وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم الرياضيات

خوارزميات امثلية ذكائية مطورة مع تقانات المعلومات الحيوية لتشفير البيانات

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة ماجستير علوم في
الرياضيات/ الرياضيات الحاسوبية

من قبل
صالح عواد خضر احمد الجاسم

بإشراف

أ.د. بان احمد حسن متراس

١٤٤٧ هـ ٢٠٢٥ م

المستخلص

تشهد نظم التشفير الحديثة تحديات متزايدة نتيجة التطور السريع في قدرات الحوسبة واساليب الاختراق، مما يستلزم البحث عن خوارزميات قوية ومرنة. ومن بين الاتجاهات الواعدة دمج الذكاء الاصطناعي وخوارزميات الامثلية الذكائية مع التشفير، لما توفره من قدرات عالية في استكشاف فضاءات الحلول الواسعة وتحقيق مستويات امان أكبر. تهدف هذه الرسالة الى تصميم خوارزميات هجينة فعالة تعتمد على الذكاء الاصطناعي لحل مسائل الامثلية المعقدة وتوظيفها في مجال التشفير وقد تم التركيز على تهجين خوارزميات سربيه مستوحاة من الطبيعة مع خوارزميات رياضية موجهة لتحسين جودة البحث وتقوية نظم التشفير.

في المرحلة الأولى تم تطوير نموذج هجيني يجمع بين خوارزمية الطائر الطنان الاصطناعي (Artificial Hummingbird Algorithm - AHA) وخوارزمية الكائنات الزقية (Tunicate Swarm Algorithm - TSA). يعتمد النموذج على تقسيم المجتمع في كل تكرار الى قسمين اعتمادا على جودة النتائج يعالج الافراد الأفضل باستخدام AHA بينما يعالج الأضعف أداء باستخدام TSA مع إعادة الترتيب وإعادة التقسيم دوريا لضمان التوازن بين الاستكشاف والاستغلال داخل فضاء الحل.

في المرحلة الثانية تم تطوير معلمتين جديدتين لمبدأ التدرج المترافق (Conjugate Gradient) يستخدمان لتحسين توجه الافراد ضمن فضاء البحث.

- النموذج الأول CG-S1 ويعتمد على ثلاث علاقات رياضية مختلفة لحساب معامل بيتا. وكل علاقة تتضمن المعلمة t كعامل تحكم مما يمنح الخوارزمية قدرة مرنة على اختبار وتكييف الاتجاه الجديد لكل تكرار.
- النموذج الثاني CG-S2 ويعتمد على علاقة واحدة ثابتة لحساب بيتا وتتمثل في استخدام صيغة تحقق استقرار اعلى ولكن بمرونة اقل مقارنة بـ CG-S1.

تم تهجين كل من النموذجين (CG-S1) و (CG-S2) مع الخوارزميتين AHA و TSA مما أسفر عن انتاج أربع خوارزميات هجينة جديدة:

TSA -CG-S2 ، -TSA -CG-S1 ، AHA -CG-S2 ، AHA -CG-S1

وقد تم تهيئة هذه الخوارزميات للتعامل مع اعداد طبيعية غير مكررة (Permutations) بهدف توليد مفاتيح تشفير فعالة تستخدم في نظام تشفير متكامل قائم على الدمج بين الطرائق التقليدية والذكية. تم في هذا السياق اعتماد بنية تشفير هجينية تقوم بتشفير النصوص أولا باستخدام خوارزمية RSA التقليدية، ثم دمج النص المشفر داخل سلسلة DNA معروفة مسبقا باستخدام مفاتيح ناتجة من الخوارزميات الذكية المقترحة.

تم تنفيذ التجارب جميعا باستخدام بيئة MATLAB بإصدار 2022، وتم اختبار أداء الخوارزميات على خمس دوال قياسية. فضلا عن تقييم قوتها في سياق التشفير باستخدام مؤشرات متعددة أظهرت النتائج فعالية الخوارزميات المهجنة من حيث جودة الحلول وسرعة التقارب والقدرة على توليد مفاتيح ذات خصائص امنية عالية، مما يبرهن على فعالية الدمج بين الذكاء الاصطناعي والخوارزميات التقليدية في بناء نظم تشفير متقدمة وامنة.

وعلى الجانب النظري، تم اثبات خاصيتي الانحدار الكافي والتقارب الشامل للخوارزميات المعتمدة على معلمتي التدرج المترافق الجديدتان مما يدعم موثوقية الأداء الرياضي للخوارزميات المقترحة عند تطبيقها في فضاءات غير خطية ومعقدة.

Ministry of Higher Education
and
Scientific Research
University of Mosul
College of Computer Science
and Mathematics
Department of Mathematics

Modified Intelligent Optimization Algorithms with Bioinformatics for Data Encryption

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Master of Science
in
Mathematics/Computational Mathematics**

By

Salih Awad Khudhur Ahmed

Supervised by

Prof. Dr. Ban Ahmad Hassan Mitras

2025 A.D. **1447 A.H.**

Abstract

Modern encryption systems face increasing challenges due to rapid advances in computing capabilities and hacking techniques, necessitating the development of robust and flexible algorithms. One promising approach is the integration of artificial intelligence and intelligent optimization algorithms with encryption, given their superior capabilities in exploring broad solution spaces and achieving greater levels of security. The thesis aims to design efficient hybrid algorithms based on artificial intelligence to solve complex optimization problems and employ them in the field of cryptography. The focus was on integrating nature-inspired swarm algorithms with mathematical algorithms to improve search quality and strengthen cryptographic systems.

In the first phase, a hybrid model was developed that combines the Artificial Hummingbird Algorithm (AHA) and the Tunicate Swarm Algorithm (TSA). The model is based on dividing the population into two parts at each iteration based on the quality of the solutions. The best-performing individuals are treated using AHA, while the weakest performers are treated using TSA, with periodic reshuffling and repartitioning to ensure a balance between exploration and exploitation within the solution space.

In the second phase, two new components based on the conjugate gradient principle were developed, which are used to improve the orientation of individuals within the search space.

- The first model, CG-S1, relies on three different mathematical relationships to calculate the beta coefficient. Each relationship includes the t parameter as a control factor, giving the algorithm the flexibility to test and adapt a new trend for each iteration.
- The second model, CG-S2, relies on a single fixed relationship to calculate beta. It uses a traditional standard formula that achieves higher stability but with less flexibility compared to CG-S1.

Both models (CG-S1 and CG-S2) were hybridized with AHA and TSA algorithms, resulting in four new hybrid algorithms.

AHA-CG-S1, AHA-CG-S2 ،TSA-CG-S1 ،TSA-CG-S2

These algorithms have been adapted to handle non-repeating integers (permutations) in order to generate effective encryption keys for use in an integrated encryption system based on combining traditional and smart methods. In this context, a hybrid encryption structure was adopted that first encrypts texts using the traditional RSA algorithm, then hides the encrypted text inside a previously known DNA string using keys generated by the proposed smart algorithms. The results showed that the use of keys generated based on non-repeating permutations contributed to enhancing encryption security and increasing the complexity of cracking the code.

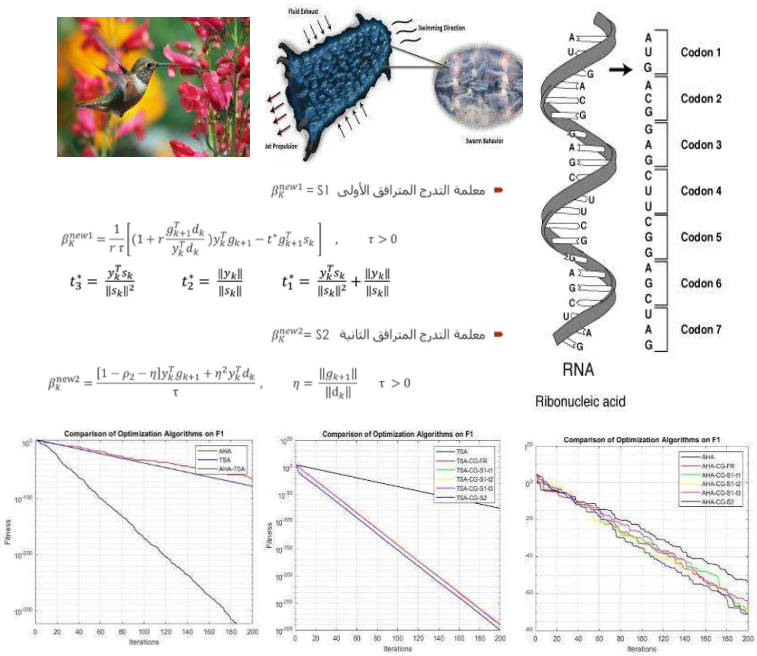
All experiments were conducted using the **MATLAB 2022** environment, and the algorithms' performance was tested on five standard functions. In addition to evaluating their robustness in the context of encryption using multiple indicators, the results demonstrated the effectiveness of the hybrid algorithms in terms of solution quality, convergence speed, and the ability to generate keys with high security properties. This demonstrates the effectiveness of combining artificial intelligence with traditional algorithms in building advanced and secure encryption systems.

On the theoretical side, **the sufficient gradient and global convergence properties** of the conjugate gradient-based algorithms were proven, which supports the reliability of the mathematical performance of the proposed algorithms when applied in non-linear and complex spaces.

.

Modified Intelligent Optimization Algorithms with Bioinformatics for Data Encryption

Author: Salih Awad Khudhur **Advisor: Prof. Dr. Al-Mitras. B.A** **Publisher: University of Mosul**

HIGHLITS	GRAPHICAL ABSTRACT
· Hybrid optimization algorithms were designed integrating Artificial Hummingbird Algorithm (AHA) and Tunicate Swarm Algorithm (TSA). · Two conjugate-gradient-based strategies (CG-S1 and CG-S2) were proposed to improve orientation of individuals in the search space. · Four new hybrid models were created: AHA-CG-S1, AHA-CG-S2, TSA-CG-S1, TSA-CG-S2. · Hybrid encryption structure was developed combining RSA with DNA-based hiding using smart-generated keys. · Results showed higher encryption security, faster convergence, and better solution quality compared with baseline methods.	

Keywords:

Hybrid optimization

Artificial Hummingbird Algorithm

Tunicate Swarm Algorithm

Conjugate Gradient

Bioinformatics

DNA cryptography

RSA encryption

Permutation-based keys

ABSTRACT

Modern encryption systems face significant challenges due to rapid advances in computing and hacking techniques, motivating the development of robust and flexible hybrid algorithms. This thesis aims to design AI-based hybrid algorithms to solve complex optimization problems and apply them in cryptography, focusing on integrating nature-inspired swarm algorithms with mathematical algorithms to improve search quality and enhance security.

A hybrid model combining the **Artificial Hummingbird Algorithm (AHA)** and the **Tunicate Swarm Algorithm (TSA)** was developed, where the best-performing individuals are processed using AHA and the weakest using TSA, with periodic reshuffling to balance exploration and exploitation.

In the second phase, two new conjugate-gradient-based models were proposed:

- **CG-S1**: Uses three mathematical relationships to calculate the beta coefficient, providing higher flexibility.
- **CG-S2**: Uses a single fixed relationship, offering greater stability but less flexibility.

Both models were hybridized with AHA and TSA, resulting in four hybrid algorithms: **AHA-CG-S1, AHA-CG-S2, TSA-CG-S1, TSA-CG-S2**.

These algorithms were adapted to handle non-repeating integers (permutations) to generate effective encryption keys within a hybrid encryption system that combines RSA with DNA-based hiding. Results showed that using these permutation-based keys enhanced encryption security and increased the complexity of code-breaking.

2025, M.Sc. Thesis @Univ. of Mosul, College of Computer Science and Mathematics, Department of Mathematics (https://www.uomosul.edu.iq/).