IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

Image Scrambling Toward Efficient Encrypted Image Retrieval in Cloud Computing

Ms. Payal Ramteke[1], Ms. Akshata Nawale[2], MS. Priti Kashyap[3], Ms. Pornima Petkar[4]
Students, Computer Science and Engineering[1-4]
Shri Sai College of Engineering and Technology, India

Abstract: *A previously proposed image encryption method, which applied dual scrambling at both the pixel position and bit levels, was subjected to cryptanalysis. The original algorithm rearranged pixel locations using a chaotic sequence and further scrambled individual pixel bits (0s and 1s) through a second chaotic sequence derived from a user-provided key. While the designers claimed that the method could withstand chosen-plaintext attacks, detailed analysis revealed that its security primarily relied on three components: the pixel position scrambling sequence (T), the bit-level scrambling sequence (WT), and the diffusion sequence (S). Among these, only the generation of sequence T was influenced by the original image's pixel values, whereas WT and S remained independent of the image content. This structural weakness allowed attackers to successfully perform chosen-plaintext attacks and recover these equivalent key streams, effectively decrypting the image. The feasibility of this attack was confirmed through both theoretical evaluation and experimental validation. To address this vulnerability, the authors introduced an improved encryption algorithm designed to resist chosen-plaintext attacks and mimic the behaviour of a one-time pad system.*

Keywords: cryptanalysis; chosen plaintext attack; image encryption; chaotic system

DOI: 10.48175/IJARSCT-28197