Continuous Encryption Functions For Biometric Based Information Security Over Networks And Other Applications

Tech ID: 32832 / UC Case 2021-813-0

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Published Application	2023026203	08/17/2023	2021-813

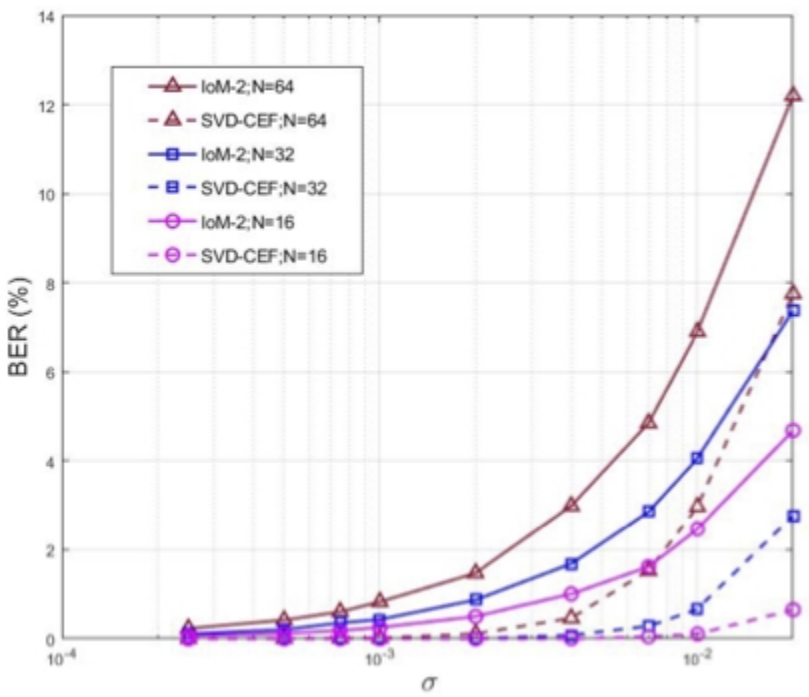
FULL DESCRIPTION

Background

Biometric based passwords or keys are useful for information security over networks with much reduced burden for legitimate users. A crucial tool needed for biometric security is the so called non-invertible continuous functions – used to transform a private biometric feature (such as a fingerprint) into a secure password. Prior designs of these functions can be inverted within a time that is a polynomial function of the dimension of the biometric feature. In other words, if some of the previously used passwords based on a common biometric feature are known, the attacker can recover the biometric feature and hence knows all future passwords based on this feature. Prior designs have also ignored the need to prevent an attacker from finding a surrogate feature that yields the same passwords as the original biometric feature.

Current Invention

Prof. Yingbo Hua at UCR has designed a novel, patent pending Continuous Encryption Function (CEF) that is non-invertible – non-invertible within a polynomial time. The ready to implement CEFs are all related to singular value decomposition (SVD), eigen value decomposition (EVD) or some other 3 factor factorization of a matrix consisting of random modulations of the input vector. The CEFs also enable new system level designs. The encrypted identifications can be used to securely exchange information between two users.



Bit error rates (BER) of SVD-CEF in comparison with current best in class – index of max hashing method

CONTACT

Venkata S. Krishnamurty
venkata.krishnamurty@ucr.edu
tel: .

OTHER INFORMATION

KEYWORDS

Biometrics, Encryption, Cyber security, Biometric passwords, Network security, Continuous encryption function, Non-invertible encryption function

CATEGORIZED AS

- **Computer**
  - Security
  - Software
- **Security and Defense**
  - Cyber security

RELATED CASES

2021-813-0

ADVANTAGES

The significant features and benefits of this invention are:

- The input or surrogate input of the CEF cannot be determined from its output regardless of the amount of output exposed.
- The CEF is non-invertible within polynomial time.
- No part of the CEF's output can be predicted from other parts of its output without knowing the input.
- Relieves users of the burden of remembering long and secure passwords for their online tasks.
- The SVD-CEF is also less sensitive to noise.

SUGGESTED USES

Applications that could benefit from this invention are:

- Information security over the internet
- Password and biometric based password security
- Physical layer security of wireless networks
- End-to-end cybersecurity

STATE OF DEVELOPMENT

The encryption functions have been designed and tested and readily implementable.

RELATED MATERIALS

- Continuous Encryption Functions for Security Over Networks

University of California, Riverside

Office of Technology Commercialization

200 University Office Building,

Riverside,CA 92521

otc@ucr.edu

research.ucr.edu/