IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

Data Embedding with Reversible Encoding

D. Surendhar[1] and R. Mahalakshmi[2]
PG Student, Department of computer Applications[1]
Associate Professor, Department of computer Applications[2]
Vels Institute of Science, Technology and Advanced Studies, Pallavarm, Chennai, India
surendharvfc@gmail.com and mahabs69.research@gmail.com

Abstract: *Data Embedding with Reversible Encoding (DERE) has been introduced for preserving image privacy and data embedding. DERE usually involves three parties, namely, the image provider, data hider, and receiver. On the security with key setting, there are three categories: share independent secret keys (SIK), shared one key (SOK), and share no secret keys (SNK). In SIK, the image provider and data hider must respectively and independently share secret keys with the receiver, whereas in SNK, no secret key is shared. However, the literature works proposed SNK-type schemes by using homomorphic encryption (with exorbitant computation cost). In this paper, we address the SOK setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key. To realize our SOK scheme in a simple manner, we propose a new technique by using multi-secret sharing as the underlying encryption, which indeed induces a blow-up issue of the key size. For preserving the efficiency of the key size, we apply a compression by using lightweight cryptographic algorithms. Then, we demonstrate our SOK scheme based on the proposed techniques, and show effectiveness, efficiency, and security by experiments and analysis. We address shared one key (SOK) setting, where only the image provider shares a secret key with the receiver, and the data hider can embed a secret message without any knowledge of this key.*

Keywords: Key Generation, Image Encryption, Message Embedding, Decryption and Extraction.