**IMAGE** **ENCRYPTION: SECURE DATA TRANSFER**

**INTRODUCTION**

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets.

The need for a secure computing environment has never been greater. Right now, information security professionals are in great demand and the importance of the field is growing every day. All the industry leaders have been placing their bets on security in the last few years.

Now, applications must be coded from the ground up with security in mind, as these applications will be used by people who expect the security and privacy of their data to be maintained. This series intends to serve as a very brief introduction to information security with an emphasis on networking.

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfil such a task, many image encryption methods have been proposed.

**I. Cryptography:** The many schemes used for enciphering constitute the area of study known as cryptography. There are three types of cryptography: **1.1 Secret Key Cryptography** This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption. The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption. **1.2 Public Key Cryptography**

This type of cryptography technique involves two key crypto systems in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob’s public key and Bob can decrypt the message with its private key

**1.3 Hash Functions**

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus. Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information Therefore it’s very important to protect our image from unauthorized access.

**ABSTRACT:**

*Digital image encryption algorithm based on chaos and improved DES, 2009*

Zhang Yun-Peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [10] researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. Their result show high starting value sensitivity, and high security and the encryption speed.

*A Novel Image Encryption Algorithm Based on Hash Function, 2010*

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [11] proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.