International Conference on Nuclear Security 2020

Contribution ID: **415** Type: **Paper**

Biometrics security and privacy protection

Monday 10 February 2020 14:45 (15 minutes)

Physical security at nuclear facilities is an important licensing and design consideration. The ultimate objective of the physical protection system (PPS) is to prevent the accomplishment of unauthorized overt or covert actions to nuclear facilities and nuclear materials. When a physical protection system is applied to a nuclear facility or to nuclear materials, its objective is to prevent radiological sabotage of facilities and theft of nuclear materials. Thus an effective system of physical protection also plays an important role in preventing illicit trafficking of nuclear materials. One of the main pillars of physical protection is controlling personnel access to facilities via Identification technology Systems. Identification technology is changing as fast as the facilities, information, and communication it protects. Recent years have seen a rapid adaptation of using various biometric systems for trusted human automatic recognition and controlling personnel access to nuclear facilities attributed to its high accuracy performance, discriminability, difficulty to be imitated and faked, and stability. Biometrics refers to the physiological or behavioral characteristics of an individual. Many physical characteristics, such as face, fingerprints, iris and behavioral characteristics, such as voice and gait are believed to be unique to an individual. With the exponential growth of using biometric systems, there is an increasing concern that the privacy anonymity of individuals can be compromised by biometric technologies. Unlike passwords and credit cards, which can be revoked and replaced when compromised, biometrics is always associated with a person and cannot be reissued. Biometrics is not secret; the iris of individual can be observed anywhere they look, people leave their fingerprints on everything they touch, and the person will not realize that his/her biometric is disclosed. Biometrics absolutely are sensitive information, therefore biometrics should be protected, because it may be misused by any attacker. To overcome the vulnerabilities of biometric systems, a number of recent strategies can be used such as biometric watermarking, visual cryptography, Steganography and cancelable biometrics. In this article, we provide an overview of various methods for preserving the privacy and security of the individual's biometrics data.

State

Egypt

Gender

Male

Author: Dr ZAHRAN, Osama (Assoc. Prof. at Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt)

Co-author: Mr ASAKER, Ahmed (Nuclear Security Head for First Egyptian Research Reactor)

Presenter: Mr ASAKER, Ahmed (Nuclear Security Head for First Egyptian Research Reactor)

Session Classification: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible

Track Classification: CC: Innovative technologies to reduce nuclear security risks and improve cost effectiveness, where feasible