A Hybrid Whale Optimization Algorithm with Chaotic Maps for Secure Cryptographic Key Generation

Neeraj Kumar Jha; Yogesh Sonvane; Deepa Barethiya
Dept. of MCA, G H Raisoni College of Engineering and Management, Nagpur, India

Anupam Chaube
Dept. of Sci. & Tech., G H Raisoni College of Engineering and Management, Nagpur, India

Abstract:
Data security depends on the generation of cryptographic keys, which must be unpredictable and resistant to cryptanalytic attacks. This research introduces a unique Hybrid Whale Optimization Algorithm with Chaotic Maps (HWOA-CM) for secure cryptographic key creation. The classic Whale Optimization Algorithm (WOA) exhibits good exploration and exploitation capabilities but may suffer from early convergence and limited unpredictability. We tackle this by incorporating chaotic maps into WOA to boost security, increase diversity, and improve search effectiveness. The chaotic sequences influence population initialization and adaptive parameter tuning, introducing high sensitivity to initial conditions and preventing predictability in key generation. Experimental results demonstrate that the proposed HWOA-CM approach generates highly unpredictable, non-repetitive, and cryptographically strong keys, validated through statistical randomness tests and security analysis. Comparisons with conventional key generation methods highlight its superiority in terms of entropy, key space, and resistance to cryptographic attacks. This research establishes HWOA-CM as a promising approach for enhancing the security of encryption systems.

Keywords:
WOA, HWOA-CM, Cryptographic keys, Benchmarks Functions, Cryptanalytic.

1. Introduction

Cryptographic security is crucial in the digital era to shield personal information from hackers and illegal access. The creation of robust cryptographic keys is a basic element of secure encryption systems. Traditional key generation methods sometimes rely on pseudo-random number generators (PRNGs),
which may have vulnerabilities and patterns that adversaries could exploit. Metaheuristic optimization techniques have been investigated as potential substitutes to improve the security and unpredictable nature of key creation.

The Whale Optimization Algorithm (WOA) is a bio-inspired metaheuristic that imitates humpback whales' communal hunting style. Because of its balanced exploration and exploitation processes, it has proven to be incredibly effective in solving optimization problems. However, standard WOA can suffer from issues such as premature convergence, stagnation in local optima, and limited randomness, making it less suitable for cryptographic key generation.

To overcome these limitations, this paper proposes a Hybrid Whale Optimization Algorithm with Chaotic Maps (HWOA-CM) for cryptographic key generation. Chaotic maps introduce nonlinearity and ergodicity, ensuring high randomness and unpredictability in the generated keys. By integrating chaotic sequences into WOA, the proposed approach enhances the diversity of the search process, improves key randomness, and increases resistance to cryptanalytic attacks.

This study evaluates the effectiveness of HWOA-CM by analyzing its randomness, key space, and security properties using standard statistical tests. Comparative analysis with conventional methods demonstrates that the proposed approach significantly improves the unpredictability and robustness of cryptographic key generation.

DOI: https://doi.org/10.5281/zenodo.18372972

ISSN NO-2584-2706

2. Literature Review

Creating cryptographic keys is a crucial part of secure communication; these keys need to be extremely resilient and unpredictable to withstand cryptanalytic attacks.Many approaches have been investigated over time to increase key security, including conventional pseudo-random number generators (PRNGs), chaos-based strategies, and bio-inspired optimization algorithms. An overview of current methods is given in this part, along with the reasons for combining chaotic maps with the Whale Optimization Algorithm (WOA) for safe cryptographic key creation.

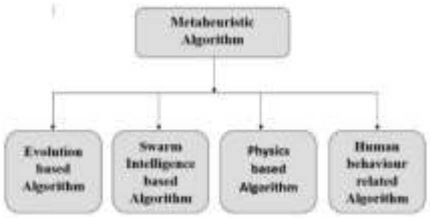


Fig 1. Classification of Metaheuristic Algorithm.

Reference No.	Algorithm Name	Author Name	Year
1	Fruit Fly Optimization	W. Y. Lin	2016
2		Y. Cheng et al	2018
3	Hybrid Ant Colony	X. Wang et al	2018
4	Global Optimization	I. E. Grossmann	1996
5		R. V. Rao et al	2016
6	Grey Wolf Optimization	M. El-Kenawy	2020
7	Particle Swarm Optimization	M. Nouiri et al	2018
8	Multi-objective Optimization	Y. Li et al	2018
9	Harris Hawks Optimizer	D. Yousri et al	2020
10	Genetic Programming	R. Al-Hajj et al	2017
11	Evolutionary Computing	R. Al-Hajj et al	2016
12	Classical & non-classical	R. A. Meyers	2000
13	Quadratic Programming	N. Steffan at al	2012
14	Grasshopper Optimization	M. Mafarja et al	2018
15	Water Cycle	A. A. Heidari et al	2017

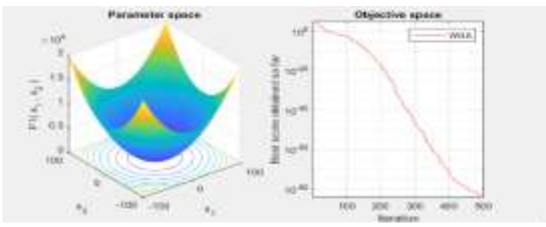
Table 1. Literature Review

Functions	Dimensions	Range	f_{min}
$F_1(S)=\sum_{m=1}^{d} S_m^2$	(10,30,50,100)	[-100 , 100]	0
$F_2(S)=\sum_{m=1}^{d}\lvert S_m\rvert+\prod_{m=1}^{d}\lvert S_m\rvert$	(10,30,50,100)	[-10 ,10]	0
$F_3(S)=\sum_{m=1}^{d}(\sum_{n=1}^{m} S_n)^2$	(10,30,50,100)	[-100 , 100]	0
$F_4(S)=\max_m\{\lvert S_m\rvert, 1\le m\le d\}$	(10,30,50,100)	[-100 , 100]	0
$F_5(S)=\sum_{m=1}^{d-1}[100(S_{m+1}-S_m^2)^2+(S_m-1)^2]$	(10,30,50,100)	[-30 , 30]	0
$F_6(S)=\sum_{m=1}^{d}([S_m+0.5])^2$	(10,30,50,100)	[-100 , 100]	0
$F_7(S)=\sum_{m=1}^{d} mS_m^4+random[0,1)$	(10,30,50,100)	[-1.28, 1.28]	0
$F_8(S)=\sum_{m=1}^{d}-S_m\sin(\sqrt{\lvert S_m\rvert})$	(10,30,50,100)	[-500,500]	-418.98295
$F_9(S)=\sum_{m=1}^{d}[S_m^2-10\cos(2\pi S_m)+10]$	(10,30,50,100)	[-5.12,5.12]	0
$F_{10}(S)=-20\exp(-0.2\sqrt{(\frac{1}{d}\sum_{m=1}^{d}S_m^2)})-\exp(\frac{1}{d}\sum_{m=1}^{d}\cos(2\pi S_m))+20+e$	(10,30,50,100)	[-32,32]	0
$F_{11}(S)=1+\sum_{m=1}^{d}\frac{S_m^2}{4000}-\prod_{m=1}^{d}\cos\frac{S_m}{\sqrt{m}}$	(10,30,50,100)	[-600, 600]	0
$F_{12}(S)=\frac{\pi}{d}\{10\sin(\pi r_1)+\sum_{m=1}^{d-1}(r_m-1)^2[1+10\sin^2(\pi r_{m+1})]+(r_d-1)^2\}+\sum_{m=1}^{d}u(S_m,10,100,4)$ $r_m=1+\frac{S_m+1}{4}$ $u(S_m,k,x,i)=\begin{cases}x(S_m-k)^i & S_m>k\\ 0 & -k<S_m<k\\ x(-S_m-k)^i & S_m<-k\end{cases}$	(10,30,50,100)	[-50,50]	0
$F_{13}(S)=0.1\{\sin^2(3\pi S_1)+\sum_{m=1}^{d}(S_m-1)^2[1+\sin^2(3\pi S_m+1)]+(s_d-1)^2[1+\sin^2 2\pi S_d]\}$	(10,30,50,100)	[-50,50]	0

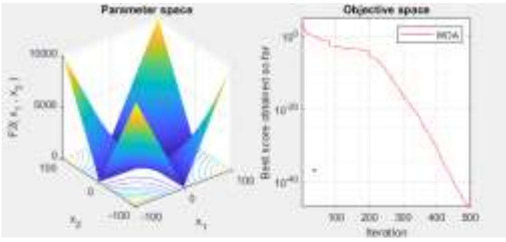
Functions	Dimensions	Range	f_{min}
$F_{14}(S)=(\frac{1}{500}+\sum_{n=1}^{25}\frac{1}{n+\sum_{m=1}^{2}(S_m-a_{mn})^6})^{-1}$	2	[-65.536, 65.536]	1
$F_{15}(S)=\sum_{m=1}^{11}[a_m-\frac{S_1(b_m^2+b_mS_2)}{b_m^2+b_mS_3+S_4}]^2$	4	[-5,5]	0.00030
$F_{16}(S)=4S_1^2-2.1S_1^4+\frac{1}{3}S_1^6+S_1S_2-4S_2^2+4S_2^4$	2	[-5,5]	-1.0316
$F_{17}(S)=(S_2-\frac{5.1}{4\pi^2}S_1^2+\frac{5}{\pi}S_1-6)^2+10(1-\frac{1}{8\pi})\cos S_1+10$	2	[-5,5]	0.398
$F(S)=[1+(S_1+S_2+1)^2(19-14S_1+3S_1^2-14S_2+6S_1S_2+3S_2^2)]\times[30+(2S_1-3S_2)^2(18-32S_1+12S_1^2+48S_2-36S_1S_2+27S_2^2)]$	2	[-2,2]	3
$F_{18}(S)=-\sum_{m=1}^{4}d_m\exp(-\sum_{n=1}^{3}S_{mn}(S_n-q_{mn})^2)$	3	[1,3]	-3.32
$F_{20}(S)=-\sum_{m=1}^{4}d_m\exp(-\sum_{n=1}^{6}S_{mn}(S_n-q_{mn})^2)$	6	[0,1]	-3.32
$F_{21}(S)=-\sum_{m=1}^{5}[(S-b_m)(S-b_m)^T+d_m]^{-1}$	4	[0,10]	-10.1532
$F_{22}(S)=-\sum_{m=1}^{7}[(S-b_m)(S-b_m)^T+d_m]^{-1}$	4	[0, 10]	-10.4028
$F_{23}(S)=-\sum_{m=1}^{7}[(S-b_m)(S-b_m)^T+d_m]^{-1}$	4	[0, 10]	-10.5363

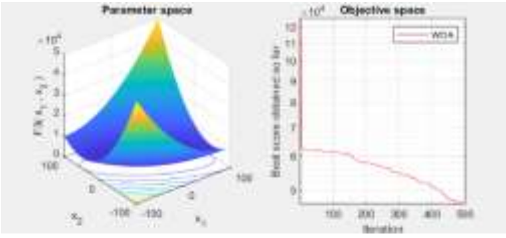
Table 2. Standard UM Benchmark Functions.

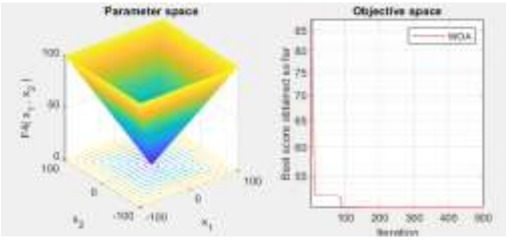
3. Result and Discussion

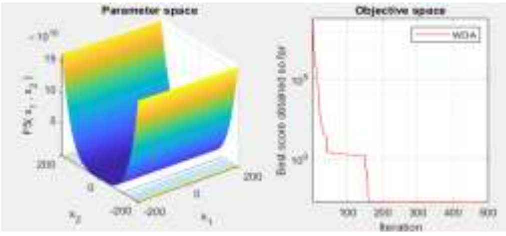


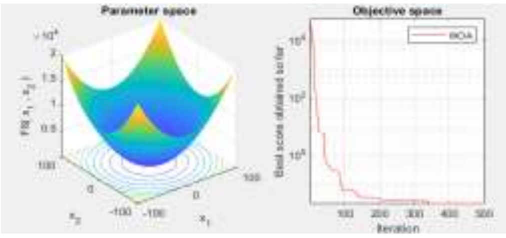
DOI: https://doi.org/10.5281/zenodo.18372972

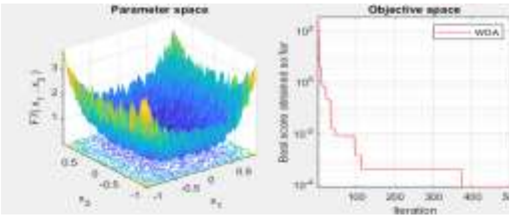


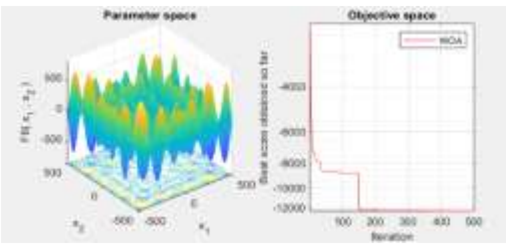


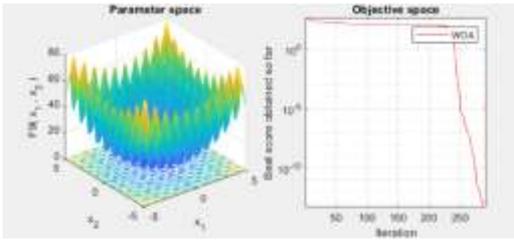


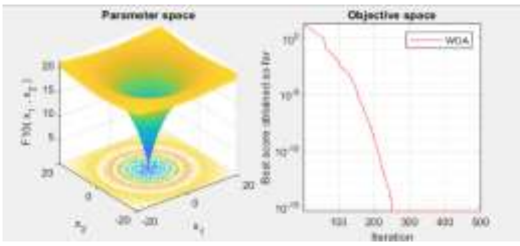


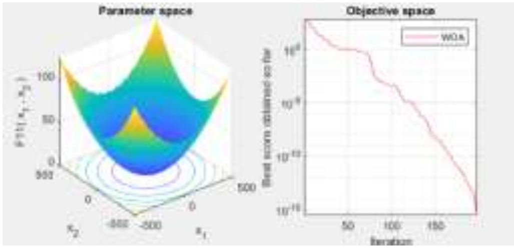


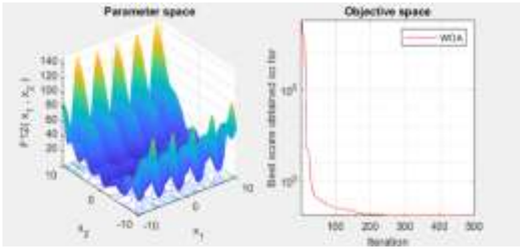


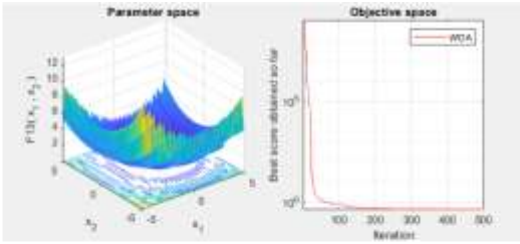


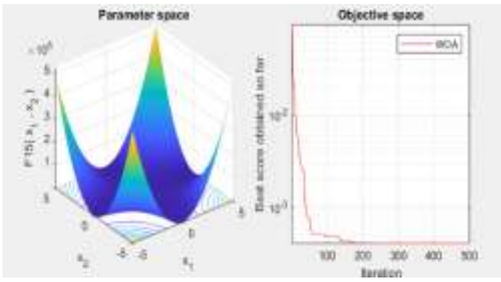




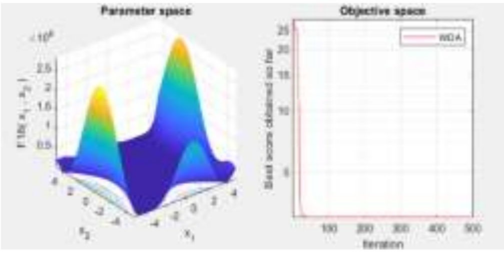


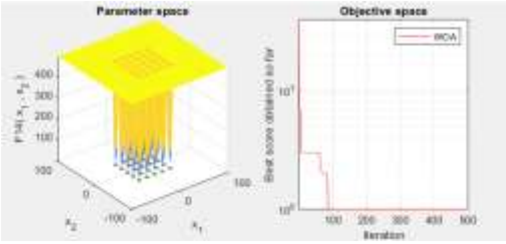


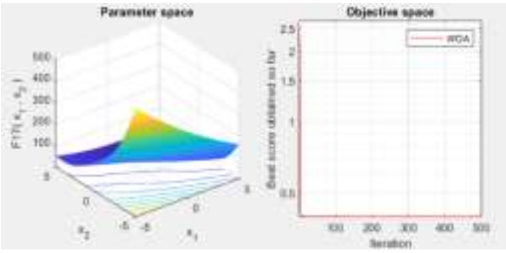


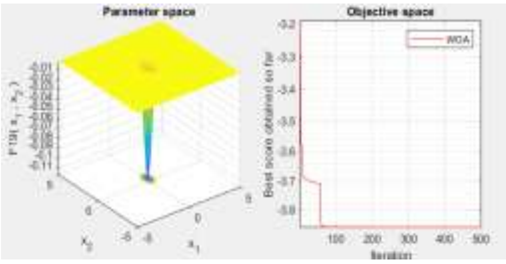


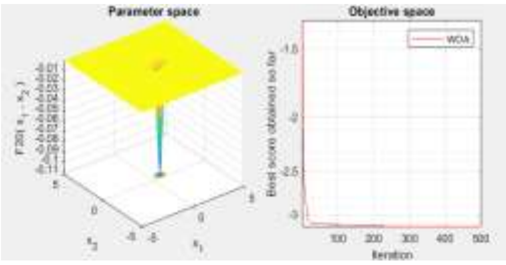
DOI: https://doi.org/10.5281/zenodo.18372972

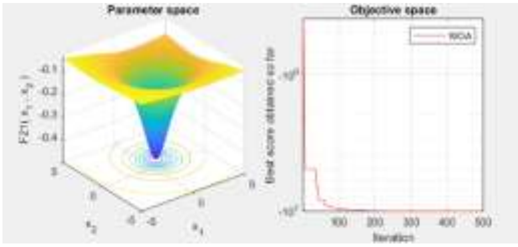


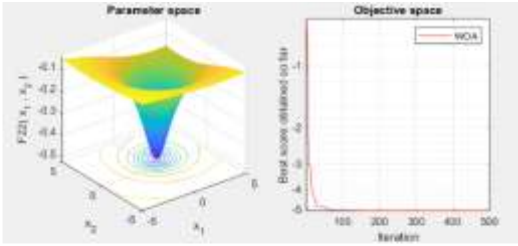












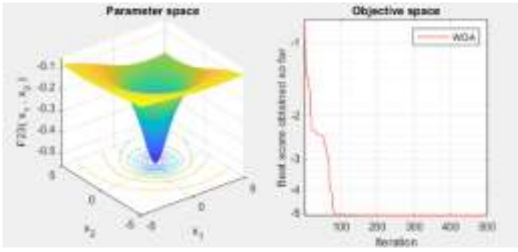


Fig 2: Search Space for Benchmark Functions applied on Hybrid WOA & Chaotic Maps Algorithm

FUNCTION NUMBER	ORIGINAL VALUES	CHAOTIC MAPS
F1	7.2012e-85	2.7 608E-79
F2	2.8055e-53	3.9068e-48
F3	46531.249	2.303
F4	50.152	0.0016774
F5	27.4197	0.49865
F6	0.3242	0.0029256
F7	0.00085143	0.0013083
F8	-12332.6161	-12569.4866
F9	0	5.6843e-14
F10	4.4409e-16	3.9968e-15
F11	0	0
F12	0.014063	0.00047752
F13	0.41996	0.0087351
F14	0.998	1.992
F15	0.00040806	0.00039241
F16	-0.0316	-1.0316
F17	0.39802	0.39789
F18	3	3
F19	-3.8613	-3.8623
F20	-3.1538	-2.8362
F21	-10.1302	-10.0294
F22	-5.0875	-10.3703
F23	-5.1268	-10.2468

Table 3. Results for Original WOA with Chaotic Maps

DOI: https://doi.org/10.5281/zenodo.18372972

ISSN NO-2584-2706

4. Conclusion

Hybridization of Whale Optimization Algorithm (WOA) with Chaotic maps was tested on 23 Benchmark functions(F1-F23) out of which it performs better and provides optimal values in 15 functions which was F3, F4 F5, F6, F8, F12, F13, F15, F16, F17, F19, F22, F23.

5.References

[1] W. Y. Lin, "A novel 3D fruit fly optimization algorithm and its applications in economics," Neural Compute. Appl., 2016, doi: 10.1007/s00521-015-1942-8.

[2] Y. Cheng, S. Zhao, B. Cheng, S. Hou, Y. Shi, and J. Chen, "Modelling and optimization for collaborative business process towards IoT applications," Mob. Inf. Syst., 2018, doi: 10.1155/2018/9174568.

[3] X. Wang, T. M. Choi, H. Liu, and X. Yue, "A novel hybrid ant colony optimization algorithm for emergency transportation problems during post-disaster scenarios," IEEE Trans. Syst. Man, Cybern. Syst., 2018, doi: 10.1109/TSMC.2016.2606440.

[4] I. E. Grossmann, Global Optimization in Engineering Design (Nonconvex Optimization and Its Applications), vol. 9. 1996.

[5] R. V. Rao and G. G. Waghmare, "A new optimization algorithm for solving complex constrained design optimization problems," vol. 0273, no. April, 2016, doi: 10.1080/0305215X.2016.1164855.

[6] E.-S. M. El-Kenawy, M. M. Eid, M. Saber, and A. Ibrahim, "MbGWO-SFS: Modified Binary Grey Wolf Optimizer Based on Stochastic Fractal Search for Feature Selection," IEEE Access, 2020, doi: 10.1109/access.2020.3001151.

[7] M. Nouiri, A. Bekrar, A. Jemai, S. Niar, and A. C. Ammari, "An effective and distributed particle swarm optimization algorithm for flexible job-shop scheduling problem," J. Intell. Manuf., 2018, doi: 10.1007/s10845-015-1039-3.

[8] Y. Li, J. Wang, D. Zhao, G. Li, and C. Chen, "A two-stage approach for combined heat and power economic emission dispatch: Combining multi-objective optimization with integrated decision making," Energy, 2018, doi: 10.1016/j.energy.2018.07.200.

[9] D. Yousri, T. S. Babu, and A. Fathy, "Recent methodology-based Harris hawks optimizer for designing load frequency control incorporated in multi-interconnected renewable energy plants," Sustain. Energy, Grids Networks, 2020, doi: 10.1016/j.segan.2020.100352.

[10] R. Al-Hajj and A. Assi, "Estimating solar irradiance using genetic programming technique and meteorological records," AIMS Energy, 2017, doi: 10.3934/energy.2017.5.798.

[11] R. Al-Hajj, A. Assi, and F. Batch, "An evolutionary computing approach for estimating global solar radiation," in 2016 IEEE International Conference on Renewable Energy Research and Applications, ICRERA 2016, 2017. doi: 10.1109/ICRERA.2016.7884553.

[12] R. A. Meyers, "Classical and Nonclassical Optimization Methods Classical and Nonclassical Optimization Methods 1 Introduction 1 1.1 Local and Global Optimality 2 1.2 Problem Types 2 1.3 Example Problem: Fitting Laser-induced Fluorescence Spectra 3 1.4 Criteria for Optimization 4 1.5 Multicriteria Optimization 4," Encycl. Anal. Chem., pp. 9678–9689, 2000, [Online]. Available: https://pdfs.semanticscholar.org/5c5c/908bb00a54439dcee50ec1ada6b735694a94.pdf

[13] N. Steffan and G. T. Heydt, "Quadratic programming and related techniques for the calculation of locational marginal prices in distribution systems," in 2012 North American Power Symposium (NAPS), 2012, pp. 1–6. doi: 10.1109/NAPS.2012.6336310.

[14] M. Mafarja et al., "Evolutionary Population Dynamics and Grasshopper Optimization approaches for feature selection problems," Knowledge-Based Syst., vol. 145, pp. 25–45, 2018, doi: 10.1016/j.knosys.2017.12.037.

[15] A. A. Heidari, R. Ali Abbaspour, and A. Rezaee Jordehi, "An efficient chaotic water cycle algorithm for optimization tasks," Neural Compute. Appl., vol. 28, no. 1, pp. 57–85, 2017, doi: 10.1007/s00521-015-2037-2.

DOI: https://doi.org/10.5281/zenodo.18372972