

A Novel Image Encryption Optimization Technique

Dr. Shantappa G Gollagi
Computer Science & Engineering
Hirasugar Institute of Technology
Nidasoshi, India
shantesh1973@rediffmail.com

Dr. Srividya R
Information Science & Engineering
CMR Institute of Technology
Bengaluru, India
srividya.ramisetty@gmail.com

Dr. Santhosh Kumar G
Director/Principal
East West College of
Engineering,
Bengaluru, India
skg2185@gmail.com

Dr. Piyush Kumar Pareek
Computer Science & Engineering
Nitte Meenakshi Institute of Technology
Bengaluru, India
Orcid Id: 0000-0003-2287-0122

Abstract— *Image file confidentiality is a difficult issue these days for a variety of reasons in a range of industries, including medical, defence, academia, and many more. A range of practical ways have been studied in recent years to safeguard image data, however owing to technological improvements, such existing solutions have significant limits in current systems. Several academics have investigated a number of methodologies and strategies for maintaining picture secrecy and shielding top-secret information from attackers while images are sent via communications infrastructure. In this paper, a unique picture encryption technique based on a chaotic map and DNA encoding is jointly used for image encryption in a more pragmatic approach, as necessary in today's world to safeguard private data. This approach was tried and confirmed on a personal laptop with a 64-bit operating system, Windows 10, with 16 GB RAM and the MATLAB R2020a version loaded (Random Access Memory). The results of this suggested approach reflect the best NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changed Intensity) scores for a variety of selected photos for testing. This method works with a variety of image formats and is in great demand in today's world for safeguarding sensitive data or information while being transmitted across a communications infrastructure. More research is needed in the future to identify practical answers, as current communication networks are quickly changing throughout the world owing to technology breakthroughs.*

Keywords—Communication, Data, Encryption, Information, Image, NPCR, UACI.

I. INTRODUCTION

Digital image security has grown very difficult and daunting throughout the world due to a myriad of technical difficulties as well as the sharing of photographs over the web via communications media. During delivery, picture secrecy is a critical but top concern, and numerous techniques to protecting data packets via communications infrastructure have been examined. Data encryption and authentication are major roadblocks for individuals all across the world[1]. The analysis and testing of different unique ways for protecting sensitive data during communication for securing private data from various

attackers is both complicated and vital. Various academics have looked at a variety of data security approaches, including cryptography, which is a useful strategy for safeguarding sensitive information and reducing the risk of unwanted access during communication[2].

Data or information protection is one of the most important aspects of correspondence, which necessitates extra caution in order to preserve personal information. As the photographs are broadcast, their security becomes progressively more challenging. Photographic metadata is distinct from that of other data types such as text, music, video, and so on. Secure techniques are required when critical but equal data is communicated from one side to the other by humans in the context of images or documents. Traditional cryptographic methodologies and procedures serve a critical role in assuring the safety of sensitive data or information when it is sent through a communication medium. The picture content is critical for defending against intruders since it contains a variety of useful information. There appear to be a range of file formats that include a great deal of critical information that may be shared via social media[3], [4]. The categorization of picture encryption techniques is shown in Figure 1.

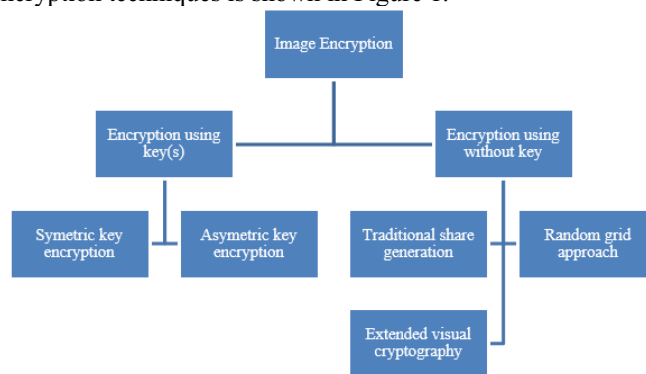


Fig. 1. Illustrates the classification of image encryption approaches. As research, engineering, and culture have evolved, the technology sector has grown to symbolise a major position internationally, where a narrow division of multiple digital image apps is becoming disproportionately widespread. Electronic advantages have been the most commonly used media types, having uses in domains as varied as diplomacy, economics, security, and education. On the other hand, picture transmission security is in jeopardy owing to