# A Novel Image Cryptosystem Based on a 3D Chaotic Hash Function

**By**

**Wafaa Hamdan Selman Alshoura**

**Supervisor**

**Dr. Ayman M. Abdalla**

**Co-Supervisor**

**Prof. Dr. Abdelftah A. Tamimi**

## ABSTRACT

Due to the recent developments in multimedia communication techniques and the rapid increase in the number of social media users, protecting multimedia information has become more essential. As a basic component of multimedia, the image deserves special attention, especially images containing sensitive information. They need to be protected from unauthorized access.

One of the most secure techniques for image protection is to encrypt the image in a form difficult to understand and difficult to be returned to the original unless a decryption key is provided. Recently, many algorithms have provided techniques to encrypt an image based on the methods of image confusion and diffusion. These two methods are general techniques for image encryption that take many variations, where confusion means that each bit of the encrypted image should depend on several parts of the key, and diffusion means that

changing a single bit of the original image should change at least half of the bits in the encrypted image. In addition, chaos theory provides more secure ways to encrypt an image employing a combination of confusion and diffusion operations.

This thesis presents a new system to encrypt images based on a 3D chaotic hash function, where the hash value used is a secret compound key. The secret compound key consists of a password, initial conditions, control parameters, and coupling parameters, in addition to an independent key. The hash function produces a secondary key stream that is used in two encryption methods proposed with the system; the first is a diffusion method and the second is a confusion method. The decryption process of this system uses the original compound key to recover the original image without any loss of information. The secondary key is regenerated at the receiving end. It is not sent with the encrypted image.

Evaluation of the proposed system was done using many images with different sizes, including grayscale and color images. Multiple measurements of the experimental results showed this system is strong against statistical, differential, and brute force attacks. The proposed system was shown to have high encryption complexity and sensitivity to the encryption key and the input image, providing a high level of security. The system can be used in social, military, and medical applications, and in many other fields that require image confidentiality and security.