

**AN EFFICIENT HOMOMORPHIC IMAGE ENCRYPTION ALGORITHM
FOR CLOUD STORAGE**

N.N.D. Malshika^{*} and G.S. Wijesiri

Department of Mathematics, University of Kelaniya, Kelaniya, Sri Lanka

^{}dulshanmalshika1199@gmail.com*

Today, an increasing amount of data is transmitted via the Internet. This data includes not only text but also audio, images, and other multimedia. Images are commonly used in our daily lives. However, it is vital to building a secure encryption scheme when delivering images over an unsecured network. Homomorphic cryptographic techniques protect privacy while allowing computation on encrypted data. Moreover, it is a type of encryption that allows users to compute encrypted content without decrypting it. Many public-key encryption techniques, including homomorphic encryption schemes, are theoretically proven but not deemed practical for various reasons, including the huge size of the public key. The study uses the Hermite Normal Form (HNF) encryption technique to provide an efficient homomorphic encryption algorithm for image processing operations on encrypted images saved in the cloud or transmitted over an unprotected connection. The HNF method has proven highly versatile and secure, making it ideal for homomorphic encryption. The scheme was tested using some generated codes in python language. Analyses like histograms and correlation are performed to verify the proposed scheme's efficiency. The experimental results demonstrate that the suggested strategy can accomplish efficiency and security for cloud users.

Keywords: Decrypt, Encrypt, HNF, Homomorphic encryption