Partial Image Encryption and Decryption Methods for Real Time Applications

ABSTRACT:

Information security plays a very important role in the field of communication and data storage. Image encryption is one of the ways for information security. The use of image and video communication has increased dramatically in recent years. Moreover it is becoming increasingly important to securely transmit data in limited bandwidth. Encryption and decryption produce bottlenecks (narrow congested area) in real time secure image and video communication. Many approaches have been used or proposed to provide security for information disseminated over the networks. These include encryption, authentication, and digital signatures. For video, the method has been adopted to protect unwanted interception and viewing of any video while in transmission over the networks.

The fully layered technique (whole content is first compressed) is the traditional image and video content protection scheme using various typical keys (DES, AES, IDEA, etc.). The typical encryption algorithms are inadequate because exact specific characteristics of this kind of data (high-transmission rate with limited bandwidth). The protection of an image and Video content in modern inclination is identified as Partial image encryption. Image encryption processing, which is vital to the economy and the quality of life of people and is increasingly affected by the pre-dominantly digital world today. Communication networks are essential to share the information. Thus these systems are increasingly requiring higher levels of security control to allow access to information to authorized personnel only. It is suggested that partial image encryption approach is an inexpensive and simple encryption method. The variety of security systems can be used for image transmission in the partial image encryption method. Partial encryption may make real time secure communication feasible because it can be easily be implemented and it is computationally simple. The goal of partial encryption of a bit stream is to make the entire stream somehow useless for anyone that who cannot decrypt the ciphered subset. The main goal of partial encryption is to reduce the amount

of data to encrypt while achieving a required level of security. The important feature in partial encryption is to make the protected part as small as possible. Encryption can be done in two ways, the first is by pixel position scrambling and second is by pixel value manipulation, for better image encryption use both approaches. Partial image encryption algorithm used to reduce the quantity of data to encrypt while achieving a satisfactory and low-cost protection.

Dr. Parameshachari B D **B.E., M.Tech., Ph.D, SMIEEE, MIETE, MISTE**
Professor & Head,
Dept. of Telecommunication Engineering.
GSSS Institute of Engineering and Technology for Women,
(Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India)
K R S Road, Near Vikranth Tyres,
Mysore - 570016
Mobile: +91-8762693561/ +919886211981
E-Mail: hodte@gsss.edu.in, parameshbkit@gmail.com, drpbd81@ieee.org
https://orcid.org/0000-0002-3997-5070
Scopus Author Id: 55342182200

Scholar Index:

https://www.scopus.com/authid/detail.uri?authorId=55342182200
https://scholar.google.co.in/citations?user=BDSMDeUAAAAJ&hl=en
http://www.researcherid.com/rid/F-7045-2018