CHAPTER 61

INSTITUTE OF INFORMATICS & COMMUNICATION
&
CLUSTER INNOVATION CENTRE

Doctoral Theses

01. MANISH KUMAR
Design and Development of Encryption Models Based on Dynamic Key Driven Shuffling Methods.
Supervisors : Dr. Sanjeev Singh and Dr. M. K. Das
Th 24202

Abstract
(Not Verified)

The reach of the internet is enabling users to share voluminous data in shape of images on the daily basis and their security has become a major issue to be addressed. It is noticed in the literature that almost every existing crypto systems based on chaos lacks in one or other features desired in the design of an ideal crypto system. This may also be due to the inherent properties of inappropriate chaotic dynamical system chosen or its parameters used in the design of crypto system. Essential processes of the cryptosystems like key scheming, confusion, shuffling and diffusion uses chaos based systems and each of them is affected by the poor selection of chaotic system or their control parameters. Learning from the foregoing discussion, cryptosystems based on chaotic dynamical systems are proposed. The role of chaotic dynamical systems in the encryption and decryption processes is made as an essential part. The design itself takes care of maximum participation of the encryption key into encryption/ decryption processes. Various loop holes related to key, confusion, shuffling and diffusion are addressed in different chapters and their solutions are proposed. A unique shuffling method and FBM based diffusion approach makes the cipher image more robust against various known attacks. An important feature of 3-D matrix based cryptosystem is to ensure the integrity of data at receiver end, which is achieved without using the checksums. A practical implementation of one of the cryptosystems designed for IoT applications is implemented with a health parameter monitoring device and general purpose sensor platform with on board WiFi. Simulations on various hardware and software platforms and related security analysis shows the strength and capabilities of the cryptosystems. Various comparisons in terms of security parameters with existing cryptosystems is also carried out.

Contents

1. Introduction. 2. Image security using chaos based dynamical systems and reversible cellular automata 3. Tamper detection and encryption using 3-D matris 4. Lightweight encryption model for IoT ecosystem and its application in healthcare devices 5. Securing bulk data using fractional brownian motion based diffusion mechanism 6. Conclusion and future scope. Bibliography.

.