With the development of technology our day to day life is becoming easier and convenient. Traditional way of making assure safety password protocol system is used. But this protocol has some drawbacks: it can be stolen, user can forget their password. As this security issue has become a talk of topic all over the world, the UK government started using biometric trait for identification in 190. After this several study took place for designing biometric system and having a good recognition accuracy. This technology uses physical or behavioral traits of user to solve the problem of authentication. Biometric system is consisting of four modules which are sensor module, feature extraction module, template database and a matching module. The process of authentication goes through in two stage: Enrollment stage and verification stage. When a user put his thumb on the sensor a picture of fingerprint is taken by the sensor module. Further from this picture the system extracted some data and make it suitable to generate template data and save them in a database for the verification stage. After that a query is made for matching the data with the template database to make sure that the user is a valid person. Imposing this for solving the security issue there arises two concern one is biometric traits cannot be revoked and reissued when the biometric information of a person is compromised. If a person fingerprint image is stolen it cannot be replacing in the template database as this information is unique.

Another problem is this biometric information are not secret. A user can leave his fingerprint on any surface without his/her acknowledgement. Ratha et al. has detected eight point from where this biometric information can be stolen or tempered. Namely, attacks on the interface, attacks on the modules: feature extraction module and matching module, attacks on the template database and also the channels from where the biometric information is flowing. One of the attack is spoofing which is an interface level attack occurs because of the fake biometric presentation. An experiment was taking place by attacking with the fake fingerprints. The result showing that the acceptance rate of fake fingerprint 67%. Liveness detection is a well-known countermeasure to distinguish between the fake fingerprint and the real fingerprint. Two scientist proposed to detect the perspiration phenomenon to differentiate the living fingers from the fake non – living fingers. Another researcher coli er al. utilized the static feature as well as the dynamic features of a fingerprint image which to prevent the spoofing attack. Galbally et al. proposed a method which use fingerprint parameterization based on the quality of fingerprint images. He proposed it as a classification problem where the result will be real or fake. Kim, a researcher proposed to design an image descriptor to handle liveness detection. He used a property of image which is dispersion. The difference of dispersion in the image gradient field will be different if the fingerprint is being faked. The most effective method is convolution neural network which is proposed by Jung & Heo to deal with the spoofing attack. This method uses robust framework for training and detection. Another problem in biometric system achieving the matching accuracy.

This accuracy of a biometric system can be measured by using three factor: False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (ERR). This accuracy depends on the image quality and the matching algorithms. There is a platform which is FVC-ongoing where researcher can upload their matching algorithm to evaluate the FAR, FRR and ERR. From now on, the best matching algorithm which name is HXKJ and its ERR = 0.022%. Another factor about gaining best accuracy of a matching algorithm is using template protection. From several studies researchers found that matching accuracy with template protection is worse than the without template protection. With or without template protection are tested on ideal condition where the result of with template protection is worse because of information loss in the process of feature adaptation.