جامعة الموصل
كلية علوم الحاسوب والرياضيات

# تطوير وتنفيذ أنموذج أمني متعدد المستويات لسرية البيانات على الكوكل درايف

نادية معن محمد ثابت

أطروحة دكتوراه

علوم الحاسوب

إشراف

د. نجلاء بديع إبراهيم الدباغ

أُستاذ مساعد

1442 هـ 2020 م

## المستخلص

جاءت هذه الأطروحة لتركز على التهديدات الداخلية المقدمة من موفري الخدمات السحابية، ولتطوّر أنموذجا أمنياً يؤدي إلى رفع أداء نظام المعلومات الامني للمؤسسات، حيث يمكن التحكم في خطر الوصول غير المصرح به باستخدام تقانات التشفير والكتابة المغطاة. تم تقديم أنموذج أمني مطور ومتعدد المستويات يضم طرائق جديدة لتشفير وتضمين البيانات لغرض تخزينها في السحابة بطريقة آمنة وحمايتها من الهجمات، فضلاً عن تقليل الكلفة والوقت اللازم للتخزين. اذ أُقترحت وطُبقت طريقة تشفير مهجنة تضم ثلاث مستويات أمن هي ترميز "Deoxyribose Nucleic Acid" (DNA)، شفرة فيجينير المطورة وخوارزمية "Advance Encryption Standard" (AES). كما عُزز أمن البيانات من خلال تضمين البيانات اذ أُقترحت طرائق تضمين جديدة باعتماد خوارزمية البت الاقل اهمية الهاشية "Hash Least Significant Bit" (HLSB) وباعتماد خوارزميات مابعد الحدس (أمثلية سرب الطيور، خوارزمية البحث عن طائر الوقواق)، تم الوصول الى نتائج جيدة.

يتضمن تنفيذ الأنموذج المطور اولاً تقسيم البيانات على عدة مستويات وفقاً لأهميتها من وجهة نظر مالك البيانات ثم تحديد العملية المنفذة على البيانات (تشفير / تشفير وتضمين) اعتماداً على المستوى الأمني المطلوب لسرية البيانات. لقياس كفاءة طريقة التشفير المقترحة المطُبقة على النص والصورة أُستخدمت عدة مقاييس منها وقت التشفير، ووقت فك التشفير، والإنتاجية "Throughput"، وتأثير الانهيار "Avalanche Effect"، وأظهرت النتائج أن الطريقة المقترحة تعطي نتائج مقبولة. اذ كانت قيم المقاييس لطريقة التشفير المقترحة والمطبقة على النص كالآتي: قيمة "Throughput" مساوية لـ (5632 بت/ثانية)، وقيمة "Avalanche Effect" مساوية لـ (63%) مقارنةً بقيمته باستخدام خوارزمية (AES) التي كانت مساوية لـ (59%). أما قيم المقاييس لطريقة التشفير المقترحة المطبقة على الصورة فهي كالآتي: قيمة "Throughput" مساوية لـ (7468 بت/ثانية)، وقيمة " Avalanche Effect" مساوية لـ (63%). أكدت هذه المقاييس تعزيز الأمن والحماية السحابية للبيانات المخزونة في السحابة من خلال تحسين "Throughput" و "Avalanche Effect".

ولقياس كفاءة طرائق التضمين المقترحة أُستخدمت عدة مقاييس منها الرسم البياني "Histogram"، مقياس نسبة الاشارة الى الضوضاء "Peak Signal to Noise Ratio" (PSNR)، ومعدل مربع الخطأ "Mean Square Error" (MSE)، ومعامل الإرتباط " Normalized (NC)

Correlation" ونسبة البت الخطأ (BER) "Bit Error Rate". تمت مقارنة نتائج كل طريقة تضمين مقترحة مع نتائج التقانات المستخدمة الأخرى واظهرت النتائج الحصول على تشويش طفيف على الصور المستخدمة نتيجة تضمين البيانات داخل الصورة، وملاحظة ذلك من خلال نتائج الـ (PSNR) العالية نسبياً ونتائج الـ (MSE) القليلة، اذ كانت قيمة (PSNR) لطريقة التضمين الهجينة المقترحة باعتماد خوارزمية بحث طائر الوقواق الهجينة (86.8626 dB)، في حين كانت قيمة (PSNR) لطريقة التضمين المقترحة باعتماد خوارزمية بحث طائر الوقواق (85.9911 dB)، ثم قيمة (PSNR) لطريقة التضمين المقترحة باعتماد أمثلية سرب الطيور (86.0031 dB).

ولإثبات الكفاءة والمقاومة لهجوم محتمل تم تعريض طرائق التضمين المقترحة لهجوم الملح والفلفل "Salt & Pepper" وجاءت النتائج مبينة كفاءة الطريقة من خلال قيم (NC) وقيم (BER) التي تم الحصول عليها. استخدمت الخدمة السحابية (Google Drive) ضمن الأنموذج المطور لتنفيذ التخزين السحابي سواء أكان للبيانات العادية أم المشفرة والصور بعد التضمين. لتحسين الأداء، يتيح الأنموذج سهولة التطوير والتوسيع لنظام المعلومات للمؤسسات مع مرور الوقت، فضلاً عن أنه تم تبيان ميزات الأنموذج المطور بالمقارنة مع الدراسات السابقة.

نُفذ العمل على حاسوب ذي معالج (core i7)، يعمل بنظام ويندوز (10) مع لغة ماتلاب (R2014a).

University of Mosul
College of Computer Science
and Mathematics

# *Developing & Implementation of Multilevel Secure Model for Data Confidentiality on Google Drive*

**Nadia Maan Mohammed Thabit**

**Ph.D. / Thesis**

**Computer Science**

**Supervised By**

**Dr. Najla Badie Ibraheem Al-Dabagh**

**Assistant Professor**

**2020 A.D.** **1442 A. H.**

## Abstract

This thesis came to focus on the internal threats presented by cloud services providers, and to develop a security model that leads to an increase in the performance of the security information system for organizations. The risk of unauthorized access can be controlled using encryption and steganography technologies. An advanced, multi-level security model has been introduced that includes new ways to encrypt and embed data for the purpose of securely storing data in the cloud and protecting it from attacks, as well as reducing the cost and time required for storage. A hybrid encryption method has been proposed and implemented to encrypt data before storing it in the cloud. The hybrid encryption method includes three security levels: DNA coding (Deoxyribose Nucleic Acid), enhanced Vigner code and AES (Advance Encryption Standard) algorithm. Data security was also enhanced by embedding of data, as new embedding methods were proposed by adopting the Hash Least Significant Bit (HLSB) algorithm and by adopting meta-heuristic algorithms ("Particle Swarm Optimization", "Cuckoo Search algorithm"), Good results were reached.

The implementation of the developed model involves first dividing the data into several levels according to its importance from the point of view of the data owner, then determining the process implemented on the data (Encryption/ Encryption & Embedding) depending on the security level required for confidentiality of the data. To measure the efficiency of the proposed encryption method applied to text and image, several metrics were used including Encryption Time, Decryption Time, Throughput and Avalanche Effect. The experiments showed that the suggested scheme yielded acceptable outcomes. As the metrics values for the proposed encryption method applied to the text were as follows: the value of Throughput is equal to (5632 bit/sec), and the value of Avalanche Effect is equal to (63%) compared to its value using the AES algorithm that was equal to (59%). The metrics of the proposed encryption method applied to the image are as follows: Throughput value equal to (7468 bit/sec) and Avalanche Effect value equal to (63%). These metrics confirmed enhanced security and cloud protection for data stored in the cloud by improving Throughput and Avalanche Effect.

To measure the proficiency of the suggested embedding methods, several metrics were used, including the Histogram, “Peak Signal to Noise Ratio (PSNR)”, “Mean Square Error (MSE)”, “Normalized Correlation (NC)” and “Bit Error Rate (BER)”. The expermintes of each suggested embedding method were compared with the results of other used techniques. The results showed a slight distortion of the images used as a result of embedding data inside the image, and note this through the relatively high PSNR results and the few MSE results, where the value of the PSNR for the proposed hybrid embedding method based on the hybrid cuckoo search algorithm was (86.8626dB), whereas, the proposed PSNR value for the embedding method based on the cuckoo search algorithm was equal to (85.9911dB), while the value of the proposed PSNR for the method of embedding based on the particle swarm optimization was equal to (86.0031 dB).

To demonstrate the efficiency and resistance to a potential attack, the proposed embedding methods were exposed to Salt & Pepper attack. The results showed the efficiency of the method through the NC and BER values obtained. Google Drive cloud service used within the developed model to implement cloud storage, whether for normal data, encrypted and images after embedding. To improve performance, the model allows for the easy development and expansion of the enterprise information system over time, in addition to the advantages of the developed model compared to previous studies.

The work was done on a computer with a core_i7 processor, running Windows 10 with Matlab R2014a.