

PALMPRINT AND CRYPTANALYSIS BASED BIOMETRIC SECURITY SYSTEM USING DEEP LEARNING

Kolloju Ramesh¹, Ravi Bolimera¹, Ravichand Sankuru¹, Kuthuru Thapan Reddy¹,
Janga Pranay¹, Kore Pradeep¹

¹Dept. of ECE, Nalla Narasimha Reddy Education Society's Group of Institutions

In a time when worries about data security and privacy are growing, it is critical to develop strong and trustworthy biometric authentication solutions. In order to create a highly effective and safe identification system, this abstract presents a revolutionary method to biometric security that combines the individuality of palmprints with cutting-edge deep learning algorithms and cryptanalysis. A subset of biometric authentication called palmprint recognition relies on each person's unique combination of veins, ridges, and wrinkles. This modality has many benefits, such as resistance to forgeries, non-intrusiveness, and ease of acquisition. However, obstacles including stance, noise, and changes in illumination have made it difficult to integrate into real-world security systems. Recurrent Neural Networks (RNNs), one type of deep learning architecture, are trained on a huge palmprint dataset in order to extract discriminative features and enhance recognition performance. To safeguard palmprint templates during transmission and storage and prevent possible assaults on the privacy and integrity of the system, sophisticated encryption algorithms are used. A multi-layered defensive mechanism is produced by the biometric security system's integration of cryptanalysis and deep learning. To sum up, a state-of-the-art method for biometric security combines cryptanalysis, deep learning, and palmprint recognition.