

A Review of Image Scrambling Technique Using Chaotic Maps

Shafali Agarwal*

Independent Researcher, Los Angeles, California, USA.

Received 12 September 2017; received in revised form 09 November 2017; accepted 07 December 2017

Abstract

Image scrambling is a process to convert a meaningful image into an unidentifiable or an unordered image by changing the pixel position such that an unauthorized user should not be able to access the original contents. The paper summarizes the various chaotic maps based scrambling methods with their performance measures. The discussion focuses on the scrambling techniques like Arnold map, Affine map, Baker map, Henon map, Logistic map, Fibonacci sequence, Fibonacci-Lucas sequence, and Fibonacci P-code transformation used to shuffle the image pixels in various image encryption algorithms. Each scrambling method is observed by using the adjacent pixels correlation coefficient, NPCR and UACI, scrambling/unsrambling speed, mean value analysis, entropy and peak signal-noise ratio. A comparative table is used to represent the reasonable computational outcome of each analysis parameter. The relative analysis of the performance and security measure highlights the weakness and strength of discussing scrambling techniques and can be used in the case-based image cryptosystem in future research.

Keywords: image scrambling, chaotic map, performance parameters, scrambled image

References

- [1] M. Khan and T. Shah, "A literature review on image encryption techniques," 3D Research, vol. 5, no. 4, p. 29, December 2014.
- [2] F. S. Abed, "A new approach to encoding and hiding information in an image," International Journal of Computer Science Issues, vol. 8, no. 5, pp. 514-523, September 2011.
- [3] J. Fridrich, Method for encrypting and decrypting data using chaotic map, U.S. Patent, 6,064,738, May 16, 2000.
- [4] R. C. Hilborn, Chaos and nonlinear dynamics: an introduction to scientists and engineers, 2nd ed. New York: Oxford University Press, 2001.
- [5] X. Wu, H. Hu, and B. Zhang, "Parameter estimation only from symbolic sequence generated by chaos system," Chaos Soliton & Fractals, vol. 22, no. 2, pp. 359-366, October 2004.
- [6] R. Rhouma and S. Belghith, "Cryptanalysis of a spatiotemporal chaotic cryptosystem," Chaos Solitons & Fractals, vol. 41, no. 4, pp. 1718-1722, August 2009.
- [7] L. Shujun and X. Zheng, "Cryptanalysis of a chaotic image encryption method," IEEE International Symp. Circuits and Systems (ISCAS 2002), vol. 2, pp. 708-711, 2002.
- [8] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," Optics & Laser Technology, vol. 101, pp. 30-41, May 2018.
- [9] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Philip, "2D sine logistic modulation map for image encryption," Information Science, vol. 297, pp. 80-94, March 2015.
- [10] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," Information Science, vol. 339, pp. 237-253, April 2016.
- [11] J. M. Vilarly, C. J. Jimenez, and R. Perez, "Image encryption using the Gyration transform and random phase masks generated by using chaos," Journal of Physics: Conference Series, vol. 850, pp. 012012-1-012012-7, 2017.

* Corresponding author. E-mail address: shafali.agarwal@gmail.com

- [12] X. Y. Wang, S. Wang, Y. Zhang, and K. Guo, "A novel image encryption algorithm based on chaotic shuffling method," *Information Security Journal: A Global Perspective*, vol. 26, no. 1, pp. 7-16, 2017.
- [13] M. Kanafchian and B. Fathi-Vajargah, "A novel image encryption scheme based on Clifford attractor and noisy logistic map for secure transferring images in navy," *International Journal of e-Navigation and Maritime Economy*, vol. 6, pp. 53-63, April 2017.
- [14] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic map," *Optics and Lasers in Engineering*, vol. 96, pp. 39-49, September 2017.
- [15] M. Mikhail, Y. Abouelseoud, and G. ElKobrosy, "Two-phase image encryption scheme based on FFCT and fractals," *Security and Communication Networks*, vol. 2017, pp. 7367518-1-7367518-13, 2017.
- [16] H. Oğraş and M. Türk, "A robust chaos-based image cryptosystem with an improved key generator and plain image sensitivity mechanism," *Journal of Information Security*, vol. 8, no. 1, pp. 23-41, January 2017.
- [17] Y. Sun, L. Chen, R. Xu, and R. Kong, "An image encryption algorithm utilizing julia sets and hilbert curves," *PLoS ONE*, vol. 9, no. 1, January 2014.
- [18] Q. Zhang, S. Zhou, and X. Wei, "An efficient approach for DNA fractal-based image encryption," *Applied Mathematics & Information Sciences*, vol. 5, no. 3, pp. 445-459, 2011.
- [19] G. A. Sathishkumar, K. B. Bagan, and N. Sriraam, "Image encryption based on diffusion and multiple chaotic maps," *International Journal of Network Security and its Applications*, vol. 3 no. 2, pp. 181-194, March 2011.
- [20] Y. Xu, H. Wang, Y. Li, and B. Pei, "Image encryption based on synchronization of fractional chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3735-3744, October 2014.
- [21] M. Ahmad, U. Shamsi, and I. R. Khan, "An enhanced image encryption algorithm using fractional chaotic systems," *Procedia Computer Science*, vol. 57, pp. 852-859, 2015.
- [22] M. Kumar, P. Powduri, and A. Reddy, "An RGB image encryption using diffusion process associated with chaotic map," *Journal of Information Security and Applications*, Elsevier, vol. 21, pp. 20-30, April 2015.
- [23] N. K. Pareek, V. Patidar, and K. K. Sud, "Substitution-diffusion based image cipher," *International Journal of Network Security & Its Applications*, vol. 3, no. 2, pp. 149-160, March 2011.
- [24] J. X. Chen, Z. L. Zhu, C. Fu, H. Yu, and L. B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variable selection mechanism," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 3, pp. 846-860, March 2014.
- [25] M. Prasad and K. L. Sudha, "Chaos image encryption using pixel shuffling," *Computer Science & Information Technology*, pp. 169-179, 2011.
- [26] N. K. Pareek, "Design and analysis of novel digital image encryption scheme," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, pp. 95-108, March 2012.
- [27] H. J. Liu and X. Y. Wang, "Colour image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320-3327, May 2010.
- [28] S. Sathyanarayana, M. Kumar, and K. Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points," *International Journal of Network Security*, vol. 12, no. 3, pp. 137-150, 2011.
- [29] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "Hash key - based image encryption using crossover operator and chaos," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4753-4769, April 2016.
- [30] D. I. G. Amalarethinam and J. S. Geetha, "Image encryption and decryption in public key cryptography based on MR," *International Conf. Computing and Communications Technologies*, IEEE Press, February 2015, pp. 133-138.
- [31] Z. Hua, Y. Wang, and Y. Zhou, "Image cipher using a new interactive two-dimensional chaotic map," *IEEE International Conf. Systems, Man, and Cybernetics*, IEEE Press, October 2015, pp. 1804-1808.
- [32] Z. Hua, B. Zhou and Y. Zhou, "Image content-based encryption algorithm using high-dimensional chaotic system," *International Symp. Nonlinear Theory and its Applications*, December 2015, pp. 554-557.
- [33] H. Liu and C. Jin, "A color image encryption scheme based on Arnold scrambling and quantum chaotic," *International Journal of Network Security*, vol. 19, no. 3, pp. 347-357, May 2017.
- [34] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *Springerplus*, vol. 5, no. 289, pp. 1-12, March 2016.
- [35] Y. Wu, Y. Zhou, S. Aгаian, and J. P. Noonan, "2D Sudoku associated bijections for image scrambling," *Information Sciences*, vol. 327, pp. 91-109, January 2016.

- [36] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Information Sciences*, vol. 396, pp. 97-113, August 2017.
- [37] N. Dwivedi, R. K. Gupta, and S. Agarwal, "Image encryption using curved scrambling and diffusion," *International Journal of Engineering and Technology*, vol. 8, no. 6, pp. 2990-2996, January 2017.
- [38] S. Somaraj and M. A. Hussain, "Image encryption using edge map and key image", *Indian Journal of Science and Technology*, vol. 10, no. 4, pp. 1-4, January 2017.
- [39] J. S. Teh and A. Samsudin, "A chaos-based authenticated cipher with associated data," *Security and Communication Networks*, vol. 2017, pp. 9040518-1-9040518-15, 2017.
- [40] V. I. Arnold, "First steps in symplectic topology," *Russian Math. Surveys*, vol. 41, no. 6, pp. 1-21, 1986.
- [41] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, July 2004.
- [42] Z. Tang, and X. Zhang, "Secure image encryption without size limitation using Arnold transform and random strategies," *Journal of Multimedia*, vol. 6, no. 2, pp. 202-206, 2011.
- [43] A. Chopra, M. Ahmad, and M. Malik, "An enhanced modulo-based image encryption using chaotic and fractal keys," *International Conf. Advances in Computer Engineering and Applications*, July 2015, pp. 501-506.
- [44] A. Nag, J. P. Singh, S. Khan, S. Biswas, D. Sarkar, and P. P. Sarkar, "Image encryption using affine transform and XOR operation," *Proc. Signal Processing, Communication, Computing and Networking Technologies*, IEEE Press, September 2011, pp. 309-312.
- [45] Y. Dong, J. Liu, C. Zhu, and Y. Wang, "Image encryption algorithm based on chaotic mapping," *Proc. Computer Science and Information Technology*, IEEE Press, January 2011, pp 289-291.
- [46] S. Kumar, B. Sinha, and C. Pradhan, "Comparative analysis of color image encryption using 2D chaotic maps," *Information Systems Design and Intelligent Applications*, vol. 2, pp. 79-387, 2015.
- [47] D. Qi, J. Zou, and X. Han, "A new class of transform and its application in the image transform covering," *Science in China Series E: Technological Sciences*, vol. 43, no. 3, pp. 304-312, June 2000.
- [48] M. Mishra, P. Mishra, M. C. Adhikary, and S. Kumar, "Image encryption using Fibonacci-Lucas transformation," *International Journal on Cryptography and Information Security*, vol. 2, no. 3, pp. 131-141, September 2012.
- [49] Y. Zhou, S. Aгаian, V. M. Joyner, and K. Panetta, "Two Fibonacci p-code based image scrambling algorithms," *Proc. SPIE 6812 Image Processing: Algorithms and Systems VI*, vol. 6812, March 2008, p. 681215.
- [50] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172-182, April 2014.
- [51] Y. Wu, J. P. Noonan, and S. Aгаian, "NPCR and UACI randomness tests for image encryption," *Journal of Selected Areas in Telecommunication*, vol. 2, pp. 31-38, April 2011.
- [52] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, October 1949.