A novel chaotic butterfly network topology based block scrambling and crown graph based bit-wise diffusion for image encryption

Vidhya R, Brindha M

Frontiers of Computer Science, DOI: 10.1007/s11704-020-9196-8

Problems & Ideas

- **Problems** of chaotic cryptosystem for the protection mechanism are
  - key streams applied for encryption mechanism fully relies on secret keys, and no relationship is made with the input image content
  - the encryption mechanism itself has loopholes which gives partial knowledge of ciphered images and ends with entire encryption system to be broken.
- **Ideas: Adaptive key generation**
  - so that different random sequences highly influenced by plain image are generated to overcome the chosen/known plain text attacks.

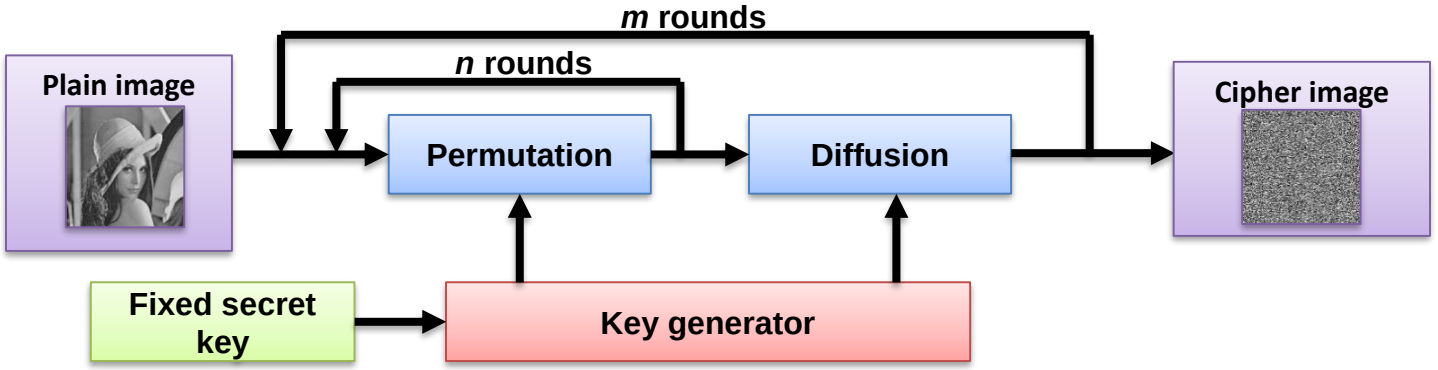

Fig.1 General chaotic encryption system with fixed secret key

Main Contributions

- An innovative Plain Image-content Dynamic key generation function is recommended for both confusion and diffusion principles. Rather than using fixed initial vectors, distinct initial vector is generated from image-content (i.e., from plain image).
- A novel conditional structure based BNT scrambling is proposed in this work. As in an image, 8 bits are needed for representing each pixel, three layer BNT is considered for bit level permutation which leads to the proposed permutation process.
- To achieve strong diffusion, a novel Crown Graph based Bit-wise Diffusion (CGBD) is proposed. The diffusion architecture follows the crown graph structure (i.e., corresponding position bit will not be encountered to diffuse the bits) to diffuse each pixel.

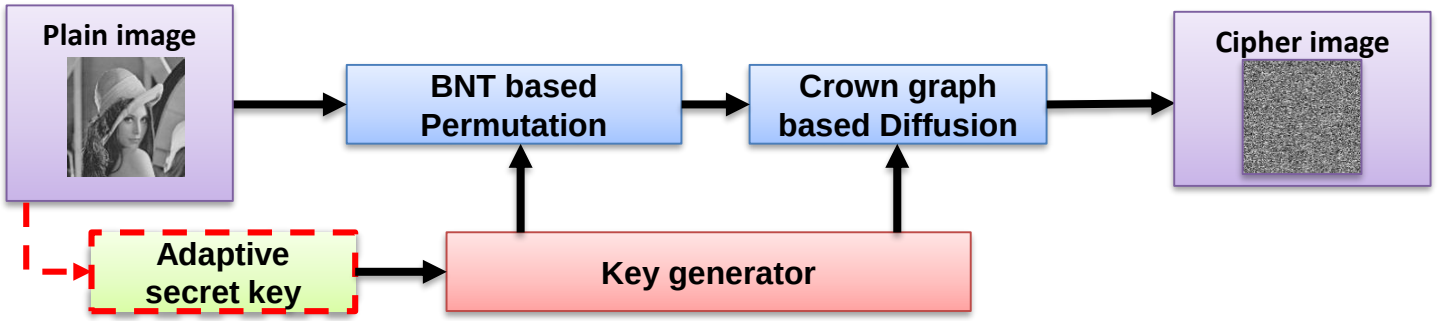

Fig.2 Proposed chaotic encryption system with Adaptive secret key