Chapter 92
A Literature Review on Image Encryption Techniques

S Geetha
School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, India

A Magnus Infanteena
School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, India

P Punithavathi
School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, India

S Siva Sivatha Sindhu
Shan Systems LLC, Jersey City, USA

ABSTRACT

Encryption is one of the techniques that ensure the security of images used in various domains like military intelligence, secure medical imaging services, intranet and internet communication, e-banking, social networking image communication like Facebook, WhatsApp, Twitter etc. All these images travel in a free and open network either during storage or communication; hence their security turns out to be a crucial necessity in the grounds of personal privacy and confidentiality. This article reviews and summarizes various image encryption techniques so as to promote development of advanced image encryption methods that facilitate increased versatility and security.

INTRODUCTION

Digital images have crossed the point of being used just as a famous pastime and are now occupying a significant part of our current communications. The proliferation in technology has driven a plethora of hand-held electronic devices and advanced personal computers to be the inevitable style of communication for progressively large portions of the population. Camera phones, digital cameras, etc., have made taking, processing and sharing of photos nearly instantaneous, leaving the way for digital images to emerge into an unavoidable element in hi-tech communications. Cloud has provided a feasible manner for facilitating storage of all these images and their use has still been enhanced by applications like Twitter, Facebook, WhatsApp, etc. The digital images carry the sensitive information of individuals,

DOI: 10.4018/978-1-7998-7705-9.ch092

organization from one region to target place. The image domains range over diverse fields – medical images, satellite images, biometric images, scanned documents etc., each with special characteristics pertaining to the domain. These images bear equivalent proximity to numerous security attacks just like the regular data and information.

The statement "information at rest" is misrepresentative in the current sense. In this age of cloud and virtualization of everything – from storage to applications to infrastructure, information very hardly has time to "stay at rest" since it is frequently being called on for use. Further to that, the strengthening advancement, commitment and sophistication of hackers, demand for new and effective ways to secure data.

Initially encryption was considered to be highly cumbersome to implement and use as well as time consuming but currently it is looked upon as the real solution. Researchers have made huge advances in how they apply encryption, shedding away the complexity of the technology, however sustaining security.

Image Encryption

The digital images carry the hypersensitive information of individuals, government and corporate sectors during their expedition in the cyber space – from the storage space to the user's device and vice versa. Most of these images, either personal or organizational, demand a proper security mechanism to provide the required protection. Hence this service of securing the images is expected to operate in the application layer of the network guarding the transmitted image against unsolicited disclosure as well as protecting the images from illicit alterations during transit. The security techniques include several aspects like authentication, copyright protection, confidentiality and access control. Three popular ways to protect digital images from unauthorized eavesdropping are encryption, steganography and watermarking (Balasubramanian, Selvakumar, & Geetha, 2013), (Cox, Miller, Bloom, Kalker, & Fridrich, 2007), (Uhl, Pommer, & Uhl, 2004). Among these three techniques, encryption has become one of the major tools to provide high level of security. It deals with the content confidentiality and access control while authentication and copyright protection are handled by watermarking techniques and confidentiality is addressed by steganography techniques (Geetha, Kabilan, Chockalingam, & Kamaraj, 2011). However, a critical perspective that holds the users against the use of traditional text encryption algorithms for image encryption stems from two reasons. The first one is the far exceeding ratio of the image size to the text size, which introduces intolerable time consumption to encrypt the image data. Secondly, image has some natural characteristics which are absent in the text data, that complicates the same encryption procedure.

Digital images demonstrate unique characteristics such as high redundancy and exhibit high correlation among pixels and they are huge in size. Further different imaging applications have varying needs, like preservation of image consistency, performing image compression for transmission and real time processing systems etc. The conventional text encryption algorithms are not designed to make use of it or they lack improvements in the algorithms catering to these innate characteristics. Owing to these factors, the researchers have designed and developed significant amount of image encryption algorithms, which are the focus of this paper.

Image encryption deals with the set of techniques that convert images between intelligible and unintelligible forms. Image encryption is the course of transforming the image into another unreadable form (which is almost a noisy 2D signal) so that only an authorized recipient can reconstruct the image and get the information in it. The forward way of converting image to unreadable form is called as encryption while the reverse process is called as the decryption. The original image is called as plain-image while the unreadable image is called as cipher-image.