Medical image encryption using high-speed scrambling and pixel adaptive diffusion

By: Hua, ZY [Hua, Zhongyuan] 1], Yi, S [Yi, Shuang] 2], Zhou, YC [Zhou, Yicong] 2]

Abstract
This paper presents a new encryption scheme of protecting medical images. It has high efficiency and shows robustness of defending some impulse noise and data loss. First, some random data are inserted into surroundings of the image. Then, two rounds of high-speed scrambling and pixel adaptive diffusion are performed to randomly shuffle neighboring pixels and spread these inserted random data over the entire image. The proposed encryption scheme can be directly applied to medical images with any representation format. We provide two kinds of operations to implement the pixel adaptive diffusion: bitwise XOR and modulo arithmetic. The former has high efficiency in hardware platforms while the latter can achieve fast speed in software platforms. Simulations and evaluations show that both encryption schemes using bitwise XOR and modulo arithmetic have high security levels, can achieve much faster speeds, and can better adapt to impulse noise and data loss interference than several typical and state-of-the-art encryption schemes. © 2017 Elsevier B.V. All rights reserved.

Keywords
Cryptosystem; Image encryption; Medical image; High-speed scrambling; Pixel adaptive diffusion

Author Information
Reprint Address: Zhou, YC (reprint author)
[2] Harbin Inst Technol, Shenzhen Grad Sch, Sch Comp Sci & Technol, Shenzhen 518055, Peoples R China
E-mail Addresses: hua Zhongyuan@hit.edu.cn; yicongzhou@umac.mo

Funding

<table>
<thead>
<tr>
<th>Funding Agency</th>
<th>Show details</th>
<th>Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Natural Science Foundation of China</td>
<td>61701317</td>
<td></td>
</tr>
<tr>
<td>Shenzhen Science and Technology Innovation Council</td>
<td>JCYJ2017030715070451</td>
<td></td>
</tr>
<tr>
<td>Macau Science and Technology Development Fund</td>
<td>FDC(V16)/2015/A1</td>
<td></td>
</tr>
<tr>
<td>Research Committee at University of Macau</td>
<td>MYRG2014-00003-FST</td>
<td>MYRG2016-00123-FST</td>
</tr>
</tbody>
</table>

Publisher
ELSEVIER SCIENCE BV, PO BOX 211, 1000 AE AMSTERDAM, NETHERLANDS

Journal Information
Performance Trends: Essential Science Indicators
Impact Factor: Journal Citation Reports

Categories / Classification
Research Areas: Engineering
Web of Science Categories: Engineering, Electrical & Electronic

See more data fields
### Cited References: 47

Showing 30 of 47  
[View All in Cited References page](#)

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Times Cited</th>
<th>Authors</th>
<th>Journal</th>
<th>Volume, Issue, Pages</th>
<th>Published Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Some basic cryptographic requirements for chaos-based cryptosystems</td>
<td>630</td>
<td>Alvarez, Gonzalo; Li, Shujun</td>
<td>INTERNATIONAL JOURNAL OF BIFURCATION AND CHAOS</td>
<td>Volume: 16, Issue: 8, Pages: 2232-2151</td>
<td>August 2006</td>
</tr>
<tr>
<td>2.</td>
<td>Cryptanalysis of a Classical Chaos-Based Cryptosystem with Some Quantum Cryptography Features</td>
<td>6</td>
<td>Arroyo, David; Hernandez, Fernando; Orue, Amaia B.</td>
<td>INTERNATIONAL JOURNAL OF BIFURCATION AND CHAOS</td>
<td>Volume: 27, Issue: 1, Article Number: 1750004</td>
<td>January 2017</td>
</tr>
<tr>
<td>5.</td>
<td>The strict avalanche criterion randomness test</td>
<td>24</td>
<td>Castro, JCH; Sierra, JM; Zemczuk, A.; et al.</td>
<td>MATHEMATICS AND COMPUTERS IN SIMULATION</td>
<td>Volume: 68, Issue: 1, Pages: 1-7</td>
<td>February 2005</td>
</tr>
<tr>
<td>6.</td>
<td>A novel chaos-based image encryption algorithm using DNA sequence operations</td>
<td>116</td>
<td>Chai, Xiuli; Chen, Yiran; Brody, Lucie</td>
<td>OPTICS AND LASERS IN ENGINEERING</td>
<td>Volume: 88, Pages: 197-213</td>
<td>January 2017</td>
</tr>
<tr>
<td>7.</td>
<td>A visually secure image encryption scheme based on compressive sensing</td>
<td>46</td>
<td>Chai, Xiuli; Gan, Zhihua; Chen, Yiran; et al.</td>
<td>SIGNAL PROCESSING</td>
<td>Volume: 134, Pages: 35-51</td>
<td>May 2017</td>
</tr>
<tr>
<td>9.</td>
<td>Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption</td>
<td>53</td>
<td>Chen, Jian; Zhu, Zhi-liang; Zhang, Li-bao; et al.</td>
<td>SIGNAL PROCESSING</td>
<td>Volume: 142, Pages: 340-353</td>
<td>January 2018</td>
</tr>
<tr>
<td>10.</td>
<td>A New Quaternion-Based Encryption Method for DICOM Images</td>
<td>16</td>
<td>Dzwonkowski, Mariusz; Papaj, Michal; Rylakowski, Roman</td>
<td>IEEE TRANSACTIONS ON IMAGE PROCESSING</td>
<td>Volume: 24, Issue: 11, Pages: 4614-4622</td>
<td>November 2015</td>
</tr>
<tr>
<td>13.</td>
<td>Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique</td>
<td>46</td>
<td>Gong, Liuhua; Liu, Xingbin; Zheng, Fen; et al.</td>
<td>JOURNAL OF MODERN OPTICS</td>
<td>Volume: 60, Issue: 13, Pages: 1074-1082</td>
<td>July 2013</td>
</tr>
<tr>
<td>14.</td>
<td>Designing Hyperchaotic Cat Maps With Any Desired Number of Positive Lyapunov Exponents</td>
<td>9</td>
<td>Hua, Zhongyan; Yi, Shuang; Zhou, Yicong; et al.</td>
<td>IEEE TRANSACTIONS ON CYBERNETICS</td>
<td>Volume: 48, Issue: 2, Pages: 463-473</td>
<td>February 2018</td>
</tr>
<tr>
<td>15.</td>
<td>Design of image cipher using block-based scrambling and image filtering</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
16. **Image encryption using 2D Logistic-adjusted-Sine map**
   By: Hua, Zhongyun; Zhou, Yicong
   INFORMATION SCIENCES Volume: 396 Pages: 97-113 Published: AUG 2017

17. **2D Sine Logistic modulation map for image encryption**
   By: Hua, Zhongyun; Zhou, Yicong; Pan, Chi-Man et al.
   INFORMATION SCIENCES Volume: 339 Pages: 237-253 Published: APR 2021

18. **Title [not available]**
   By: Hutter, T; Pemshaber, M.; Hammerle-Uhl, J.; et al.
   Weaknesses in Security Considerations Related to Chaos-Based Image Encryption Published: 2016
   Publisher: Springer
   [Show additional data]

19. **Medical image retrieval based on knowledge-assisted text and image indexing**
   By: Labaste, Caroline; Lim, Joe; Hwee Chevallet, Jean-Pierre; et al.
   IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY Volume: 17 Issue: 7 Pages: 889-900 Published: JUL 2007

20. **Medical Image File Formats**
   By: Lambina, Michele; Marino, Loredana
   JOURNAL OF DIGITAL IMAGING Volume: 27 Issue: 2 Pages: 200-206 Published: APR 2014

21. **Cryptanalyzing an Image Scrambling Encryption Algorithm of Pixel Bits**
   By: Li, Chengqing; Lin, Dengdong; Lu, Jinhui
   IEEE MULTIMEDIA Volume: 24 Issue: 3 Pages: 64-71 Published: JUL-SEP 2017

22. **Breaking a novel image encryption scheme based on improved hyperchaotic sequences**
    By: Li, Chengqing; Liu, Yaansheng; Xie, Tao; et al.
    NONLINEAR DYNAMICS Volume: 73 Issue: 3 Pages: 2083-2089 Published: AUG 2013

23. **Cracking a hierarchical chaotic image encryption algorithm based on permutation**
    By: Li, Chengqing
    SIGNAL PROCESSING Volume: 118 Pages: 203-210 Published: JAN 2016

24. **Modified computational integral imaging-based double image encryption using fractional Fourier transform**
    By: Li, Xiao-Wei; Lee, In Hwan
    OPTICS AND LASERS IN ENGINEERING Volume: 66 Pages: 112-121 Published: MAR 2015

25. **Image encryption using DNA complementary rule and chaotic maps**
    By: Liu, Honggu; Wang, Xingyuan; Kadir, Abdurahman
    APPLIED SOFT COMPUTING Volume: 12 Issue: 5 Pages: 1457-1466 Published: MAY 2012

26. **Introduction to the DICOM standard**
    By: Mildenberger, P; Eichelberg, M; Martin, E
    EUROPEAN RADIOLOGY Volume: 12 Issue: 4 Pages: 920-927 Published: APR 2002

27. **Image encryption based on non-affine and balanced cellular automata**
    By: Ping, Ping; Xu, Feng; Wang, Zhi-Jian
    SIGNAL PROCESSING Volume: 105 Pages: 419-429 Published: DEC 2014

28. **Synchronization of Markovian jumping inertial neural networks and its applications in image encryption**
    By: Prakash, M.; Balasubramaniam, P; Lakshmanan, S.
    NEURAL NETWORKS Volume: 83 Pages: 86-93 Published: NOV 2016

29. **Image Encryption With Multorders of Fractional Fourier Transforms**
    By: Tao, Ran; Meng, Xiang-Yi; Wang, Yue
    IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY Volume: 5 Issue: 4 Pages: 734-738 Published: DEC 2010

30. **A chosen-plaintext attack on the Microsoft BASIC protection**
    By: van den Assem, R.; van Elk, W.J.
    Computers & Security Volume: 5 Issue: 1 Pages: 36-45 Published: March 1986

Showing 30 of 47  View All Cited References page