Comparative performance of the classifiers for cryptosystem identification*

Shri Kant †
Coordinator, Joint Cipher Bureau
Department of Defence R & D
M. G. Road, Metcalfe House
Delhi 110 054, India

Rajesh Kumar Asthana ‡
Bharat Lal Jangid §
Scientific Analysis Group
Defence R&D Organisation
Metcalfe House
Delhi 110054, India

Abstract

In the present work the problem of cryptosystem identification from their cipher texts have been addressed. The supervised classification models from statistical decision theory and Artificial Neural Network have been employed for the purpose. These classification models have been validated on known data sets from UCI repository. After validation the models have been used for crypto system identification. Several feature extraction and selection techniques have been made use of for carrying out the comparative performance of the classifiers.

Keywords and phrases : *Feature extraction, classification, functional approximation, density estimation, artificial neural network, blind verification.*

1. Introduction

The categorization of input data into identifiable classes by extraction of significant features or attributes of the data is defined as pattern recognition [1]. In pattern recognition there are three major steps i.e. sampling

*This paper was presented at '*Pre-ICM International Convention on Mathematical Sciences*' held at Department of Mathematics, University of Delhi, 18-20 December, 2008.

†*E-mail*: shrikant.ojha@gmail.com

‡*E-mail*: rajasthana_drdo@rediffinail.com

§*E-mail*: jbharatlal_ce@yahoo.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 4, pp. 347–368