INDICON 2013

Impact of Engineering on Global Sustainability
13 - 15 December, IIT Bombay, Mumbai, India
IEEE Bombay Section and IEEE India Council

IEEE BOMBAY SECTION

Digital Image Encryption using Improved Chaotic Map Lattice

Radhika Chapaneri[#], Santosh Chapaneri[@], Dr. Tanuja Sarode[#]

[#]TSEC, [@]SFIT, University of Mumbai

1. The Big Problem: Image Encryption

Security of digital images is crucial to preserve privacy.

Medical Imaging
Satellite Images
Military Images
Applications
Multimedia Security
Confidential video conference
Pay-per-view TV
Aadhar card Enrolment

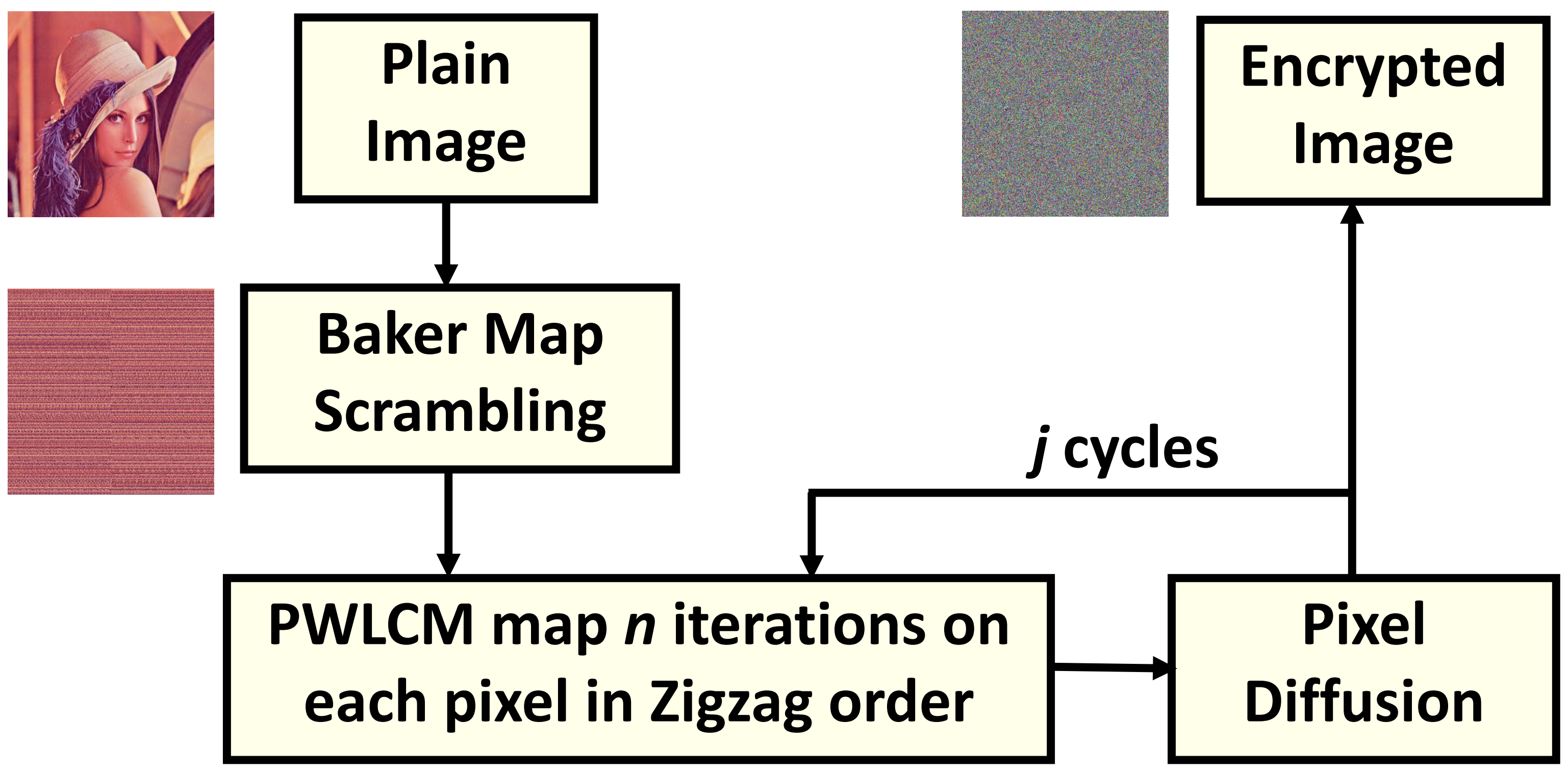
Figure 1. Applications of Image Encryption

Features: High correlation; Bulk capacity; Redundancy

Problem: Conventional Algorithms (DES, RSA) not applicable

2. Solution: Chaos-Based Cryptography

- **Flaws of original Chaotic Map Lattice (CML):** Improper keys, Non-invertible, key space violating basic principles
- **Proposed Solution**: Improved CML (ICML) achieving both confusion as well as diffusion



Plain Image

Baker Map Scrambling

PWLCM map *n* iterations on each pixel in Zigzag order

Pixel Diffusion

j cycles

Encrypted Image

Figure 2. Schematic of Proposed Solution (ICML Encryption)

3. Details of ICML

- 256-bit secret key => Key space is 2^{256}
- Instead of Logistic Map, use Piecewise Linear Chaotic Map (PWLCM) => highly chaotic with positive Lyapunov exponent
- Invertible since conversion of A/D and D/A done before and after making *n* iterations of the map
- Pixel diffusion achieved using "XOR plus mod" operation, incorporating a different PWLCM

4. Results and Analysis

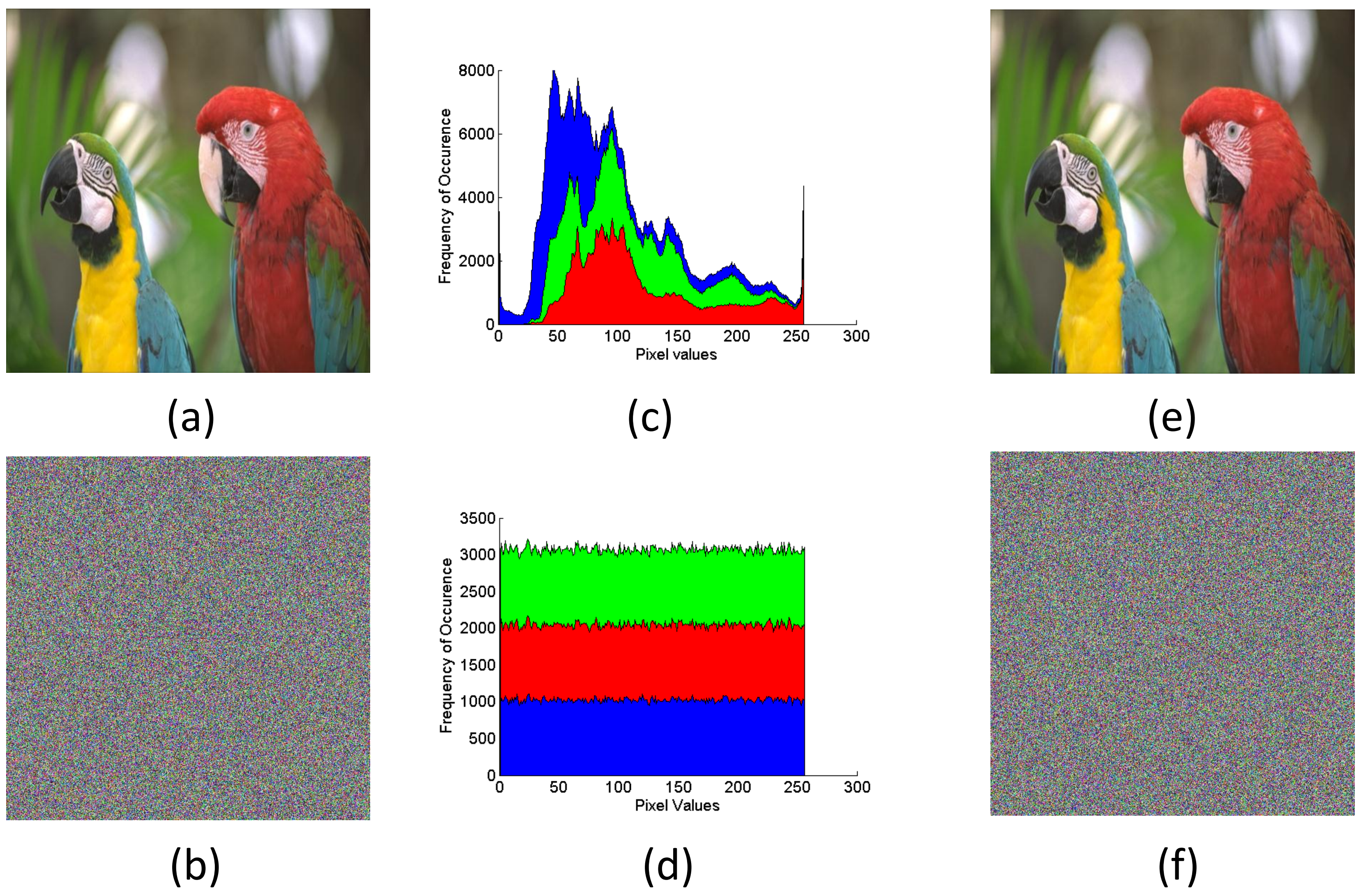


Figure 3. (a) Plain Image, (b) Encrypted Image with *K*, (c) & (d) Histograms of (a) & (b), (e) Decrypted Image with correct *K*, (f) Decrypted Image with one-bit change in *K*

Table 1. Statistical Analysis of ICML

Test Criteria	Ideal Random Image	CML Cipher Image	Proposed ICML Cipher Image
NPCR %	99.5693	84.3281	**99.6384**
UACI %	33.2824	31.7260	**33.5668**
Entropy	8	7.4957	**7.9994**
Correlation	0	0.1693	**0.0046**
Kurtosis	1.8054	5.3549	**1.8062**
χ^2 test (histogram uniformity)	293	55,114	**200**

5. Discussion

- Highly sensitive to changes in input image as well as changes in key => resists differential cryptanalytic attacks
- Achieves both confusion and diffusion by effective use of chaotic maps => resists known/chosen-plaintext attacks
- High level of security, large key space, passes statistical moment analysis tests
- Solution suitable for grayscale as well as colour images

Contact email: radhikachapaneri@gmail.com
santoshchapaneri@gmail.com