Abstract

Encryption security and encryption speed are two important aspects of image encryption algorithms. Due to their increasingly large size, video images present a great challenge to currently available cryptographic algorithms; the processes of encryption and decryption of images are so computationally intensive that they introduce delays beyond acceptable real-time application limits. [1] In this paper we introduce a new algorithm that uses dynamic square matrices as both encryption keys and the control stream to verify which key will be used for each block. The study case showed in this paper works on GF(7) and for encryption key sizes varying from 3X3 to 12X12. The goal is to provide a highly secure encryption algorithm with a wide space for encryption speed.

References

- "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video"; Las Vegas, Nevada, USA September 20-September 23
  ISBN: 0-8186-7180-7
- "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed..."

- "Gauss Jordan elimination method for computing outer inverses," Predrag S. Stanimirovi_c1, Marko D. Petkovi_c2.
- Yong Zhang "Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling" 2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)

**Index Terms**

Computer Science

Security

**Keywords**

Galois field   real time   image encryption