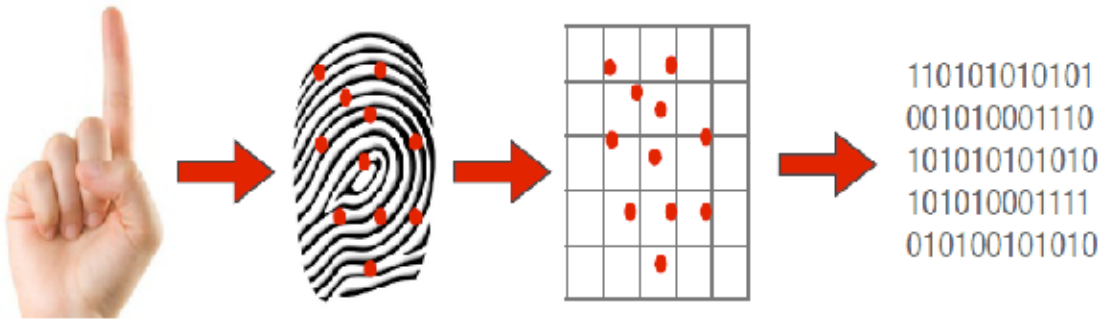
Information about biometrics

A common concern related to procedures like fingerprint analysis is fear of misuse of personal information. Potential issues such as stealing or tampering with the information discourages users from putting their trust in biometric technology. However, there is no scope for copying the information, and even if it is stolen, it can't be misused for causing any harm. The process of biometric analysis is constantly undergoing research to completely eradicate any such possibility.

Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints from the stored data.



The fingerprint templates are stored on a standalone server located within the secure state data center. This server is not connected to any other application or database. If you have been fingerprinted in the past for employment or for any other identification purposes, you must still enroll your fingerprints in the Oregon Vital Events Registration System (OVERS), as there are no ties to other governmental databases or agencies.

If you have any questions or concerns, please contact the OVERS help desk at 971-673-0279.