**PROPOSED ARCHITECTURE FOR IMAGE ENCRYPTION**

**Image Encryption**

Nowadays, information security is becoming more important in data storage and transmission. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Many of the Internet applications such as video conferencing, military image databases, personal online photograph albums and cable television require a fast and efficient way of encrypting images for storage and transmission.

Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons.

* One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data.
* The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data.

Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. A digital image is defined as the two-dimensional(2D) rectangular array. The elements in this array are denoted as pixels. Each pixel has an intensity value i.e. the digital number which represents by 8 bits ( the values ranges between 0 – 255).

Fig.1. Proposed Architecture for Image

Original Image (\*.jpg)

Image Encryption Algorithm (AES,DES, 3DES)

Image Decryption Algorithm (AES,DES, 3DES)

Cipher Code (an Encrypted Image)

Original Image (\*.jpg)

KEY

KEY