Aashiq Banu S, Amirtharajan R, 2021. Bio-inspired cryptosystem on the reciprocal domain: DNA strands mutate to secure health data. *Frontiers of Information Technology & Electronic Engineering*, 22(7):940-956. http://doi.org/10.1631/FITEE.2000071

# Bio-inspired cryptosystem on the reciprocal domain: DNA strands mutate to secure health data



**Key words:** Medical image encryption; DNA; Chaotic attractors; Crossover; Mutation; e-Healthcare

ORCID: S. AASHIQ BANU, https://orcid.org/0000-0002-7708- 0307; Rengarajan AMIRTHARAJAN, https://orcid.org/0000-0003- 574-3045

# Motivation

- Over the past few years, the healthcare sector has embraced a digital transformation by improving quick access for faster diagnoses and transfer of medical records around the world.
- The amounts of data and applications are increasing and are transferred to the public cloud by decentralised Internet networks.
- Significant challenges are faced in telemedicine and e-healthcare because of the many different threats such as malicious attacks and data breaches.
- Security of digital information is critical in such sectors as a patient's medical images.
- Cyber criminals may be able to view medical images illegally and acquire medical services easily.
- They may steal protected health information (PHI) and exchange sensitive information on the dark web

# Methodology

## DNA

- Large-scale parallelism, small power consumption, peculiar molecular structure
  - ✓A-Adenine
  - ✓T-Thymine
  - ✓ C-Cytosine
  - ✓G-Guanine

## Integer wavelet transform

- ✓Splitting
- ✓Predicting
- ✓Updating

## Lorenz attractor

## Lü attractor

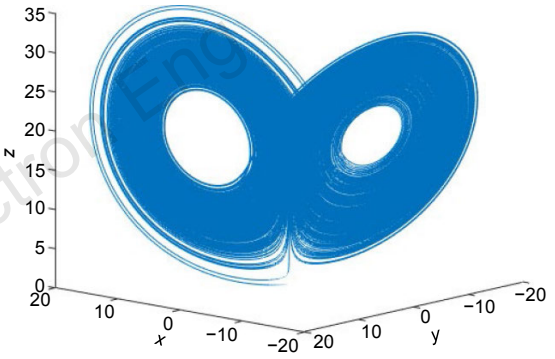


**Fig. 3 Illustration of the complex performance of the Lorentz attractor (*x*-*y*-*z* planes)**

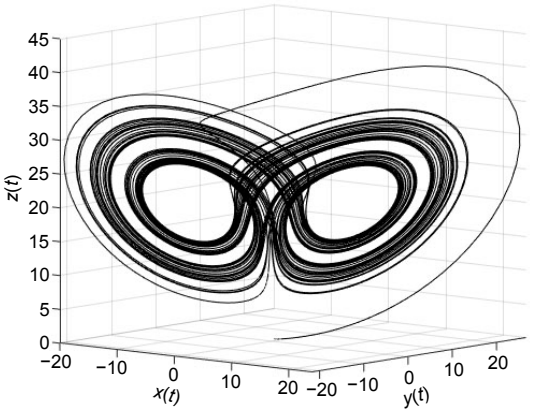


**Fig. 5 Illustration of the complex behaviour of the Lü attractor (*x*-*y*-*z* planes)**

# Proposed method

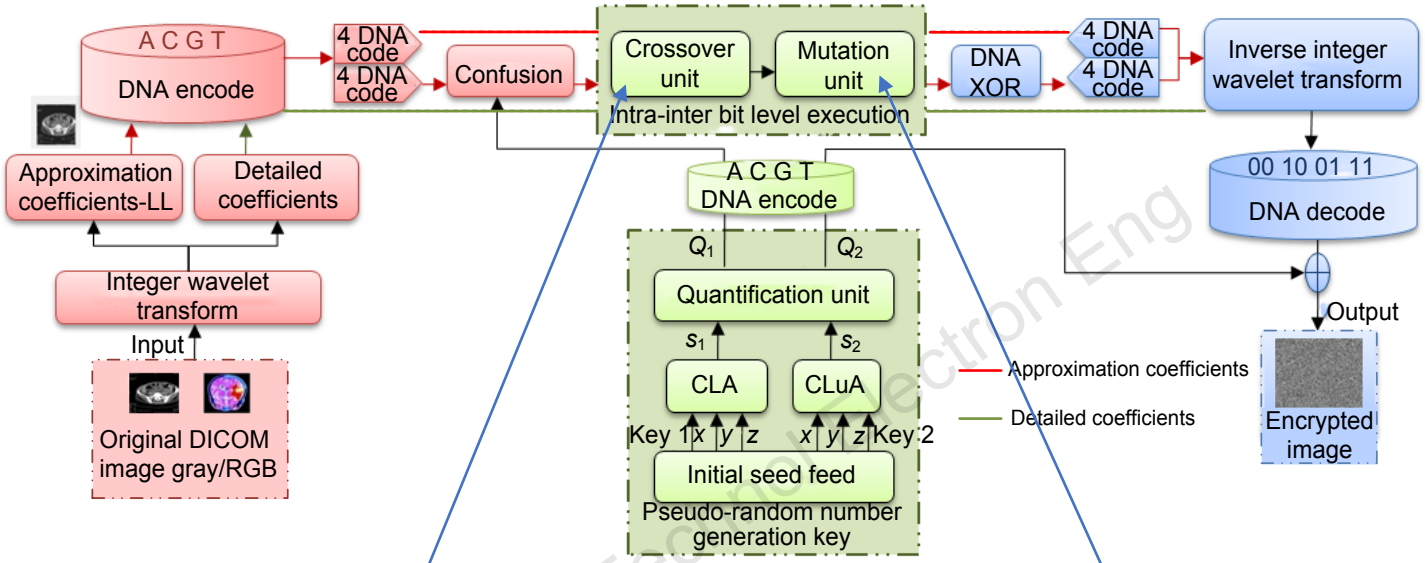


**Fig. 7 Overall architecture of the proposed method**

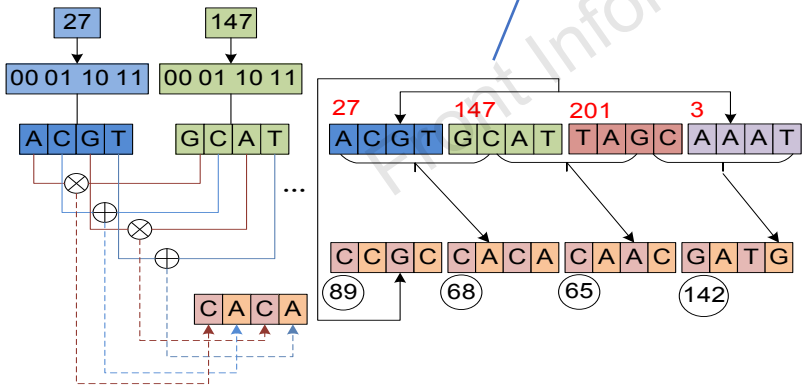


**Fig. 8 Crossover process**

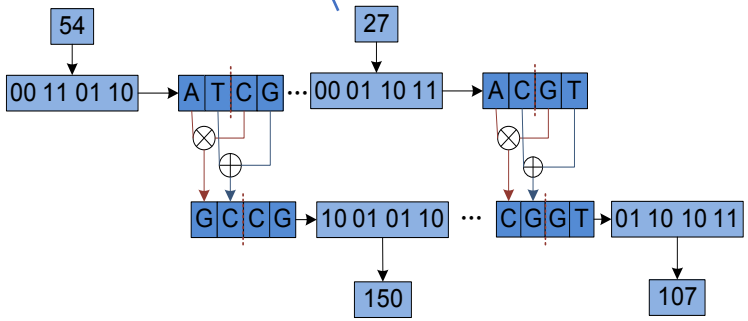


**Fig. 9 Mutation process**

# Results and analysis

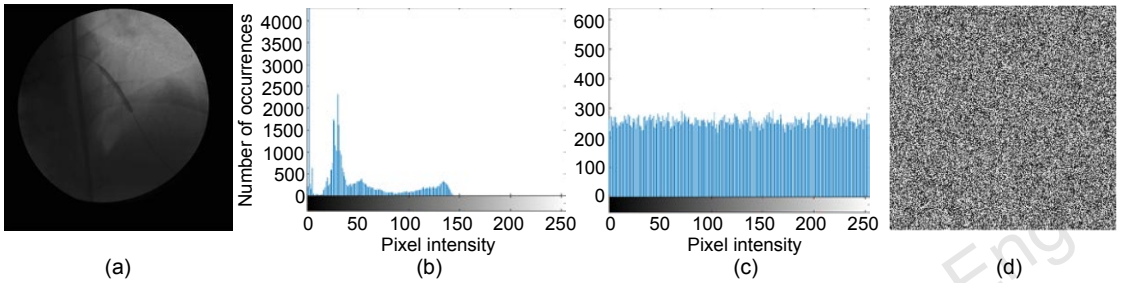


**Fig. 12 Analysis of the gray DICOM image: (a) original image; (b) histogram of (a); (c) histogram of the encrypted image; (d) encrypted image**

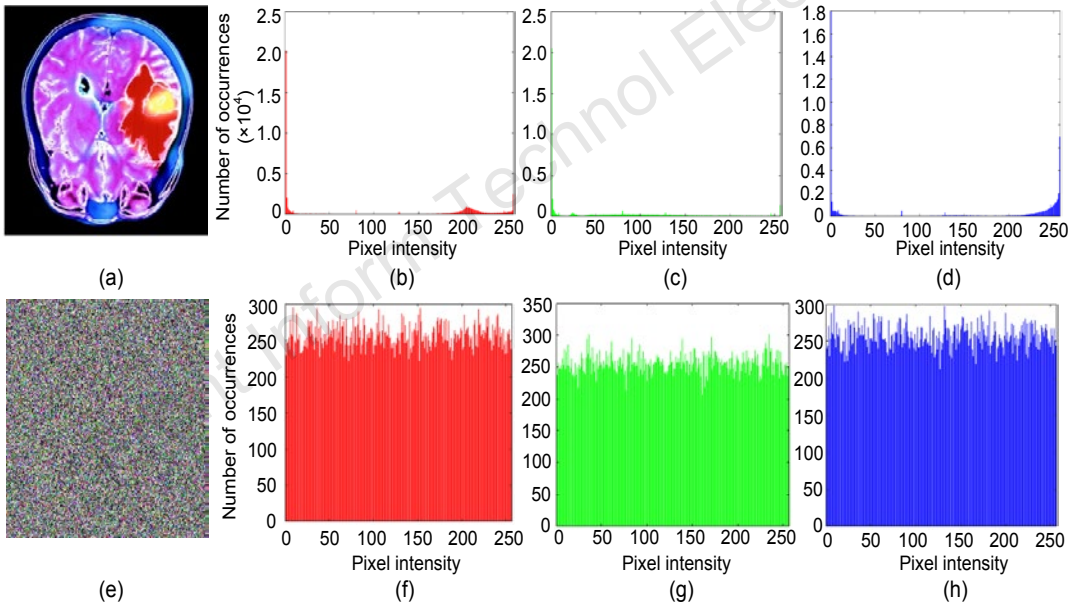


**Fig. 13 Histogram analysis of the colour DICOM image: (a) original image; (b) red plane of the original image; (c) green plane of the original image; (d) blue plane of the original image; (e) encrypted image of the original image; (f) encrypted image of the red plane; (g) encrypted image of the green plane; (h) encrypted image of the blue plane (References to colour refer to the online version of this figure)**

# Correlation coefficient & cropping attack analysis

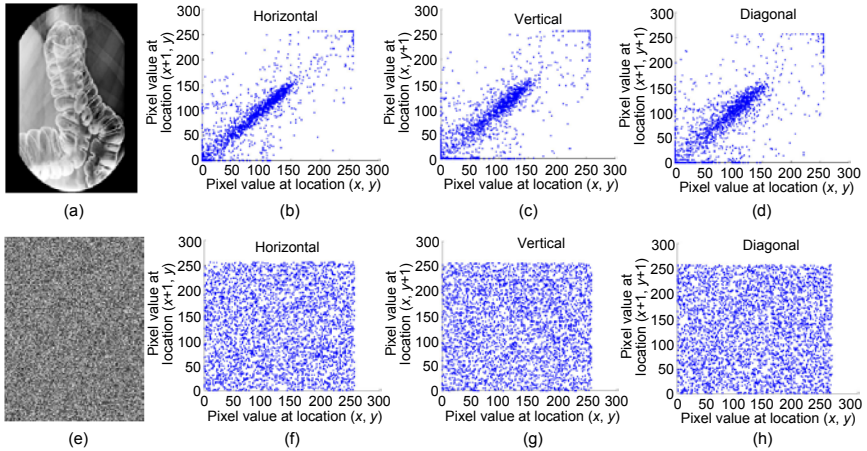


**Fig. 14 Correlation coefficient analysis of the gray DICOM image: (a) original image; (b) horizontal direction correlation of (a); (c) vertical direction correlation of (a); (d) diagonal direction correlation of (a); (e) encrypted image of (a); (f) horizontal direction correlation of (e); (g) vertical direction correlation of (e); (h) diagonal direction correlation of (e)**

**Table 4 Correlation analyses of the colour and gray DICOM images**

| Image/Plane | Type | Correlation coefficient | | |
|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal |
| Colour DICOM_R | Original | 0.9526 | 0.9620 | 0.9209 |
| | Encrypted | **0.0043** | **0.0033** | **0.0027** |
| Colour DICOM_G | Original | 0.9139 | 0.9314 | 0.8535 |
| | Encrypted | **0.0011** | **0.0047** | **0.0011** |
| Colour DICOM_B | Original | 0.9649 | 0.9727 | 0.9402 |
| | Encrypted | **0.0023** | **0.0037** | **0.0019** |
| DICOM-1 | Original | 0.9749 | 0.9766 | 0.9576 |
| | Encrypted | **−0.0013** | **−0.0033** | **0.0065** |
| DICOM-2 | Original | 0.9587 | 0.9449 | 0.9196 |
| | Encrypted | **0.0063** | **0.0047** | **−0.0012** |
| DICOM-3 | Original | 0.9635 | 0.9798 | 0.9503 |
| | Encrypted | **−0.0032** | **−0.0019** | **0.0016** |
| DICOM-4 | Original | 0.9809 | 0.9760 | 0.9603 |
| | Encrypted | **−0.0006** | **−0.0001** | **0.0015** |
| DICOM-5 | Original | 0.9898 | 0.9875 | 0.9801 |
| | Encrypted | **0.0009** | **0.0055** | **−0.0015** |

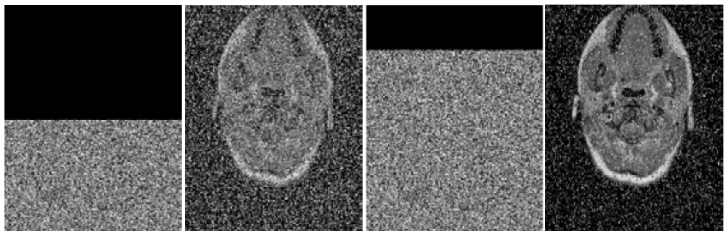


**Fig. 17 Analysis of cropping attack: (a) image with 128×256 cropped; (b) decipher of (a); (c) image with 50×256 cropped; (d) decipher of (c)**

# Key sensitivity & NIST test suite

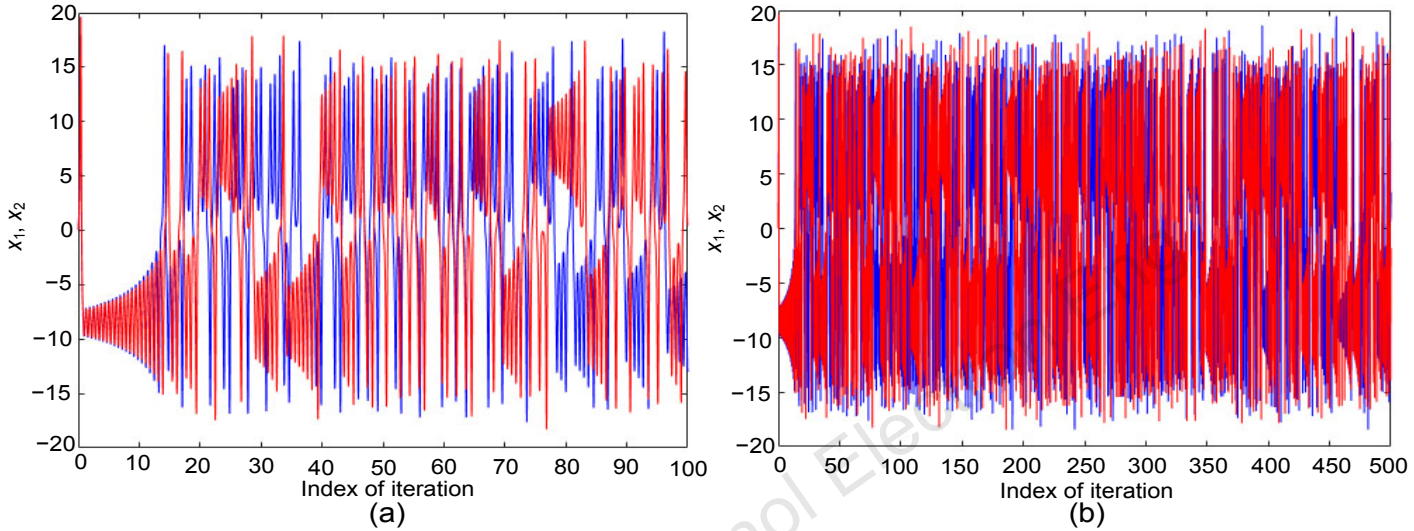


**Fig. 16 Illustration of key sensitivity with the original key set ($x_1$, red line) and key set 2 ($x_2$, blue line) for the combined Lorenz attractor for 100 (a) and 500 (b) iterations (References to colour refer to the online version of this figure)**



**Table 9 NIST test suite results**

| Test | *P* value | | | Proportion | | | Conclusion |
|---|---|---|---|---|---|---|---|
| | DICOM-1 | CLA | CLuA | DICOM-1 | CLA | CLuA | |
| Frequency | 0.3505 | 0.5341 | 0.9114 | 1.0 | 1.0 | 1.0 | Random |
| Block frequency | 0.5341 | 0.5341 | 0.7399 | 0.9 | 1.0 | 1.0 | Random |
| Cumulative sum I | 0.5341 | 0.3504 | 0.9114 | 1.0 | 1.0 | 1.0 | Random |
| Cumulative sum II | 0.0668 | 0.7399 | 0.7399 | 1.0 | 1.0 | 1.0 | Random |
| Runs | 0.5341 | 0.7391 | 0.9114 | 1.0 | 0.9 | 1.0 | Random |
| FFT | 0.7399 | 0.3504 | 0.7399 | 1.0 | 1.0 | 1.0 | Random |
| Nonoverlapping template | 0.5341 | 0.1222 | 0.3504 | 1.0 | 1.0 | 1.0 | Random |
| Overlapping template | 0.1223 | 0.9114 | 0.2133 | 1.0 | 1.0 | 1.0 | Random |
| Approximate entropy | 0.5341 | 0.9914 | 0.7399 | 1.0 | 1.0 | 1.0 | Random |
| Serial I | 0.5341 | 0.5341 | 0.3504 | 1.0 | 1.0 | 1.0 | Random |
| Serial II | 0.5341 | 0.0179 | 0.5341 | 1.0 | 1.0 | 1.0 | Random |
| Linear complexity | 0.3505 | 0.3505 | 0.7399 | 1.0 | 1.0 | 0.9 | Random |

# Performance comparison

**Table 10 Performance comparison**

| Reference | Domain | Entropy | NPCR (%) | UACI (%) | Keyspace | NIST test |
|---|---|---|---|---|---|---|
| Chen et al., 2020 | Spatial | 7.9971 | 99.62 | 33.44 | $2^{256}$ | × |
| Ravichandran et al., 2016 | Spatial | 7.9992 | 99.99 | 33.37 | $10^{168}$ | × |
| Ravichandran et al., 2017 | Spatial | 7.9972 | 99.59 | 33.43 | $10^{168}$ | × |
| Belazi et al., 2019 | Spatial | 7.9991 | 99.61 | 33.47 | $>2^{716}$ | × |
| Liu H et al., 2019b | Spatial | 7.9984 | 99.61 | 33.45 | $>2^{128}$ | × |
| Liu H et al., 2019a | Spatial | 7.9993 | 99.59 | 49.70 | $10^{112}$ | × |
| Rehman et al., 2019 | Spatial | 7.9993 | 99.61 | 33.46 | $10^{254}$ | × |
| Dagadu et al., 2019a | Spatial | 7.9994 | 99.59 | 33.41 | $>2^{128}$ | × |
| Farah et al., 2020 | Spatial | 7.9990 | 99.56 | 33.41 | $>2^{128}$ | × |
| Chai et al., 2019 | Spatial | 7.9993 | 99.58 | 33.46 | $10^{98}$ | × |
| Liu JZ et al., 2019 | Spatial | 7.9991 | 99.61 | 33.42 | $10^{74}$ | × |
| Dagadu et al., 2019b | Spatial | 7.9972 | 99.64 | 33.43 | $10^{74}$ | × |
| Dzwonkowski and Rykaczewski, 2019 | Spatial | 7.9969 | NA | NA | $2^{256}$ | × |
| Kumar et al., 2019 | Spatial | 4.7453 | 99.60 | 33.46 | $10^{60}$ | × |
| Suri and Vijay, 2020 | Spatial | 7.9519 | 99.45 | 31.35 | $>2^{128}$ | × |
| Praveenkumar et al., 2015 | Spatial | 7.9972 | 99.59 | 33.47 | $2^{269}$ | × |
| Belazi et al., 2017 | Transform | 7.9025 | 99.64 | 33.43 | $2^{208}$ | × |
| Arumugham et al., 2018 | Transform | 7.9916 | NA | NA | $2^{168}$ | × |
| Bolourian Haghighi et al., 2019 | Transform | 7.9970 | 99.61 | 33.46 | $>2^{128}$ | × |
| Luo Y et al., 2015 | Transform | 7.9820 | 99.47 | 33.37 | $10^{78}$ | × |
| Guan et al., 2019 | Transform | 7.9923 | 99.63 | 33.61 | $10^{58}$ | × |
| Aashiq Banu and Amirtharajan, 2020 | Spatial-transform | 7.9980 | 99.68 | 33.47 | $10^{238}$ | × |
| **This paper** | **Transform** | **7.9973** | **99.64** | **33.44** | $\mathbf{10^{203}}$ | ✓ |

# Conclusions

- A bio-inspired medical image encryption method is proposed which employs DNA blended with combined chaotic attractors.
- To intensify the substitution and permutation phase, a crossover and mutation process is performed.
- Statistical and differential attack analyses have been carried out to verify its security and complexity.

# References


1. Arumugham S, Rajagopalan S, Rayappan JBB, et al., 2018. Networked medical data sharing on secure medium—a web publishing mode for DICOM viewer with three layer authentication. *J Biomed Inform*, 86:90-105. https://doi.org/10.1016/j.jbi.2018.08.010
2. Belazi A, El-latif AAA, Belghith S, 2016. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process*, 128:155-170. https://doi.org/10.1016/j.sigpro.2016.03.021
3. Belazi A, El-Latif AAA, Diaconu AV, et al., 2017. Chaos- based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Opt Laser Eng*, 88:37-50. https://doi.org/10.1016/j.optlaseng.2016.07.010
4. Belazi A, Talha M, Kharbech S, et al., 2019. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access*, 7:36667-36681. https://doi.org/10.1109/ACCESS.2019.2906292
5. Bolourian Haghighi B, Taherinia AH, Mohajerzadeh AH, 2019. TRLG: fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA. *Inform Sci*, 486: 204-230. https://doi.org/10.1016/j.ins.2019.02.055
6. Chai XL, Gan ZH, Yuan K, et al., 2019. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neur Comput Appl*, 31(1):219-237. https://doi.org/10.1007/s00521-017-2993-9
7. Chen YC, Tang CM, Ye RS, 2020. Cryptanalysis and improvement of medical image encryption using high- speed scrambling and pixel adaptive diffusion. *Signal Process*, 167:107286. https://doi.org/10.1016/j.sigpro.2019.107286
8. Dagadu JC, Li JP, Addo PC, 2019a. An image cryptosystem based on pseudorandomly enhanced chaotic DNA and random permutation. *Multim Tools Appl*, 78(17): 24979- 25000. https://doi.org/10.1007/s11042-019-7693-2
9. Dagadu JC, Li JP, Aboagye EO, 2019b. Medical image encryption based on hybrid chaotic DNA diffusion. *Wirel Pers Commun*, 108(1):591-612. https://doi.org/10.1007/s11277-019-06420-z
10. Daubechies I, Sweldens W, 1998. Factoring wavelet transforms into lifting steps. *J Four Anal Appl*, 4(3):247- 269. https://doi.org/10.1007/BF02476026
11. Devi RS, Thenmozhi K, Rayappan JBB, et al., 2019. Entropy influenced RNA diffused quantum chaos to conserve medical data privacy. *Int J Theor Phys*, 58(6):1937-1956. https://doi.org/10.1007/s10773-019-04088-6
12. Dhall S, Pal SK, Sharma K, 2018. Cryptanalysis of image encryption scheme based on a new 1D chaotic system. *Signal Process*, 146:22-32. https://doi.org/10.1016/j.sigpro.2017.12.021
13. Diaconu AV, 2016. Circular inter–intra pixels bit-level permutation and chaos-based image encryption. *Inform Sci*, 355-356:314-327. https://doi.org/10.1016/j.ins.2015.10.027