Chapter 33
A Contemplator on Topical Image Encryption Measures

Jayanta Mondal
KIIT University, India

Debabala Swain
KIIT University, India

ABSTRACT

Images unduly assist digital communication in this aeon of multimedia. During times a person transmits confidential images over a flabby communication network, sheer protection is an accost contention to preserve the privacy of images. Encryption is one of the practice to clutch the reticence of images. Image encryption contributes a preeminent bite to charter security for secure sight data communication over the internet. Our work illustrates a survey on image encryption in different domains providing concise exordium to cryptography, moreover, furnishing the review of sundry image encryption techniques.

INTRODUCTION

Information technology in the web is proliferating without warning, causing massive users communicating via interactive media, especially; image, audio, and video. Images immerse the ample snippet of digital communication and play a consequential role in communication, for instance; military, medical agencies and diplomatic concerns (Shannon, 1949). Images, carrying significant private information, needs absolute protection during transportation or storage. In short, an image entails protection from diverse security attacks. The major motive to safeguard images is to ensure confidentiality, integrity and authenticity. Various techniques are at disposal for keeping images secure and encryption is one of them. Encryption does transform images into a cipher images mostly by assistance of a key. Later, an authorized user can recover the original image by decryption, the reverse process of encryption. This process is a part of the study called cryptology. Cryptology is the addition of cryptography; science of making ciphers, and cryptanalysis; science of breaking ciphers.

DOI: 10.4018/978-1-7998-1763-5.ch033

The field of modern cryptography provides a theoretical upheld focused around which a person can comprehend what indubitably these concerns are, the finest approach to assess practices that fancy to light up them and the means to gather conventions in whose safety one can have conviction (Kumar, Aggarwal, & Garg, 2014). Modern automated progresses have made private information by and large available. Security concerns over internet data made cryptography the field of interest for the researchers. The traditional and basic issue of cryptography is to provide secure communication over an untrusted channel. A has to send a secret message to B over an unsecured media, which can be hacked. The late forge ahead in technology, exceptionally in automation and information industry, allowed huge business for electronic interactive multimedia data through the Internet. This advancement made the web highly accessible with its contents, which encouraged obvious security problems. Digital security is maintained by some methods used to protect the sight and sound substance (Shannon, 1948). This whole picture acutely centered on cryptography.

PRELIMINARIES

Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

- **Plaintext:** Plaintext is the original intelligible message.
- **Ciphertext:** Ciphertext is the transformed message.
- **Encryption:** Encryption is the process (algorithm) for transforming a plaintext into a ciphertext.
- **Decryption:** Decryption is the reverse process of encryption, i.e. transforming the ciphertext back to plaintext.
- **Key:** Key is the most important data used by encryption algorithms, known to the both authorized parties. Encryption mechanisms relies on the key. Encryption algorithms are available for all, so, attacker's objective is to achieve the key.

Basic cryptography process for a text message at its simplest form can be described as:

Plaintext $P=[P_1, P_2, \ldots, P_X]$ of length X, where X belongs to finite alphabet set. The key $K=[K_1, K_2, \ldots, K_Y]$ of length Y. Ciphertext $C=[C_1, C_2, \ldots, C_Z]$ of length Z. With message P and key K the encryption algorithm creates the ciphertext $C=EK(P)$. The plaintext can be achieved by $P=DK(C)$. D being the decryption algorithm.

A cryptosystem thus can be formulated mathematically as a five tuple *(P, C, K, E, D)* where the following should satisfy:

1. P is a finite set of possible plaintext.
2. C is a finite set of possible ciphertext.
3. K, the key space, is the finite set of possible keys.
4. E is encryption rule, and, D is decryption rule.
5. $\forall k \in K, \exists e_k \in E, \exists d_k \in D$

Each $e_k: P \rightarrow C$ and $d_k: C \rightarrow P$ are functions,
Such that $\forall x \in P, d_k(e_k(x))=x$