First Libyan International Conference on Engineering Sciences & Applications (FLICESA_LA)
13 – 15 March 2023, Tripoli – Libya

استخدام تقنيتي الضغط والتشفير لحماية الملفات النصية في الحوسبة الالكترونية

حنان علي الزلعوطي 1 ، هناء سعد التائب 2
[1]المعهد العالي للتقنية الصناعية النجيلة ، جنزور، ليبيا
[2]الجامعة المفتوحة طرابلس ، جنزور، ليبيا
habaaahados@gmail.com[2] ،zalwotee82@gmail.com[1]

الملخص: يهدف هذا البحث الى انشاء نظام حماية البيانات وإمكانية الاستفاده منه في تقنيات الحوسبة الاكترونية. نظرا لما تتطلبه هذه التقنية من توفير مساحة لتخزين المعلومات مع ضمان حمايتها في نفس الوقت . ففي هذا البحث تم الدمج بين تقنية التشفير باستخدام خوارزمية معيار تشفير البيانات **(**DES(Data Encryption Standard وتقنية الضغط باستخدام خوارزمية هافمان اضافة الى عملية الدمج التي تم فيها تشفير النص المضغوط من خلال خلط كل 8 بت متجاوران ببعضهما لتغيير ناتج عملية الضغط واخفاء معالم الضغط . كما تم استخدام مفتاح سري بطول 16 بايت للتأكد من هوية المستخدم و تم تضمينه داخل النص بعد عملية الضغط مع 16بايت الاولى للنص المصغوط . وفي هذه الورقة سوف يتم تقديم النتائج من حيث نسبة الضغط والوقت اللازم لتنفيذ المقترح ومقارنتها بدراسة اخرى تم فيها الاعتماد على خوارزمية **DES** مع خوارزمية LZW .

الكلمات المفتاحية: السحابة الحاسوبية، التشفير ، الضغط ، خوارزمية معيار تشفير البيانات.(DES) ، خوارزمية هافمان.

1. المقدمــة.

ان زيادة استخدام الانترنت والتواصل بين الكيانات وزيادة انتشاراستخدام انترنت الاشياء ، زادت معها حجم البيانات التي يتم حفظها في خوادم الحوسبة الاكترونية.وبالتالي زادت اهمية حماية وامن المعلومات معها ، الامر الذي جعل العالم اليوم يوجه انظاره لهذه التقنية وايجاد الحلول والطرق لحماية المعلومات وتوفير المساحة التخزينية وسعة وسائل النقل [1]. هناك العديد من انظمة حماية المعلومات وتختلف باختلاف استخداماتها وشكل البيانات التي تنتج عنها . منها علم التشفير وهو علم يهتم بتغيير محتوى الرسائل وجعلها غير مفهومة دون الاهتمام بحجمها ويتم فيه استخدام المفاتيح لتشفير البيانات وفكها فمنها ما يستعمل مفتاح واحد للتشفير وفك التشفير تسمى بخوارزميات التشفير بالمفتاح المتماثل كما هو في خوازمية معيار تشفير البيانات (Data Encryption Standard **(DES)**) وخوارزميةمعيار التشفير المتقدم Advanced Encryption Standard (AES). [2] ومنها مايستخدم مفتاحان حيث لايكون مفتاح التشفير هو نفسه في فك التشفير وتسمى خوارزميات المفتاح الغير متماثل مثل خوارزمية (RASA).[1][2] [3][4]

وهناك ايضا تقنيات تعمل على تشفير البيانات ولكن يتم التركيز على تقليص حجمها وهي تقنية الضغط حيث يتم تقليص حجم البيانات وتوفير المساحة التخزينية اضافة الى تغيير محتواها لما يجعلها سرية ولكن بدون استخدام المفاتيح ولكن هناك نوعان منها مايتم الضغط وحذف بعص المعلومات الغير مهمة وتسمى خوارزميات الضغط بالفقد مثل خوارزمية ضغط الصور JPEG . والنوع الاخر لا يتم فيه فقد المعلومات ويسمى الصغط بدون فقد مثل خوارزمية هافمان (Huffman) ,وخوارزمية تبديل النص (LZW).[2][5][6]

ونظرا لاهمية هاتين التقنيتين تم في هذا البحث العمل على دمجهما لاستخدامها في نقل او حفظ البيانات عبر الانترنت. وتوفير الية تعمل وتوفر نتائج للاجابة على التساؤلات التالية :

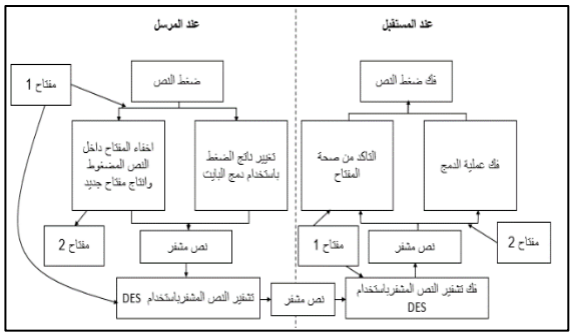
- كيف يتم تقليص حجم البيانات بافضل نسبة ضغط ؟
- كيف يتم تغيير البيانات الناتجة من عملية الضغط دون الزيادة في حجمها حجمها ؟
- كيف يتم تضمين المفتاح السري داخل النص بشكل امن مع توفير مفتاح سري اخر لزيادة التعقيد وامن البيانات؟
- كيف يتم زيادة سرعة عمل خوارزمية DES ؟
- كيف يتم حل مشكلة توفر خوارزمية DES على الانترنت مما يسهل في عملية فكها والعمل على تغيير نتاج الفك بحيث تكون غير مفهومة ؟

ومن الدراسات التي عملت في هذا الموضوع كالتالي :

- في سنة 2017 ، هاريش كومر وراشجخار واخران قدما بحثا لحماية البيانات في استخدام انترنت الاشياء والسحابة الحاسوبية بتوفير نظام حماية على مستويين باستخدام خوارزمية هافمان لتوليدالمفتاح وخوارزمية الحمض النووي DNA لتشفير البيانات .[1]
- في سنة 2018 قدم مجموعة من الباحثين صديق الغرار، حنين البرغي ونورا ماضي بحثا تم فيه تصميم وتنفيذ نظام لحماية البيانات بالاعتماد على تشفير المفتاح ثم اخفاؤه داخل النص المشفر بطريقة لا يمكن استعادتها للتغلب على عملية توزيع المفتاح وجعل الخوارزمية اكثر امنا وتم تجربتها على العديد من النصوص وكانت النتائج من الصعب اكتشاف المفتاح مع بساطة الخوارزمية المقترحة .[3]
- في سنة 2021 ، قدمت الباحثة نجاح الشديد نظام حماية محادثة على الانترنت بدمج خوارزمية الضغط LZW و خوارزمية التشفير DES لحماية البيانات مع عملية الدمج بين كل عددين عشريين الناتجين من عملية الضغط وانتاج مفتاح جديد وكانت النتائج مرضية الا انها اعتمدت على الحروف الكبيرة فقط في الخوارزمية ، وكان هناك تحسين في نتائج نسبة الضغط بسيطة بينما زادت سرعة التشفير بنسبة ما يقارب 50% تقريبا.[2]

2. المنهجية المتبعة :

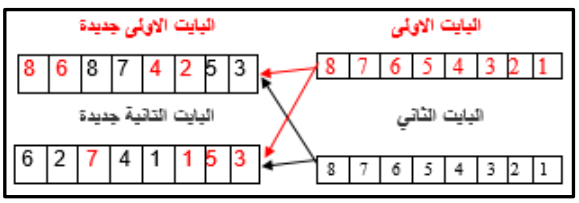
تم في هذا البحث تصميم وتنفيذ نظام التشفير كما هو موضح بالشكل (1) والخطوات التالية :



شكل رقم (1): النظام المقترح لتشفير النص

1.1. عند المرسل :

- قراءة النص السري .
- ضغط البيانات باستخدام هافمان العمل على تحويل النص المضغوط الذي على شكل 0 و 1 الى اعداد عشرية كل عدد في بايت واحد فيه 8 بت .
- دمج المفتاح السري مع النص المضغوط وتنفيذ عملية الدمج على كل النص وانتاج مفتاح جديد ونص جديد مشفر تتم هذه العملية بعد ان يتم ضغط النص وتجميع كل 8 بت في بايت واحد ثم يتم دمج البتات من كل منهما وانتاج بايتين جديدين اخرين وفقا للشكل التالي :



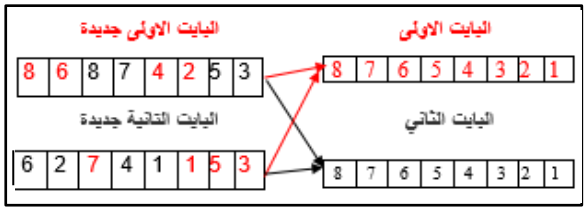
شكل رقم (2): دمج البايت

وعند تطبيق عملية الدمج لاخفاء المفتاح مع النص المضغوط ينتج عنه مفتاح جديد يستخدم في فك الدمج عند المستلم .

- تشفير النص الناتج من عمليتي الضغط والدمج باستخدام خوارزمية DES بمفتاح طوله 16 بايت .

1.2. عند المستقبل :

- قراءة النص المشفر وشجرة هافمان .
- فك التشفير باستخدام خوارزمية DES ومن خلال المفتاح .
- فك عملية الدمج بادخال المفتاح الناتج عند المرسل من الدمج والتاكد من ان الشخص المستلم هو المخول بذلك .وتتم عملية فك الدمج كعملية عكسية كما في الشكل التالي :



شكل رقم (3): فك دمج البايت

3. التنفيذ :

تم تصميم وتنفيذ النظام المقترح باستخدام لغة C#.net كما هو موضح بالشكل (4) بسيط وغير معقد وتم اجراء العديد من الاختبارات وكانت العملية ناجحة حيث يتم عرض الصورة النهائية للنص :

شكل رقم (4): نظام التشفير

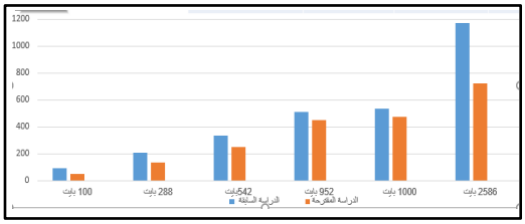
وتم مقارنة النتائج مع نتائج الدراسة [2] التي تضمنت نفس هذه الدراسة الا انه تم استبدال خوارزمية LZW بخوارزمية هافمان مع اختلاف ترتيب البتات في عملية الدمج ونفس المفتاح المستخدم وكانت النتائج والمقارنات وفقا للجدول التالي :

1.3. مقارنة النتائج وفقا لحجم النص الناتج من التشفير :

تمت مقارنة نتائج التشفير في النظام المقترح مع دراسة سابقة بتشفير ستة ملفات نصية مختلفة الحجم كما هو موضح في الجدول 1 والشكل رقم(5) :

جدول (1): مقارنة نتيجة التشفير من حيث حجم الملف

ت	حجم النص بالبايت	الدراسة السابقة	الدراسة المقترحة
1	100	88	48
2	288	208	136
3	542	336	249
4	952	508	448
5	1000	536	472
6	2586	1168	720



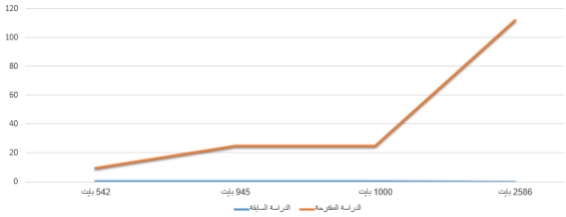
شكل رقم (5): مخطط مقارنة نتيجة التشفير من حيث الحجم

2.3. مقارنة النتائج وفقا لزمن التنفيذ:

تم مقارنة نتيجة زمن التنفيذ بين الدراسة السابقة والدراسة المقترحة بالملي ثانية وكانت النتائج ان زمن التنفيذ في الدراسة السابق اقل بكثير من الدراسة المقترحة كما هم مبين في الجدول والشكل لتاليين:

جدول (2): مقارنة وقت التنفيذ لتشفير النص بين الدراستين السابقة والمقترحة

ت	حجم النص بالبايت	الدراسة السابقة	الدراسة المقترحة
1	542	0.287	9.005
2	952	0.369	24.227
3	1000	0.318	24.868
4	2586	0.51	111.94



شكل رقم(6): مخطط مقارنة زمن تنفيذ التشفير بين الدراسة السابقة والمقترحة .

4. الاستنتاجات

1- النظام المقترح بسيط وسهل الاستخدام .

2- عملية اخفاء المفتاح وعملية الضغط زادت من صعوبة اكتشاف نوع الخوارزمية المستخدمة في التشفير .

3- عملية الدمج لم تعمل على زيادة حجم الملف كما انها زادت في صعوبة اكتشاف الخوارزمية المستخدمة في الضغط واخفت معالم نتائجها .

4- ساهم الضغط بطريقة هافمان في تقليص حجم الملف اكثر مما هو عليه باستخدام LZW مما يوفر مساحة تخزينية وسرعة نقل الملفات عبر الانترنت.

5- ان الطريقة المقترحة كانت نتائجها افضل من الدراسة السابقة من حيث حجم الملف ، عدم تغيير في الحروف الانجليزية سواء الكبيرة او الصغيرة بعكس الدراسة السابقة التي تعمل على الحروف الكبيرة فقط .

6- الدراسة المقترحة تتطلب ارسال شجرة هافمان ولكن هذا لن يؤثر على اكتشاف الية الضغط بسبب الدمج والتشفير وهذا قد يجعل المهاجم من اعتقاد ان البيانات مضغوطة فقط .

7- ان زمن تشفير النص لم يتم التقليل منه ويرجع ذلك لان خوارزمية هافمان بعد ان يتم تمثيل الشجرة لها يتم الدوران مجددا على النص لوضع البت الخاصة بكل حرف.

4. التوصيات

1- نوصي باستخدام هذه الطريقة مع عملية الاخفاء في الصورة كنظام حماية .

2- تجربة النظام المقترح على نوع بيانات اخرى.

3- العمل على ايجاد الية لاخفاء شجرة هافمان .

4- تحسين النظام وايجاد طريقة لتقليص الوقت المستغرق بطريقة افضل.

5. المراجع

[1] A Novel Approach for securing data in IoTcloud Using DNA Cryptography and Huffman Codin Algorith , Harish Kumar N, Dr.Rajshekhar M Patil , Deepak G, Murthy B M, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).

[2] An investigation of the design, analysis and performance evaluation of the Improvement the protection system for online chatting , Najah Abdualkader Alshadid, Thesis submitted to department of computer siences in libyan academy of the Requirements of Master,2021.

[3] New Text Encryption Method Based on Hidden Encrypted, Seddeq E. Ghrare, Haneen A. Barghi, Nora R. Madi Symmetric Key, ACIT 2018, June 1-3, 2018.

[4] Implementation of a bit permutation-based advanced encryption standard for securing text and image filesm, Heidilyn V. Gamido, Indonesian Journal of Electrical Engineering and Computer Science,Vol. 19, No. 3, September 2020, pp. 1596~1601

[5] Application of Huffman Data Compression Algorithm in Hashing Computation, Lakshmi Narasimha Devulapalli Venkata, Thesis Presented to The Faculty of the School of Engineering and Applied Sciences Western Kentucky University,2018.

[6] Study on Data Compression Using Huffman Coding Algorithms, D.Jasmine Shoba, Dr.S.Sivakumar, International

Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 1, Jan – Feb 2017.