Chapter 41
A New Image Encryption Method Based on Improved Cipher Block Chaining with Optimization Technique

Kuppusamy Krishnamoorthy
Alagappa University, India

Mahalakshmi Jeyabalu
Alagappa University, India

ABSTRACT

Security of images in transmission medium is most prime issue found in literature. Encryption of images is a way to secure it from unauthorized access. The authors in this chapter insist on the encryption of images via block ciphers. Block ciphers works simultaneously as well as on chunks. In this chapter, an encryption method using improved cipher block chaining is proposed to encrypt RGB color images. For every encryption methodology, key generation process is the most important phase. The authors proposed sub-optimal key generation algorithm and this nature inspired optimization technique reveals complex keys, remains very useful for decision making in dynamic environment. Key generation is crafted as complex with this mathematical model that overcomes the predicament key problem exists in existing methods and upgrades quality of encryption. Results of the proposed algorithm show the efficiency and its resistance against various cryptanalytic attacks.

INTRODUCTION

Security of the data, when transmitted through communication medium is most prime issue found in literature. In recent decades, images are used as a medium to transfer the messages between the consigner and consignee since it is considered to be more secure than the text data. It is used at various fields such as in defense services, Health care services, E- Learning etc. Fundamental issue is that the images need utmost protection while pass through networks, to resist it from various authentications and authoriza-

DOI: 10.4018/978-1-5225-9866-4.ch041

tion vulnerabilities. Intruders may hack the information completely or partially modify some content. Various security mechanisms like authentication, digital signatures, and cryptographic algorithms are used to protect images from unauthorized attacks (Mahalakshmi & Kuppusamy, 2016).

Cryptography is the science of designing mathematical models to secure the images from interloper attacks. Encryption and Decryption are the two phases to be handled in any cryptographic process. Encryption is the phase of converting the original user defined plain data into unintelligible format called cipher, where as decryption remains as the reverse to convert the cipher back to original. The encryption may be categorized either as full encryption or partial (Ramkrishna Das& Saurabh Dutta, 2013). Symmetric key Encryption and Asymmetric Key Encryption are the two categories of cryptography for which the Symmetric key uses single secret key shared between the consigner and consignee. In Asymmetric key encryption two keys are involved, one for the encryption and another for the decryption. The authors in this chapter focus on novel symmetric key encryption method to secure the images.

Various encryption algorithms are developed with ultimate goal to reduce the computational cost and increasing its performance (Yas & Alsultanny, 2008). Secret key algorithms are devised to work either as streams or as blocks. In stream cipher encryption finite numbers of characters are encrypted, and in block ciphers blocks or chunks of data is encrypted simultaneously (Panduranga, &Naveen Kumar, 2012). The main objective of this chapter is to develop an algorithm to elevate security to the images that are passed through the open networks between the sender and receiver. A plenty of approaches are employed to encrypt the images by various authors in the literature. This chapter brings out a new hybrid algorithm, to encrypt the RGB (Red, Green, Blue) image. This approach is expressed by a mathematical model formulated with improved cipher block chaining, the mode used for encrypting data at chunks. Every block of data differs and also it is the self synchronizing mode where the error propagation is less. It overcomes various security threats to the images when transferred between communicating entities.

Authentication and integrity maintenance of the images when transferred through open networks is considered in this chapter. Security policies must be examined by both sender and receiver so as to maintain the authenticity of the image. The image encryption method proposed in this chapter, is based on block cipher combined with logical substitution operations to strengthen the encryption code. In the scheme of key generation, the optimization technique is operated so as to minimize the cost of algorithm by means of time and speed. The genetic algorithm is one among the optimization technique, is the direct approach that uses a specific objective function to minimize the total cost of the taken for the execution. Genetic Algorithm is mainly consumed for specific selection of features in the images to extract or to cipher. Multi-objective function is generated for the proposed algorithm, one is to minimize the execution cost and the other is to reduce the execution speed. Genetic Algorithm is iterative optimization procedure used to solve complex optimization problems either it is maximize or to minimize (Kalyanmoy Deb, 2005). GA's are characterized by its robustness against attacks as well as ability to work with non-convex problems (Fossati et al., 2015).

Organization of the Chapter

In Section 2, the authors explained the various related symmetric key algorithms and their outcomes. After a fast overview, in section 3, the proposed encryption algorithm for the RGB color images is presented in more detail, particularly key scheming. In section 4, experimental results are placed to demonstrate the algorithm's performance on RGB images. Then, in section 5, the algorithm used in this chapter for image encryption and decryption using the proposed approach is in-depth compared with existing accepted algorithms of various authors by means of security analyses and verify the robustness of the algorithm. In Section 6, the conclusion of this approach is drawn.