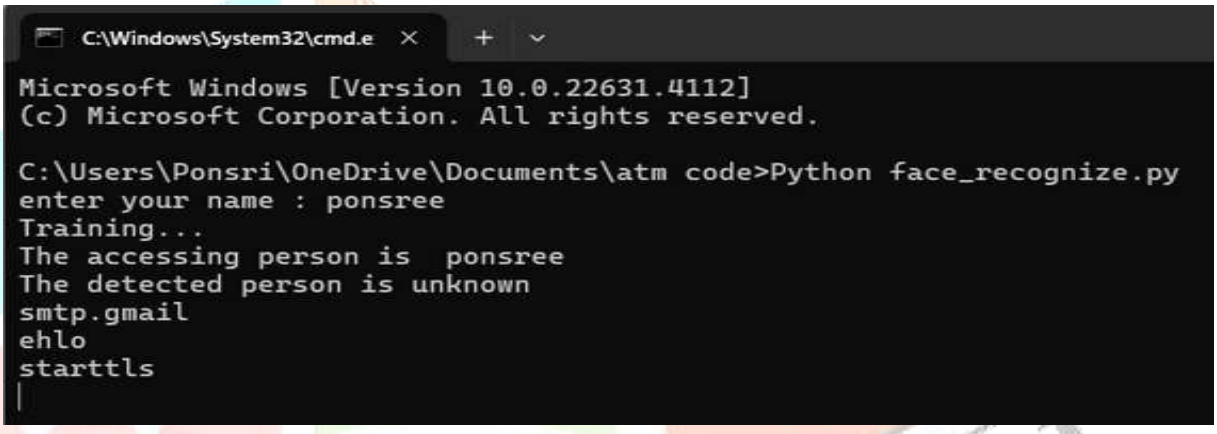

Figure 5.2 Unauthorized user

In the above figure, if the detected face does not match the user's registered face, the accessing person is an unauthorized user and the image of the unauthorized person along with an OTP is sent to the authorized user's registered mail.

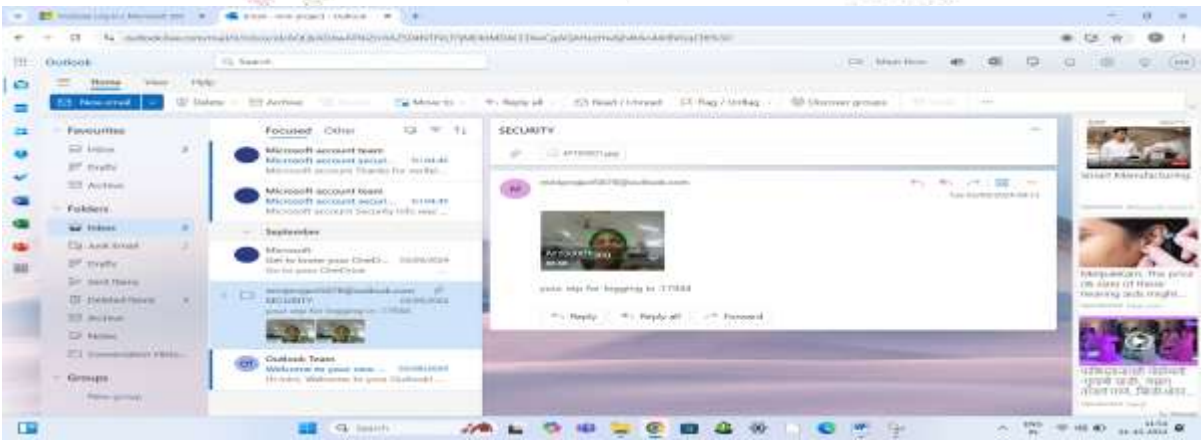

Figure 5.3 Security alert message sent to user's registered mail id

In the above figure, a security alert message is sent to the user's registered mail via SMTP which contains OTP along with an image of the unauthorized person.

Figure 5.4 Unauthorized user accessing through OTP

In the above figure, if the unauthorized person is known to the authorized user, the authorized user can share the OTP with them. If the person is unknown, we can send the image of the unauthorized person to the police, and the transaction will be cancelled. The transaction will only proceed if the correct OTP is entered.

IV. CONCLUSION

In conclusion, the system is all-inclusive and robust in providing a solution towards securing online money transfers and ATM transactions. With the integration of face recognition with OTP verification, the multi-layered approach does ensure the existence of measures towards reducing risks of unauthorized access and fraudulent activities. The usage of facial recognition along with advance techniques such as liveness detection ensures that only the registered user can gain access. Furthermore, Haar Cascade Classifier and OpenCV allow easy and accurate face detection. Another added dynamic layer of security for every transaction from the OTP sent to the registered user's email also requires an extra level of authentication. This layered security model prevents illegal transactions and misuse but also fosters a secure and user-friendly experience. Overall, this system offers a significant advancement in

safeguarding sensitive financial operations, contributing to a safer and more reliable transaction environment.

V. FUTURE ENHANCHEMENTS

Future improvements of the security system may include adding even more advanced biometric features, such as fingerprint recognition, for further verification of the identity. This is yet another multi-modal approach to a biometric system that will further enhance its immunity to spoofing and unauthorized access. The twins might be an exemption to the system. Few photographs have a scope so that photos might bypass the security in that situation. Scope for future, which uses High quality, Durable Cameras, are the usages of three-dimensional cameras if the conditions like the probability of occurrence of twins as well as using the feature of photography. Further advancement to increase the challenges of highly accurate spoofing attempts is achievable by making use of further advanced methods like 3D facial recognition and thermal imaging. Improve facial recognition accuracy with AI techniques, enabling adaptability to various lighting conditions and user's reliable performance in diverse environments.

REFERENCES

[1] D. Baehrens, T. Schroeter, S. Harmeling, M. Kawanabe, K. Hansen, and K.-R. Müller, "How to explain individual classification decisions," J. Mach. Learn. Res., vol. 11, pp. 1803–1831, Aug. 2010.

[2] A. Abaza, M. A. Harrison, T. Bourlai, and A. Ross, "Design and evaluation of photometric image quality measures for effective face recognition," IET Biometrics, vol. 3, no. 4, pp. 314–324, 2014.

[3] G. Aggarwal, S. Biswas, P. J. Flynn, and K. W. Bowyer, "Predicting performance of face recognition systems: An image characterization approach," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Colorado Springs, CO, USA, Jun. 2011, pp. 52–59.

[4] L. Best-Rowden and A. K. Jain, "Learning face image quality from human assessments," IEEE Trans. Inf. Forensics Security, vol. 13, pp. 3064–3077, 2018.

[5] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in Proc. 13th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG), Xi'an, China, May 2018, pp. 67–74.

[6] D. R. Faria, M. Vieira, F. C. C. Faria, and C. Premebida, "Affective facial expressions recognition for human-robot interaction," in Proc. 26th IEEE Int. Symp. Robot Hum. Interact. Commun. (RO-MAN), Aug. 2017, pp. 805–810.

[7] X. Wang, Y. Liu, F. Wang, J. Wang, L. Liu, and J. Wang, "Feature extraction and dynamic identification of drivers' emotions," Transp. Res. Part F, Traffic Psychol. Behav., vol. 62, pp. 175–191, Apr. 2019.

[8] K. Martin, E. Q. Wang, C. Bain, and M. Worsley, "Computationally augmented ethnography: Emotion tracking and learning in museum games," in Proc. Int. Conf. Quant. Ethnogr. Cham, Switzerland: Springer, 2019, pp. 141–153.

[9] K. Bahreini, R. Nadolski, and W. Westera, “Towards multimodal emo-tion recognition in e-learning environments,” Interact. Learn. Environ., vol. 24, no. 3, pp. 590–605, Apr. 2016.

[10] J.J. Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.