تضمين الرساله السرية داخل نص عربي مُشكّل

ا.م.د. هالة بهجت عبد الوهاب	ا.م.د. سهاد مال الله كاظم	الباحثة. استبرق عبد الرضا كاظم
قسم علوم الحاسبات	قسم علوم الحاسبات	قسم علوم الحاسبات
الجامعة التكنلوجية	الجامعة التكنلوجية	الجامعة التكنلوجية
بغداد\العراق	بغداد\العراق	بغداد\العراق

الخلاصة

خلال السنوات الماضية، أصبح علم أمنية المعلومات هو محل اهتمام لكثير من الباحثين التي تحاول جهودهم أن تتوصل إلى حلول وتقنيات و أفكار جديدة تضمن نقل المعلومات بأمان من خلال شبكة الانترنت للحيلولة دون حدوث اختراق وكشف تلك المعلومات. ونتيجة لذلك، توجد العديد من التقنيات والأساليب التي تستخدم حالياً في أمن المعلومات و يعتبر علم التضمين (Steganography) من أهم هذه الطرق. علم التضمين هو العلم الذي يهتم باخفاء المعلومات الرقمية داخل وسيط الكتروني دون احداث أي تشويه أو تعديل ملحوظ في هذا الوسيط.

يهدف هذا البحث الى طرح طريقة جديدة ومبتكره في تضمين الرسائل السرية داخل النصوص العربية المشكّلة وذلك من خلال الاستفادة من اللغة العربية كونها تتمتع بخصائص و ألفاظ وتراكيب وصرف ونحو وأدب وخيال، مع الاستطاعة في التعبير عن مدارك العلم المختلفة و لانها تحتوي على مميزات تختلف عن بقية اللغات الاخرى في تضمين المعلومات السرية في الوقت الحاضر مثل وجود الحركات واختلاف شكل بعض الحروف حسب مواقعها داخل الكلمة وكثرة القواعد الاعرابية والنحوية فيها. لذلك فهي تُعد لغة غنية جدا في هذا المجال ولها قدرة كبيرة وكفوءة على حمل المعلومات السرية المراد ارسالها من طرف الى طرف اخر.

تم تقييس جودة طريقة التضمين المقترحه داخل النصوص العربية المُشكّلة بالاعتماد على المقايس الشائعه في علم التضمين ومنها مقياس السعة و الذي يعمل على تقييس قدرة وسعة النص العربي المشكّل على تضمين واستيعاب حجم المعلومات السرية المُراد اخفاءها بداخِله. و مقياس الشفافية والذي يعمل على تقييس مدى توقع المهاجمين والمتنصتين على وجود معلومات سرية مُضمّنة داخل النص العربي المشكّل وقدرتهم على استخراج تلك المعلومات السرية من النص .

وكانت النتائج كفوءة وعالية جدا وتمتاز بتحقيق حماية وكفاءة ممتازة وجودة عالية في العمل في مجال التضمين بالنصوص العربية المشكّلة من حيث السعة و الشفافية مقارنة مع الطرق السابقة.

1. اهمية الاخفاء داخل النصوص العربيه

اللغة هي وسيلة من وسائل الاتصال الفكري بين أبناء المجتمع وهي أداة التفاهم ونقل الأفكار والحضارة من جيل إلى آخر,وتعد اللغةالركيزة الاساسية في المجتمع، فعبر اللغة يتم نقل المعلومات والتقنيات والحضارة من جيل إلى آخر. إن الاهتمام باللغة نابع من أهمية اللغة في حياة الشعوب، فاللغة هي الوسيلة التي يمكن بها تحليل أية صورة أو فكرة ذهنية إلى أجزائها أو خصائصها، والتي بها يمكن تركيب هذه الصورة مرة أخرى في أذهاننا وأذهان غيرنا، وذلك بتأليف كلمات ووضعها في ترتيب خاص [1].

اللغة العربية هي إحدى اللغات الإنسانية المنحدرة من اللغات السامية، وعلى الرغم من كون أنَّ للعربية السبق في مجال اللسانيات ولكن الأبحاث في معالجة اللغة العربية حاسوبيا كانت متأخرة، واحدى أسباب تأخر العمل في مجال اللسانيات الحاسوبية العربية هو مشاكل التشكيل في اللغة العربية

أن الهدف الاساسي من وجود هذه الحركات هو للتمييز بين كلمة واخرى لها نفس الحروف وتختلف بالمعنى مثلا (يَكونْ , يُكَّوْن) [2]. تعد النصوص العربية المشكلة وسيلة فعالة وممتازة في مجال اخفاء البيانات السرية وذلك من خلال استخدام علامات التشكيل العربية في تضمين البيانات السرية[3]. ان الاخفاء داخل النصوص يكون على نوعين : اما اخفاء داخل نصوص الكترونية مثل النصوص المكتوبة ببرنامج الوورد داخل الحاسبة, او اخفاء داخل نصوص اعتيادية مكتوبة على ورق. يُعد الاخفاء داخل النصوص الالكترونية من اصعب واعقد انواع الاخفاء للبيانات وهذا يعود الى صعوبة عملية التضمين داخل النصوص وصعوبة التحديث عليها بطريقة لايتم كشفها او اختراقها مقارنة مع بقية الوسائل. هنالك عدة طرق للاخفاء داخل النصوص مثلا استخدام الخواص الفيزيائية للتعامل مع النص كأضافة الفاراغات(space) والأسطر (Line) وايضا استخدام الطرق التي تُعنى بالترتيب القواعدي والمعنوي للنص [4] .

2. الهيكل الشجري +B [7,6,5]

شجرة +B هي واحدة من طرق هيكلة البيانات (data structure) والتي تستخدم في التطبيقات التي تحتاج إلى ترتيب كمية كبيرة من البيانات أو للتطبيقات التي تحتاج إلى طريقة بحث كفوءة داخل بيانات كبيرة الحجم. نستطيع اعتبار شجرة +B كطريقة فهرسة لقاعدة البيانات (index to database) لذلك تسمى في بعض الأحيان الفهارس (indices).

عند خزن قيد معين في قاعدة بيانات معينة سوف يخزن موقع القيد داخل شجرة +B وكذلك يخزن مفتاح ذلك القيد (key)، فلذلك فإن أوراق (leaves) الشجرة ستكون متكونة من مفتاح كل قيد موجود في قاعدة البيانات علاوة على موقع ذلك القيد (reference number) داخل القاعدة. وعند البحث عن قيد معين داخل قاعدة البيانات، سوف نحتاج إلى معرفة مفتاح ذلك القيد، وشجرة +B ستوفرْ قيمة موقع ذلك القيد داخل قاعدة البيانات، وباستخدام هذه القيمة نستطيع الوصول إلى القيد في

قاعدة البيانات بصورة مباشرة. كما أن محتويات شجرة +B موجودة بالترتيب وهذا يعني إمكانية استرجاع القيود داخل قاعدة البيانات بالترتيب باستخدام شجرة +B.

شجرة +B متوازنة، لاحظ الشكل(1)، والمقصود بهذا أن البحث عن أي مفتاح في أوراق الشجرة (leaves) له نفس العمق، وبسبب هذه الخاصية فإن البحث عن قيد معين داخل ملايين القيود أصبح مضمونا حتى في أسوأ الحالات.

3. أهمية الترميز الرباعي بأستخدام تقنيات الحمض النووي

يُعدُ الحمض النووي هو الوسيلة الاساسية لحفظ وتوارث المعلومات الجينية للخلايا الحية. حيث يقوم بحفظ ونقل المعلومات الخاصة بالخلايا الحية لملايين السنين . وهو يتألف من سلسلتين من النيوكليوتيدات تلتفان حول بعضهما بشكل حلزوني كما هو مبين بالشكل رقم (2). ان حوسبة الحمض النووي بدأت منذ عام 1994 عندما قام العالم ليونارد ادلمان بتجربة اثبت من خلالها امكانية التعامل مع الانظمة الحاسوبية بواسطة الحمض النووي بدون استخدام الالات الحاسوبية وانما بأستخدام الانابيب المختبرية. ان الترميز الشائع في مجال الحاسبات بشكل عام هو الترميز الثنائي او الترميز العشري الذي يعتمد على قيمتين فقط (0,1) كل قيمة تسمى (بت) , وفي هذا الترميز فأن كل 8 بتّات تعادل بايت واحد. اما بالنسبة الى الترميز بالحمض النووي فأن الاعتماد لايكون على البتّات وانما يكون على القواعد النتروجينية الاساسية الاربعة التي تمثل بايت واحد وهي (الادينين(A) , السايتوسين(C), الكوانين(G) والثايمين(T)) بدلا من (0,1) . وهذا يعني ان الترميز بواسطة الحمض النووي يحتاج الى نصف العدد مماهو عليه بالترميز الثاني لكي يكون بايت واحد . [8]

4. الطريقة المقترحة لنظام الاخفاء

في هذه الفقرة سيتم شرح الطريقة المقترحة لنظام الاخفاء ذات المفتاح السري بشكل مفصل . شكل رقم (3) يبين الهيكلية العامة لنظام الاخفاء مع مراحلها الاساسية.

4.1. مرحلة ضغط الرسالة السرية وتحويلها الى أرقام سرية بأستخدام الهيكل الشجري

في هذه الفقرة سيتم تصميم قاموسا الكترونياً يكون ملائماً لاغراض الاخفاء وفي هذا القاموس سنعطي للرسالة كلها رمز واحد وبذلك قللنا حجم البيانات (اي ضغطنا الرسالة السرية) التي سنخفيها داخل الغطاء الرقمي. في هذا القاموس سوف نخزن الرسائل السرية كحدود منطقية وسنستخدم الهيكل الشجري للوصول السريع الى تلك الحدود المنطقية راجع المصدر رقم [9]. الهدف من استخدام هذه الخطوة هو تحويل الرسالة السرية الى مجموعة قليلة من الارقام السرية من خلال الاستفادة من الهيكل الشجري B+-Tree . بطريقة تمنع تكرار هذه الرسائل من أجل توفير كفاءة عالية في استخدام الذاكرة حيث يتم اعطاء لكل رسالة سرية رمز رقمي خاص بها (رمز فريد) وذلك من أجل تجنب مشكلة الغموض عند عملية استرجاع الرسالة السرية. المثال الاتي يوضح كيفية خزن وتحويل الرسائل السرية الى أرقام سرية.

الرسالة السرية الاولى: "تزخر بغداد بالكثير من المعالم التاريخية والحضارية ، واهمها المدرسة المستنصرية" .

الرمز الرقمي لها =1

الرسالة السرية الثانية : "المدينة بغداد القديمة اسماء عديدة كالمدينة المدورة ودار السلام"

الرمز الرقمي لها =2

وهكذا اصبحت الرسالة السرية الكاملة المتكونة هي عبارة عن ارقام سرية **{1,2}**

4.2. مرحلة المعالجة الاولية للرسالة السرية:

بعد المرور بمرحلة الضغط والترميز للرسالة السرية ,سيكون الناتج من تلك المرحلة عبارة عن ارقام سرية .تدخل هذه الارقام السرية المضغوطة الى مرحلة المعالجة الاولية للاخفاء .

حيث تم اقتراح طريقة جديدة للمعالجة في هذه المرحلة ويتم تقسيمها الى قسمين :

4.2.1 مرحلة الترميز للأرقام السرية بأستخدام مفهوم الحمض النووي للتراميز:

في هذه المرحلة يتم تحويل كل رقم سري الى شريط من الحمض النووي (الذي يتألف من اربعة قواعد نتروجينية اساسية وهي (الادينين(A) , السايتوسين(C), الكوانين(G) والثايمين(T)) بدلا من تحويله الى الترميز الثنائي العشري (0,1) الشائع في عمليات الاخفاء وانظمة الحاسبات كما هو مبين بالجدول رقم (1). الهدف الاساسي من استخدام الترميز بالحمض النووي هو من اجل زيادة الاحتمالية بتوقع وجود رسالة سرية مخفية داخل النص عند المتصنتين (المهاجمين) فبدلا من ان يقوم المهاجم بتوقع قيمتين (0,1) سيقوم بتوقع اربعة قيم وهي (A,T,C,G) مما يؤدي الى زيادة التعقيد في كشف الرسالة الرسالة السرية. المثال الاتي يوضح عملية تحويل الارقام السرية الى تراميز الحمض النووي:

جدول رقم (1): تحويل الارقام السرية المضغوطة الى أشرطة من الحمض النووي

الارقام السرية المضغوطة	أشرطة الحمض النووي
0	ATAC
1	AGCT
2	GGCG
. .	. .
251	GACA "فائضة"
255	GAGT "فائضة"

4.2.2. مرحلة تحويل تراميز الحمض النووي الى حركات اعرابية سرية

ان التعامل مع الحركات الاعرابية العربية في هذا البحث المقترح قد أخذ سياقاً جديداً يختلف عما سبقه من البحوث المتعلقة بأستخدام الحركات الاعرابية في الاخفاء. وفيما يلي تقسيم الحركات الاعرابية حسب استخدامها في هذه الطريقة:

أ. الحركات الاعرابيه السرية:

وهي عبارة عن اربع حركات اعرابية (الاكثر شيوعا) داخل النصوص العربية. وهي حركات سرية يجب الاتفاق عليها بين كلا الطرفين (المرسل والمستلم) وتكون ناتجة من تحويل شريط الحمض النووي الى حركات سرية كما هو مبين بالجدول رقم (2) وجدول رقم (3). وتتأثر بعملية الاخفاء (اي تتقلص داخل النص بعد عملية الاخفاء) .

جدول رقم(2): يوضح كيفية تحويل القواعد النتروجينية للحمض النووي الى حركات اعربية سرية			
(ْ) السكون =G	(ِ) الكسرة=C	(َ) الفتحة =T	(ُ) الضمة =A

جدول رقم(3): تحويل أشرطة الحمض النووي الى حركات اعرابية سرية	
الحركات الاعرابية السرية	أشرطة الحمض النووي
ُ َ ُ َ	ATAT
ُ َ ُ ِ	ATAC
ُ َ ِ َ	ATCT
.	.
.	.
ْ ُ ْ ْ	GAGG "فائضة"
ِ ُ ِ ُ	ACAC "فائضة"

ب. الحركة المسيطرة:

وهي حركة سرية يتم اختيارها من الحركات الاعرابية بأستثناء الحركات السرية . حيث يتم الاتفاق عليها بين الطرفين . وهي ولاتتأثر بعملية الاخفاء (اي تبقى على حالها داخل النص قبل وبعد عملية الاخفاء) **مثل الشدّة (ّ)** وسيتم شرحها بالتفصيل عند مرحلة التضمين .

ت. الحركات الاعرابية الغير سرية:

وهي تتمثل بجميع الحركات الاعرابية ما عدا (الحركات السرية والحركة المسيطرة) ولاتتأثر ايضا بعملية الاخفاء (اي تبقى على حالها داخل النص قبل وبعد عملية الاخفاء) مثل تنوين الفتح وتنوين الضم وتنوين الكسر والمدّة.

4.3. مرحلة المعالجة الاولية للنص المراد الاخفاء به (Cover Text) :

وهي مرحلة معالجة أولية يتم تطبيقها على النص المشكّل المراد الاخفاء به (Cover Text) حيث تتمثل المعالجة في هذه المرحلة بعملية تحديد مفاتيح الاخفاء .

تنقسم مفاتيح الاخفاء في هذا البحث المقترح الى مفتاحين اساسيين وهما (مفتاح أبتدائي ومفتاح نهائي) وتعتبر المنطقة الخاصة بالنص المراد الاخفاء بداخله والواقعة بين المفتاح الابتدائي والنهائي هي منطقة الاخفاء الفعليه . وفيما يلي شرح تفصيلي عن دور تلك المفاتيح:-

4.3.1. المفتاح الابتدائي : وهو عن دليل الهدف من وجوده هو تحديد نقطة بداية عملية تضمين الحركات السرية داخل النص المراد الاخفاء بداخله.

ان المفتاح الابتدائي المُختار في هذه الطريقة المقترحة سيكون عبارة عن قاعدة اعرابية نحوية من احدى قواعد اللغة العربية .حيث يتم الاتفاق على هذه القاعدة الاعرابية بين كلا الطرفين (المُرسل والمُستلم) وايضا يتم الاتفاق على ظهورها داخل النص المراد الاخفاء به كما هو موضح بالمثال الاتي حيث سيتم الاتفاق على قاعدة (كان واخواتها) عندما يكون اسمها خبر مقدم (شبه جملة من الجار والمجرور) , الظهور يكون الاول لهذه القاعدة داخل النص وكما هو مبين بالنص الاتي:

النص المراد الاخفاء به

أَيُّهَا النَّاسُ ، اسْمَعُوا قَوْلِي ، فَإِنِّي لَا أَدْرِي لَعَلِّي لَا أَلْقَاكُمْ بَعْدَ عَامِي هَذَا بِهَذَا الْمَوْقِفِ أَبَدًا ؛ أَيُّهَا النَّاسُ ، إِنَّ دِمَاءَكُمْ وَأَمْوَالَكُمْ عَلَيْكُمْ حَرَامٌ إِلَى أَنْ تَلْقَوْا رَبَّكُمْ ، كَحُرْمَةِ يَوْمِكُمْ هَذَا ، وَكَحُرْمَةِ شَهْرِكُمْ هَذَا ، وَإِنَّكُمْ سَتَلْقَوْنَ رَبَّكُمْ ، فَيَسْأَلُكُمْ عَنْ أَعْمَالِكُمْ ، وَقَدْبَلَّغْتُ ، فَمَنْ كَانَتْ عِنْدَهُ أَمَانَةٌ فَلِيُؤَدِّهَا إِلَى مَنْ ائْتَمَنَهُ عَلَيْهَا ، وَإِنَّ كُلَّ رِبًا مَوْضُوعٌ ، وَلَكِنْ لَكُمْ رُءُوسُ أَمْوَالِكُمْ ، لَا تَظْلِمُونَ وَلَا تُظْلَمُونَ . قَضَى اللَّهُ أَنَّهُ لَا رِبَا ، وَإِنَّ رِبَا عَبَّاسِ بْنِ عَبْدِ الْمُطَّلِبِ مَوْضُوعٌ كُلُّهُ ، وَأَنَّ كُلَّ دَمٍ كَانَ فِي الْجَاهِلِيَّةِ مَوْضُوعٌ ، وَإِنَّ أَوَّلَ دِمَائِكُمْ أَضَعُ دَمُ ، وَكَانَ مُسْتَرْضَعًا فِي بَنِي لَيْثٍ ،فَقَتَلَتْهُ هُذَيْلٌ فَهُوَ أَوَّلُ مَا أَبْدَأُ بِهِ مِنْ دِمَاءِ الْجَاهِلِيَّةِ . أَمَّا بَعْدُ أَيُّهَا النَّاسُ.

وكما هو موضح بالمثال اعلاه فأن الطريقة المقترحة قامت بأستخراج القاعدة الاعرابية (**كَانَ فِي الْجَاهِلِيَّةِ**) المتفق عليها بين الطرفين وحسب الظهور الاول لها واعتبارها نقطة بداية لعملية التضمين .

4.3.2. المفتاح النهائي : سيتم شرحه بالتفصيل ضمن مرحلة التضمين داخل النص المراد الاخفاء به (Cover Text)

4.4. مرحلة التضمين داخل النص المراد الاخفاء به (Cover Text) :

وهي مرحلة اخفاء وتضمين الحركات السرية داخل النص العربي المشكّل(Cover Text). و في هذه المرحلة تم اقتراح واستحداث عدة تقنيات وذلك من اجل الحفاظ على جودة الاخفاء وعدم تمكين المتصنتين من الشك بوجود رسالة سرية مخفية او محاولة كشفها داخل ذلك النص.

بعدما يتم تحديد المفتاح الابتدائي (القاعدة الاعرابية) تبدأ عملية التضمين وحسب مايلي:-

أ. يقوم النظام بأختيار أول حركة اعرابية سرية من الحركات السرية ومقارنتها مع أول حركة موجودة بالنص المراد الاخفاء به بعد القاعدة الاعرابية . فأذا كانت كلا الحركتين متطابقتين فهذا يعني بقاء الحركة ذاتها بنفس موقعها داخل النص المراد الاخفاء به .اما اذا كانت غير متطابقة فيتم حذف الحركة من النص والانتقال الى حركة اخرى (الحركة التالية) واعادة مقارنتها مرة اخرى مع الحركة السرية .تستمر هذه العملية لحين مطابقة أول (أربع حركات سرية) وبعد ذلك يبقى النص (cover) محافظا على حركاته بعدم حذف اي حركة منها لحين ظهور الحركة المسيطرة وكما هو مبين بالمثال الاتي:

الحركات السرية هي: ًٌٍَُِّْ

عملية تضمين اول اربع حركات سرية بعد ظهور القاعدة الاعرابية هي كما يلي :

أَيُّهَا النَّاسُ ، إِنَّ دِمَاءَكُمْ وَأَمْوَالَكُمْ عَلَيْكُمْ حَرَامٌ إِلَى أَنْ تَلْقَوْا رَبَّكُمْ ، كَحُرْمَةِ يَوْمِكُمْ هَذَا ، وَكَحُرْمَةِ شَهْرِكُمْ هَذَا ، وَإِنَّكُمْ سَتَلْقَوْنَ رَبَّكُمْ ، فَيَسْأَلُكُمْ عَنْ أَعْمَالِكُمْ ، وَقَدْ بَلَّغْتُ ، فَمَنْ كَانَتْ عِنْدَهُ أَمَانَةٌ فَلْيُؤَدِّهَا إِلَى مَنْ ائْتَمَنَهُ عَلَيْهَا ، وَإِنَّ كُلَّ رِبًا مَوْضُوعٌ ، وَلَكِنْ لَكُمْ رُءُوسُ أَمْوَالِكُمْ ، لَا تَظْلِمُونَ وَلَا تُظْلَمُونَ . قَضَى اللَّهُ أَنَّهُ لَا رِبَا ، وَإِنَّ رِبَا عَبَّاسِ بْنِ عَبْدِ الْمُطَّلِبِ مَوْضُوعٌ كُلُّهُ ، وَأَنَّ كُلَّ دَمٍ كَانَ فِي الْجَاهِلِيَّةِ مَوضُوعٌ ، وَإِنَّ أَوَّلَ دِمَائِكُمْ أَضَعُ دَمُ ابْنِ رَبِيعَةَ بْنِ الْحَارِثِ بْنِ عَبْدِ الْمُطَّلِبِ ، وَكَانَ مُسْتَرْضَعًا فِي بَنِي لَيْثٍ ، فَقَتَلَتْهُ هُذَيْلٌ فَهُوَ أَوَّلُ مَا أَبْدَأُ بِهِ مِنْ دِمَاءِ الْجَاهِلِيَّةِ

ب. **الحركة المسيطرة:** وهي عبارة عن حركة سرية ايضا يتم الاتفاق عليها بين كلا الطرفين وتقوم بعملية الفصل بين كل اربع حركات سرية. الهدف منها هو الابتعاد عن لفت الانتباه والانظار عن منطقة التضمين الفعليه داخل النص اضافة الى انها تزيد من امكانية التطابق بين النص قبل الاخفاء وبعده مماسؤدي الى زيادة كفاءة وجود نظام الاخفاء المقترح.

ت. بعد ظهور الحركة المسيطرة تبدأ عملية تضمين ثاني (اربع حركات سرية) بنفس طريقة التضمين السابقة ولحين الوصول الى الحركة المسيطرة مرة اخرى. وهكذا تستمر عملية التضمين والوقوف عند الحركة المسيطرة لحين الانتهاء من سلسلة الحركات السرية. لكن, كيف للطرف الثاني (المُستلم) ان يتمكن من معرفة انَّ عملية الاخفاء (التضمين) قد انتهت؟؟؟

في هذا البحث تم حل هذه المشكلة من خلال استخدام مفتاح نهائي للتضمين وكما يلي شرح تفصيلي حول كيفية اختيار المفتاح النهائي :

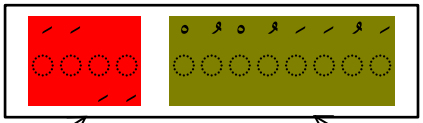
4.4.1. المفتاح النهائي للاخفاء:

وهو عبارة عن دليل, الهدفُ من وجوده هو تحديد نقطة للاشارة الى نهاية عملية التضمين داخل النص.في هذا البحث المقترح سيتم الاعتماد على احدى تراميز الحمض النووي الغير مستخدمة وكما موضحة بالجدول رقم (3) حيث ان الاعتماد على طريقة الترميز بالحمض النووي قد تمت صياغتها بأسلوب يضمن دائما وجود تراميز فائضة عن الحاجة .. هذه التراميز تعتبر غير سرية ويمكن الاتفالق على واحدة منها مع الطرف الثاني لتكون بمثابة مفتاح نهائي للتضمين.

4.4.2. آلية عمل المفتاح النهائي للتضمين :

المفتاح النهائي هو عبارة عن ترميز بالحمض النووي غير سري اي عبارة عن اربع حركات اعرابية غير سرية تندمج بنهاية سلسلة الحركات السرية ويتم تضمينها داخل النص المراد الاخفاء به بنفس طريقة تضمين الحركات السرية. وبما ان المفتاح النهائي متفق عليه بين الطرفين , فأن الطرف الثاني عندما يقوم بعملية استخراج الحركات السرية من (Cover Text) فأنه سوف يصل الى المفتاح النهائي ويتوقف. كما هو مبين بالمثال الاتي:

الحركات السرية مدمجة مع المفتاح النهائي الذي هو عبارة عن اربع حركات غير سرية وكما موضح ادناه:



المفتاح النهائي **الحركات السرية**

النص بعد عملية التضمين (Stego Text)

أَيُّهَا النَّاسُ ، إِنَّ دِمَاءَكُمْ وَأَمْوَالَكُمْ عَلَيْكُمْ حَرَامٌ إِلَى أَنْ تَلْقَوْا رَبَّكُمْ ، كَحُرْمَةِ يَوْمِكُمْ هَذَا ، وَكَحُرْمَةِ شَهْرِكُمْ هَذَا ، وَإِنَّكُمْ سَتَلْقَوْنَ رَبَّكُمْ ، فَيَسْأَلُكُمْ عَنْ أَعْمَالِكُمْ ، وَقَدْبَلَّغْتُ ، فَمَنْ كَانَتْ عِنْدَهُ أَمَانَةٌ فَلِيُؤَدِّهَا إِلَى مَنْ ائْتَمَنَهُ عَلَيْهَا ، وَإِنَّ كُلَّ رِبًا مَوْضُوعٌ ، وَلَكِنْ لَكُمْ رُءُوسُ أَمْوَالِكُمْ ، لَا تَظْلِمُونَ وَلَا تُظْلَمُونَ . قَضَى اللَّهُ أَنَّهُ لَا رِبَا ، وَإِنَّ رِبَا عَبَّاسِ بْنِ عَبْدِ الْمُطَّلِبِ مَوْضُوعٌ كُلُّهُ ، وَأَنَّ كُلَّ دَمٍ كَانَ فِي الْجَاهِلِيَّةِ مَوضُوعٌ ، وَإِنَّ أَوّل دمائكُمْ أضعُ دم ابْنِ رَبِيعَةَ بْنِ الْحَارِثِ بْنِ عَبْدِ الْمُطّلِبِ ، وَكَانَ مُسْتَرْضَعًا فِي بَنِي لَيْثٍ ، فَقَتَلَتْهُ هُذَيْلٌ فَهُوَ أَوَّلُ مَا أَبْدَأُ بِهِ مِنْ دِمَاءِ الْجَاهِلِيَّةِ

المفتاح الابتدائي (قاعدة اعرابية)

حركات المفتاح النهائي

4.5. النتائج والمقاييس

في هذه الفقرة سيتم تطبيق المقاييس الاكثر شيوعا للأخفاء داخل النصوص وذلك من اجل اختبار النتائج العملية للطريقة المقترحة اعلاه ومن ثم مقارنتها مع ألاعمال السابقة الاخرى ضمن هذا المجال في الاخفاء.

سيتم الاعتماد على تقييس جودة الاخفاء بأستخدام مقياسيين اساسيين وهما : **مقياس السعة** و الذي يعمل على تقييس قدرة وسعة النص العربي المشكّل على تضمين واستيعاب حجم المعلومات السرية المُراد اخفاءها بداخِله. **و مقياس الشفافية** الذي يعمل على تقييس مدى توقع المهاجمين والمتنصتين على وجود معلومات سرية مُضمّنة داخل النص العربي المشكّل وقدرتهم على استخراج تلك المعلومات السرية من النص.

4.5.1. مقياس السعة

يتم اختبار سعة نظام الاخفاء مع عدة نصوص عربية مُشكّلة . جدول رقم (4) يوضح نسب السعة الخاصة بكل نص في هذا النظام بالاعتماد على المعادلة الاتية :

معادلة رقم (1) نسبة السعة (بالبايت) =حجم البيانات المراد اخفاءها \ حجم النص الذي سيتم الاخفاء به

أما جدول رقم (5) يوضح نسب السعة الخاصة ببقية الطرق السابقة للآخفاء داخل لنصوص العربية

جدول رقم(4) يوضح سعة الاخفاء للطريقة المقترحة لعدة نصوص عربية مشكّلة				
رقم الاختبار	حجم الرسالة السرية (بايت)	حجم المساحة المستغلة من النص العربي المُشكّل الذي تم الاخفاء به (بايت)	نسبة سعة الاخفاء(%)	معدل سعة الاخفاء (%)
أختبار رقم (1)	1900	1929	98	79
أختبار رقم (2)	1900	2229	85	
أختبار رقم(3)	1900	3549	54	
أختبار رقم (4)	902	787	115	91
أختبار رقم(5)	902	1033	87	
أختبار رقم(6)	902	1262	71	
أختبار رقم(7)	500	482	104	106.4
أختبار رقم(8)	500	491	102	
أختبار رقم (9)	500	442	113	

جدول رقم(5) يوضح سعة الاخفاء للطرق السابقة	
عنوان ومصدر الطريقة	معدل سعة الاخفاء لها(%)
الطريقة المعتمدة في المصدر رقم [10]	74.32
الطريقة المعتمدة في المصدر رقم[11]	33.68
الطريقة المعتمدة في المصدر رقم[12]	8.019
الطريقة المعتمدة في المصدر رقم[13]	10.25
الطريقة المعتمدة في المصدر رقم[3]	6.40

من خلال الجداول اعلاه يتبين لنا مدى قوة ومثاليه نظام الاخفاء المقترح من حيث مفهوم السعة وذلك من خلال توفير سعة عالية جدا ومثالية مقارنة مع بقية الطرق السابقة . حيث نجح هذا النظام في اخفاء كميات كبيرة جدا من البيانات السرية في حجم صغير من النصوص والسبب في ذلك يعود الى استخدام تقنيات الهيكل الشجري في عملية ضغط الرسالة السرية وتقنيات الحمض النووي في عملية الترميز .

4.5.2. مقياس الشفافية

في هذه الفقرة سيتم اختبار نظام الاخفاء المقترح من جانب الشفافية او(الأمنية) . ومن أجل فهم معنى الشفافية للأخفاء سيتم اختبار التطابق(Similarity) بين النص قبل عملية التضمين وبعد تضمين الرسالة السرية بداخله واختبار مدى التشابه والاختلاف بين كلا النصين . يتم ذلك من خلال استخدام مقاييس التطابق الاتية:

1. مقياس (جارو ونكلر) للتشابه . راجع المصدر رقم (14)
2. مقياس (دايمراو-ليفينشتين) للمسافات. راجع المصدر رقم (14)

4.5.2.1. مقياس (جارو ونكلر) للتشابه

يعتبر مقياس جارو أحد مقاييس التشابه التي تقوم بقياس نسبة مدى التطابق بين كلمتين حسب المعادلات الاتية.

t= $\left\lfloor \frac{\max(|s_1|,|s_2|)}{2} \right\rfloor - 1$ معادلة رقم (2)

$$d_j = \frac{1}{3}\left(\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m}\right)$$ معادلة رقم (3)

حيث ان:

s: تمثل طول الكلمة

m : تمثل عدد الحروف المتطابقة

t: تمثل عدد مرات التحولات وتحسب من المعادلة رقم (2)

d: يمثل مقياس جارو

جدول رقم(6) يمثل مقياس جارو لنظام الاخفاء المقترح حيث يتم تطبيقة على 6 نصوص .أما جدول رقم (7)يمثل مقياس جارو لبقية الطرق السابقة للأخفاء لكن داخل النصوص الانكليزية

جدول رقم (7)يمثل مقياس جارو لبقية الطرق السابقة داخل النصوص الانكليزية	
مقياس جارو للتشابه	الطريقة السابقة ومصدرها
0.8771	الطريقة المعتمدة في المصدر رقم[15]
0.443	الطريقة المعتمدة في المصدر رقم[16]
0.95	الطريقة المعتمدة في المصدر رقم[17]

جدول رقم(6) يمثل مقياس جارو لنظام الاخفاء المقترح	
مقياس جارو للتشابه	رقم الاختبار
0.7913	اختبار رقم(1)
0.8188	اختبار رقم(2)
0.8214	اختبار رقم(3)
0.9024	اختبار رقم(4)
0.8231	اختبار رقم(5)
0.8412	اختبار رقم(6)

من الجدولين اعلاه يتضح لنا ان نسبة التطابق بين النصين هي عالية جدا مقارنة مع بقية الاعمال السابقة . ومن الجدير بالذكر اننا قمنا بتطبيق طريقة جارو ونكلر على الحركات العربية المشكلة الخاصة بالنص وذلك لان التطابق بالحروف هو موجود اصلا وبشكل تام (اي ان طريقة الاخفاء المقترحة لم تتأثر بها الحروف نهائيا . وانما فقط الحركات).

4.5.2.2. مقياس (دايمراو- ليفينشتين) للمسافات

في نظرية علوم الحاسبات , يعد (دايمرا- ليفينشتين) هو مقياس للمتباعد بين كلمتين . حيث يتم حساب اقل عدد ممكن من العمليات الضرورية للتحويل من الكلمة الاولى للكلمة الثانية وهذه العمليات هي (اضافة , حذف, تبادل بين حرف واخر او تحويل من حرف لاخر). اذا كانت النسبة المئوية الناتجة عند تطبيق هذه الطريقة هي كبيرة فهذا يعني ان الاختلاف كبير بين كلا الكلمتين . والعكس صحيح . ان استخدام هذا المقياس قد تم على عدة نصوص وكانت النتيجة مثالية وعالية جدا كما هو مبين بالجدول رقم (8)عندما تمت مقرنتها مع طريقتين اخرتين من الطريق السابقة للاخفاء داخل النصوص الانكليزية الموضحة بالجدول رقم (9).

جدول رقم (8) يبين مقياس (دايمراو- ليفينشتين) للنظام الاخفاء المقترح		
النسبة المئوية لعدد الاختلافات بين النص قبل وبعد الاخفاء	عدد الاختلافات	رقم الاختبار
18.24%	127	اختبار رقم(1)
16.93%	93	اختبار رقم(2)
17.39%	103	اختبار رقم(3)

اختبار رقم(4)	125	12.13%
اختبار رقم(5)	82	18.51%
اختبار رقم(6)	184	23.98%

جدول رقم (9) يبين مقياس (دايمراو- ليفينشتين) للبقية الطرق السابقة للأخفاء

الطريقة السابقة	عدد الاختلافات
Khan's method (I) [17]	282
Khan's method (II) [17]	326

6. الاستنتاجات

من هذا البحث تم التوصل الى الاستنتاجات الاتية:

1. اللغة العربية أنسب من اللغات الاخرى في موضوع الاخفاء وذلك لوجود ميزة التشكيل التي تنفرد بها اللغة العربية.
2. تحويل الرسالة السرية بكاملها الى رمز وحيد يقلل من البيانات المراد اخفاءها وبالتالي يوفر كفاءة في منظومة الاخفاء.
3. استخدام قاموس ذو هيكل بياني شجري من نوع +B لخزن واسترجاع الرسائل السرية يزيد من كفاءة منظومة الاخفاء وذلك من خلال زيادة سرعة تحويل الرسالة السرية الى رمز وزيادة سرعة استرجاع الرسالة السرية من الرمز وكذلك من خلال التخلص من الغموض حيث ان هناك رسالة واحدة فقط للرمز الواحد.
4. ان اختيار قاعدة اعرابية معينة داخل النص المراد الاخفاء به (cover) كمفتاح ابتدائي للاخفاء واختيار التشكيل يزيد من كفاءة منظومة الاخفاء لانه غير مثير للشكوك.
5. ان اختيار احدى اشرطة الحمض النووي لكي تكون مفتاح نهائي للأخفاء يزيد من صعوبة توقع المهاجمين لهذا الشريط .
6. ان استخدام الحركة المسيطرة داخل النص المراد الاخفاء به (cover) يقلل السعة بشكل طفيف لكنّه يُبعد لفت الانظار عن منطقة الاخفاء الفعلية .
7. بالاعتماد على الطرق الشائعة في تقييس الاخفاء داخل النصوص. فان الطريقة المقترحة في هذا البحث قد اعطت نتائج ممتازة ومثالية في تحقيق السعة(102%, 115%,98%) والشفافية (0.902 ,0.8412) للأخفاء عندما تمت مقارنتها مع بعض الاعمال السابقة.

المراجع

[1] علي، د.نبيل، "اللغة العربية والحاسوب دراسة بحثية"، تعريب للنشر/الكويت 1988م.

[2] Adnan. Gutub, Lahouari M. Ghouti, Yousef S.Elarian, Sameh M. Awaideh, Aleem K. Alvi *," **Utilizing Diacritic Marks for Arabic Text Steganography",*** Kuwait Journal of Science & Engineering (KJSE),2010.

[3] Rehab F. Hassan Dr. Nidaa F. Hassan*, "Data hiding in Arabic text based on Letters, Diacritics and Extension",* First Information Technology Conference, Iraq, April, 2009.

[4] Auday Jamal Fawzi ***,"Data Hiding in Arabic Text",*** PhD thesis , University of Technology , Iraq ,January,2007

[5] Krenn, R., "**Steganography Implementation & Detection**", 2004, www.krenn.nl/univ

[6] Niels, P. Peter, H., "**Hide and Seek: An Introduction to Steganography**", IEEE Security & Privacy, 2003, www.**pdf**-search-engine.com

[7] Hala, B. Abdul Wahab, "**Information Hiding in Written Text Using Context- Free Grammar (CFG)**", MSc. Thesis, university of Technology, Computer Science department, Iraq, 2001.

[8] Hasanen Samir, "***An improvement DNA computing Approach Using Heuristic Technique",*** PhD Thesis , University of Technology ,Iraq, August, 2008.

[9] Suhad M. Kadhem***," Using B+ Tree To Represent Secret Messages For Steganography Purpose"***, Eng.& Tech Journal, Vol (28),No(15),Iraq , March 2010.

[10] M. Hassan Shirali-Shahreza, Mohammad Shirali- Shahreza, ***"A New Approach to Persian/Arabic Text Steganography,"*** 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 06), July 2006.

[11] Adnan Gutub , Manal Fattani, ***"A Novel Arabic Text Steganography Method Using Letter Points and Extensions",*** WASET International

Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria, May ,2007.

[12] F. Al-Azawi, Moayad Fadhil, ***"Arabic Text Steganography using Kashidaa Extensions with Huffman code*** ", Asian network for Science Information, 2010.

[**13]** Adnan Abdul-Aziz Gutub, Wael Al-Alwani, and Abdulelah Bin, Mahfoodh ***"Improved Method of Arabic Text Steganography Using the Extension Kashida Character*****",** Bahria University Journal of Information & Communication Technology, December, 2010.

[14] Adil Enaanai, Abdelaziz Doukkali, Boubker Regragui ***"Noise Abatement IN The Arabic IRS Result By Applying A Sentence Morphosemantic Filter (Gene Filter Method)",*** Journal of Theoretical and Applied Information Technology,. Vol. 42 No.1, 15 August 2012.

[15] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal ***," A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method(WMM)",*** International Journal of Computer and Information Engineering ,2010.

[16] Khan Farhan Rafat, M. Sher ***"On the Limits of Perfect Security for Steganographic System"***, Department of Computer Science, International Islamic University Islamabad, 44000, Pakistan, Oct ,2013.

[17] Monika Agarwal ***,"Text Steganographic Approach : A comparison",*** International Journal of Network Security & Its Applications (IJNSA), Vol (5), No(1), Jabalpur, India, January 2013.