***Abstract:*** *Automated Teller Machine(ATM) enables the clients of a bank to have access to their account without going to the bank. As the number of ATM units increase, the machines are prone to hacker attacks, fraud, robberies and security breaches. In the past, the ATM machines main purpose was to deliver cash in the form of bank notes and to debit a corresponding bank account. However, ATM machines are becoming more complicated, and they serve numerous functions, thus becoming a high priority target to robbers and hackers. This paper gives the intersection between the ATM cards standards followed in the banks and the financial frauds. It undertakes two primary tasks: namely understanding of the traditional standard ATM card provided by the banks and a proposed methodology to make them more secure to reduce the ATM card frauds. The methodology uses the face detection procedure and online based account activation procedure which plays a prominent role to authenticate the user. This authentication mechanism is useful while transaction to secure ATM card from being cloned via skimming device, card trapping. This paper provides a generalized solution for financial fraud by the ATM card cloning or trapping that is being done in the field of E-banking.*

**Face Recognition Method:** OpenCV is a popular computer vision library started by Intel in 1999. The cross-platform library sets its focus on real-time image processing and includes patent-free implementations of the latest computer vision algorithms. OpenCV 2.3.1 now comes with a programming interface to C, C++, Python and Android. OpenCV 2.4 now comes with the very new FaceRecognizer class for face recognition, so you can start experimenting with face recognition right away. The currently available algorithms are:

* Eigenfaces
* Fisherfaces
* Local Binary Patterns Histograms

Local Binary Patterns methodology is used in this project for its high accuracy. Local Binary Patterns methodology has its roots in 2D texture analysis. The basic idea of Local Binary Patterns is to summarize the local structure in an image by comparing each pixel with its neighbourhood. Take a pixel as centre and threshold its neighbours against. If the intensity of the centre pixel is greater-equal its neighbour, then denote it with 1 and 0 if not. You’ll end up with a binary number for each pixel, just like 11001111. So with 8 surrounding pixels, you’ll end up with 2^8 possible combinations, called Local Binary Patterns or sometimes referred to as LBP codes. The first LBP operator described in literature actually used a fixed 3 x 3 neighbourhood just like this:



A more formal description of the LBP operator can be given as:

LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p s(i_p - i_c)

, with (x_c, y_c) as central pixel with intensity i_c; and i_n being the intensity of the neighbour pixel. s is the sign function defined as:

\begin{equation}
s(x) =
\begin{cases}
1 & \text{if $x \geq 0$}\\
0 & \text{else}
\end{cases}
\end{equation}

By definition, the LBP operator is robust against monotonic grey scale transformations. Dividing the LBP image into m local regions and extract a histogram from each. These histograms are called Local Binary Patterns Histograms.