Iris Cryptosystem Based on Elliptic Curve Cryptography

Ahmed A. Asaker[1], O. Zahran[3], Zeinab F. Elsharkawy[2], Sabry Nassar[1], Nabil Ayad[1], Fathi E. Abd El-samie[3]

[1]Reactors Department, Nuclear Research Center – Egyptian Atomic Energy Authority, Egypt.
[2]Engineering Department, Nuclear Research Center – Egyptian Atomic Energy Authority, Egypt.
[3]Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering, Menoufia
ahmad.asaker@gmail.com

1. Background and Goal of the present work

Nowadays, biometric identification systems provide a reliable solution for identity verification that allows restrictive access to radioactive sources location by unauthorized personnel. However, biometrics also have some specific security/privacy issues. Since the biometrics contain highly discriminatory information of the individual, the exposure of biometrics to an adversary may lead to some security breaches. In addition, it is infeasible to revoke the biometric data and publish new data. Besides, it is possible to cross-match multiple templates by compromising several databases, which may result in severe user privacy invasion. Therefore, the security and privacy issues of biometrics have been a major concern. In this work, elliptical curve cryptography (EEC) have been adopted for providing the demanded security services in this domain, it offer a potential solution that can be integrated into iris recognition systems to provide a higher level of security and make it difficult for an intruder to obtain the original IrisCode without knowing the secret information used to secure it.

2. General Proposed Iris Recognition System

In this research, a high-secure iris recognition system is presented using EEC to protect users's IrisCode during storage and transmission. Fig. 1 illustrates the different phases of the proposed iris recognition system. The proposed scheme consists of three phases begins with the IrisCode generation stage, IrisCode encryption and decryption process using EEC, and finally pattern matching. . Hamming Distance (HD) was chosen as a matching metric, which measure the similarity between two templates. The HD is the sum of non-equivalent bits between enrolled binary templates and query binary templates. If the two binary templates A, B, each have a length of N bits, the HD will be estimated as:

$$HD = \frac{1}{N}\sum_{j=1}^{N} A_j \oplus B_j \qquad \text{Eq. 1}$$

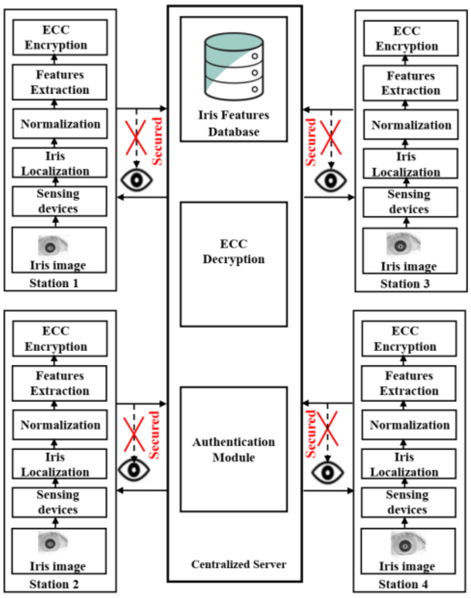

Fig. 1: Different stages of the proposed iris cryptosystem.

3. Experimental Results and Discussions

The proposed system is evaluated on CASIA-IrisV3-interval database [93]. In our experiments and evaluation, different snapshots of the right and left eye images of different classes have been considered.

In order to evaluate the proposed scheme performance, two scenarios have been considered; the traditional unprotected iris recognition scenario, and the proposed iris cryptosystem scenario. In our experiment, two HD scores are measured, which are genuine HD, and imposter HD. For genuine HD, we acquire a reference iris image of each class, which is matched with other images of the same class. In case of imposter HD, one template of a class is matched with other templates of other classes.

In the case of the traditional unprotected iris recognition scenario, a kernel probability density estimate was computed for the genuine and imposter HD distributions as shown in Fig..2 (left). The mean and standard deviation values for the genuine HD distribution are 0.2747 and 0.0460, while these values for the imposter HD are 0.4754 and 0.0114, respectively.

In the case of the proposed iris recognition scenario, a kernel probability density estimate was computed for the genuine and imposter HD results as shown in Fig. 2 (right). The mean and standard deviation values of the genuine HD distribution are 0.2747 and 0.0460, and the mean and standard deviation values of the imposter HD distribution are 0.4754 and 0.0114, respectively. By comparing the simulation results given in Fig. 2, it can be seen that the performance in the two cases is the same.

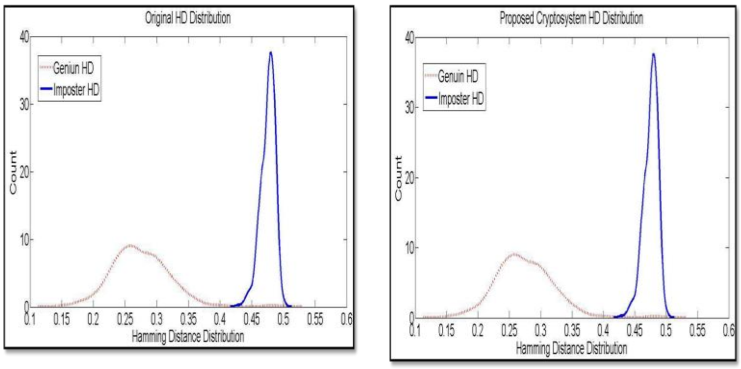

Fig. 2: Hamming distance plot for traditional unprotected iris recognition (left), the proposed iris cryptosystem (right)

For more evaluation of the proposed iris cryptosystem, other performance indicator parameters including sensitivity, specificity, NPV, PPV, EER, accuracy and decidability were also obtained for the unprotected iris recognition system and the proposed iris recognition system as summarized in Table 1.

Performance metric	unprotected IrisCodes	Proposed approach
Sensitivity	1	1
Specificity	0.9926	0.9926
NPV	1	1
PPV	0.9912	0.9912
EER	0.0037	0.0037
Accuracy	0.9960	0.9960
Decidability	6.0733	6.0733

Table 1: Summarized results of performance metrics for the original and proposed systems

It can be proved from the results in Table 1 indicate that, other performance indicator parameters are identical in both cases, which demonstrate that the proposed iris cryptosystem gives good performance similar to the case of unprotected iris.

To ensure the confidentiality of the proposed iris recognition system, the protected IrisCodes generated by the proposed system should be highly irrelevant to the original IrisCodes. To measure the similarity between the original IrisCode and the protected IrisCode created from the same iris image, the normalized correlation coefficient (NCC) was computed. Then, a kernel probability density estimate was computed for the normalized correlation coefficient.

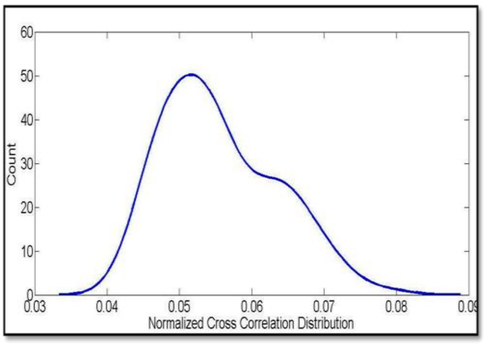

Fig. 3: NCC distribution plot between the original IrisCodes and protected versions of the same IrisCodes.

As can be seen in Fig 3, the NCC between the original IrisCode and the protected version of the same iris is very close to zero with mean and standard deviation values of the distribution of 0.0556 and 0.0078, respectively, which proves the complete difference between the protected IrisCode created by the proposed system and the original IrisCode.

4. Conclusions and Acknowledgements

- In this work, a high-security iris recognition system was proposed. The experimental results and analysis prove that the proposed technique is promising for IrisCode protection as it guarantees a high degree of privacy/security protection without affecting the performance accuracy. Finally, the proposed model for securing iris recognition system can be used for other binary biometric feature template protection schemes. Other forms of feature templates should be changed to binary to use the proposed technique.