Abstract

Reliable information security mechanisms are required in the today’s era of cyber theft. Traditional Cryptography is a powerful mechanism to achieve information security. Current cryptographic algorithms (e.g., Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA) have a very high proven security but they suffer from the key management
A Biometric Solution To Cryptographic Key Management Problem Using Iris Based Fuzzy Vault

problem. Human identification is also a challenging field. That is why if we can make a blend of
cryptography and biometric then it becomes a upcoming security tool. Using unique biometric
identity of a person the keys for cryptosystem can be made secure. Iris is one of the proven and
accurate means to identify person and it does not change throughout life of a person. This
paper presents a biometric solution to cryptographic key management problem using iris based
fuzzy vault.

Reference

- A. Bodo, Method for producing a digital signature with aid of biometric feature, German
  Patent DE 42 43 908 Al, 1994
- Juels, and M. Wattenberg, "A fuzzy commitment scheme", Proc. of sixth ACM Conf. on
in Proceedings of Third International Conference on Audio- and Video-Based Biometric Person
  Lausanne, Switzerland, 2002, p. 408.
  and challenges,” Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management),
  vol. 92, no. 6, pp. 948–960, Jun. 2004
  Proc. of IEEE Int. conf. on Multi-media and Expo, pp. 2203-2206, 2004
- Anil K.Jain, Sharath Pankanti,Umut Uludag Department of Computer Science and
  Engineering, “Fuzzy vault for fingerprint”, Michigan State University, East Lansing, MI, 48824
  2.Exploratory Computer Vision Group, IBM T.J. Watson Research Center, Yorktown Heights,
  NY, 10598
- Ari Juels RSA laboratories, 174 middlesex turnpike, bedford, ma 01730, USA ,Madhu
  Sudan Massachusetts Institute of Technology, 32 Vassar street, Cambridge, MA 02139, USA,
  “A Fuzzy Vault Scheme” , RSA Lab, Received November 27, 2002; Revised January 12, 2005;
  Accepted February 16, 2005
- Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, and Sharath
  Pankanti, Senior Member, IEEE, “Fingerprint-Based Fuzzy Vault: Implementation and
  Performance”, IEEE transactions on information forensics and security, vol. 2, no. 4, December
  2007.
- Karthik Nandakumar, Abhishek Nagar and Anil K. Jain, “Hardening Fingerprint Fuzzy
- Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, “Biometric Template Security”,
  EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January
  2008
- E. Srinivasa Reddy, Ramesh Babu; “Performance of Iris Based Hard Fuzzy Vault”
  IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January
  2008
- E. Srinivasa Reddy, Ramesh Babu; “authentication using fuzzy vault based on iris
  texture” Second Asia international Conference on Modeling & Simulation 2008, pp 361-368
- Khin Sint Sint Kyaw “iris recognition system using statistical features for Biometric
identification”, international conference on electronic computer technology, pp 554 – 556, 2009
- Book- digital Image Processing – Rafael C. Gonzalez, Richard E.Woods, Pearson Education. Pg.no.522

Index Terms

Computer Science

Information Security

Key words

Biometrics

cryptosystem

fuzzy vault

encoding

decoding

chaff points

polynomial projection

Lagrange interpolation