**On the Vulnerability of Biometric Security Systems**Biometric technology have some weak security system which can be affected and the reason is it vulnerability. For security concern, it is consequential to modernize the technology with periodical improvement. Otherwise the system can be obsolete. To solve the difficulty, combining systems with security mechanisms are the most requisite key factors. To detect the vulnerability of biometric system two situations are intensely focused. First one is impostor’s try to access the system as a substitute of real user and another one is when a person avoid his identity which is suspenseful. Sensor, Transmission Between the sensor and the Feature Extractor, Feature Extractor, Transmission of the Extracted Features, Classifier, Data Base, Transmission of the Database Templates to the classifier, Decision are the eight attack levels. Three main authentication methods handheld token (card, ID, passport, etc.), knowledge based (password, PIN, etc.) and Biometrics have some advantages and drawbacks also. Biometric technologies like fingerprint, voice, iris, face reflects some vulnerabilities and there are also solutions. Data encryption and time stamp watermarking are two methods for solution. Although once the data are decrypted in encryption there are no further data protection. Adobe Photoshop and Corel Draw with Digimac technology introduces an information which cannot be erased without hampering the image standard & this can be fruitful for time stamp data.