Scientific Journal of Faculty of Education, Misurata University-Libya, Vol. 1, No. 13, Jun. 2019

Published online in June

المجلة العلمية لكلية التربية، جامعة مصراتة، ليبيا، المجلد الأول ـ العدد الثالث عشر، يونيو 2019م

الدمج بين التشفير والإخفاء لتأمين إرسال رسالة نصية

Combining Encryption and Concealment to Secure the Transmission of Text Messages

مصطفى رمضان السريتي

m.essraiti@edu.misuratau.edu.ly

هشام محمد المهدوي

helmehdwi@gmail.com

Abstract:

With the increasing exchange of data between individuals and institutions across various electronic communications, the protection of valuable data is in demand to ensure that it is not hacked and to maintain privacy. To avoid security breaches, many protection techniques such as encryption and steganography have emerged. The purpose of this research is to integrate cryptographic and steganography techniques to secure text message sending. The Rijndael algorithm was used to encrypt the text message, and the Least Significant Bit algorithm was also used to hide the encrypted message in a color image. Experiments on the proposed system has shown its ability to increase the security of sent messages because of the inability of the human eye to distinguish the original image from the image after being covered, and the encryption of the message by using a password.

ملخص:

في ظل التبادل المتزايد للبيانات بين الأفراد والمؤسسات عبر وسائل الاتصالات الإلكترونية المختلفة، تتزايد الحاجة لحماية البيانات القيمة، لضمان عدم تعرضها للاختراق والقرصنة؛ وذلك للحفاظ على الخصوصية. ولتفادي الخروقات الأمنية ظهرت العديد من تقنيات الحماية مثل التشفير والإخفاء.

يهدف هذا البحث لدمج تقنيتي التشفير والإخفاء، لتأمين إرسال رسالة نصية، حيث أُستخدمت خوارزمية ريجنديل لتشفير الرسالة النصية، وخوارزمية البت الأقل أهمية لإخفاء الرسالة المشفرة داخل صورة ملونة. وقد أظهرت التجارب التي أجريت على النظام المقترح قدرته على زيادة تأمين الرسائل المرسلة وذلك

من خلال عدم قدرة العين البشرية على تمييز الصورة الأصلية من الصورة بعد التغطية، وتشفير الرسالة باستخدام كلمة سر.

1. مقدمة:

مع التطور المستمر في مجال الحاسوب والاتصالات، زادت حاجة المستخدمين بمختلف تصنيفاتهم لتبادل البيانات وإرسالها عبر الوسائط المختلفة من مكان لآخر حول العالم، وبعد ظهور الإنترنت، ونتيجة التطور الكبير الذي حدث في تطبيقاتها أصبحت الوسط الأكثر شيوعا لتبادل البيانات، حيث يوجد العديد من الطرق الممكنة لإرسال البيانات باستخدام الإنترنت مثل البريد الإلكتروني، والمحادثات، وسائط التواصل الاجتماعي.... إلخ. وباعتبار الإنترنت شبكة اتصال عامة يمكن للجميع الدخول إليها واستعراض البيانات فيها، الأمر الذي يجعل إرسال البيانات خلالها يواجه عدة مشاكل منها مشكلة التهديد الأمني، حيث يمكن سرقة أو قرصنة البيانات الشخصية أو السرية بعدة طرق. ولأن نظام الاتصال الجيد يوفر ثلاث خصائص مهمة: السرية والموثوقية والسلامة (Kobayashi, et al., 2009). السرية تضمن أن الأفراد المخولين فقط لهم الحق في الوصول إلى المعلومات المتبادلة، أما الموثوقية فتتيح التحقق من منشأ المعلومات المتبادلة ومالكها، في حين تضمن السلامة عدم تعديل المعلومات المتبادلة أو العبث بها. السرية ضرورية لمنع الوصول غير القانوني إلى البيانات المرسلة، في حين أن الموثوقية والسلامة مطلوبتان للتحقق من الملكية والكشف عن التلاعب في البيانات المستلمة. ولأن الخصائص الثلاث السابقة تتحقق من خلال حماية وتأمين المعلومات المتداولة عبر نظم الاتصالات المختلفة، فقد حاز أمن المعلومات على اهتمام كبير في العقود القليلة الماضية، إذ وصلت العديد من جرائم الإنترنت مثل التزوير، والتعديل، والقرصنة إلى مستويات خطيرة، ولذلك فإن قضية أمن المعلومات ظلت مقلقة وتحتاج إلى حلول متجددة. من هنا زادت الحاجة لحماية المعلومات السرية والمهمة، ما أدى إلى ظهور علم التشفير (Cryptography) لتحقيق ذلك، ويعتبر من الحلول المعروفة والشائعة لحماية البيانات. باستخدام مفهوم التشفير تصبح الرسالة غير قابلة للقراءة، حيث يحقق تشفير الوسائط الرقمية مثل الصوت، والصورة، ومقاطع الفيديو معدل حماية مرتفع، ولكن تشفير الرسائل الرقمية يجعلها لافتة لانتباه المتطفلين كونها ترسل بشكل مشفر واضح بدون إخفاءها مما يدل على أهميتها. وعلى الرغم من التطور الذي صاحب علم التشفير وتقنياته، باستخدام خوارزميات تشفير مختلفة تُطوَّر باستمرار، إلا أنه بالمقابل تُستحدث باستمرار خوارزميات وأساليب مضادة لفك التشفير وسرقة البيانات المرسلة عبر الإنترنت، ما أدى إلى فقدان الخصوصية وسرية البيانات، وهذا ما دعا إلى البحث عن أساليب أخرى

لحماية الرسائل الرقمية، مثل إخفاء البيانات (Steganography)، الذي يعد أسلوبًا جيدا لتجاوز مشكلة وضوح البيانات أثناء الإرسال (Fouad, 2017 p. 545).

ظهرت تقنية تغطية أو إخفاء المعلومات (Information Steganography)، لتقدم أداة جديدة تسهم في زيادة أمن وسرية المعلومات، وتعتمد على إخفاء (تضمين) المعلومات (Information Embedding) داخل ناقل المعلومات (Information Carrier) بحيث تكون الرسالة معلومة فقط لدى المخولين (المرسل والمستلم)، وغير معلومة من قبل المتسللين أو المتطفلين ولا يمكنهم إدراكها.

وبشكل عام، فإن الغرض من التشفير هو حماية سرية وتكامل الرسالة المرسلة وذلك بتشفير محتوياتها، بينما إخفاء البيانات يسعى لتحقيق نفس الهدف عن طريق إخفاء بتات الرسالة المرسلة داخل بتات الوسط المضيف (Zinaly, et al., 2017).

يسعى هذا البحث للدمج بين تقنيتي التشفير والإخفاء لزيادة تأمين رسالة نصية أثناء إرسالها عبر وسائل الاتصال المختلفة.

2. مشكلة البحث:

تكمن مشكلة البحث في قدرة المتطفلين على شبكات الاتصال والمتسللين إليها على اختراق هذه الشبكات بالرغم من وجود وسائل حماية ضد التسلل مثل كلمات المرور والجدران النارية، وقدرتهم على فك الرسائل المشفرة التي يتم تبادلها عبر هذه الشبكات بالرغم من تطور خوارزميات التشفير وتحديثها باستمرار، الأمر الذي أدى إلى تزايد الحاجة إلى وجود بدائل وأدوات أخرى تزيد من صعوبة وصول هؤلاء المتسللين إلى البيانات ومعرفة محتواها، وتتزايد هذه الحاجة كلما زادت أهمية وسرية هذه البيانات.

3. هدف البحث:

الهدف من البحث هو استعراض خوارزميات تشفير وإخفاء البيانات المختلفة، وتطبيق إحدى خوارزميات الإخفاء على رسائل نصية بعد القيام بتشفيرها باستخدام إحدى خوارزميات التشفير؛ لإخفائها داخل صورة ملونة. والخوارزميتان المطبقتان في هذا البحث هما: خوارزمية ريجنديل (Rijndael) للتشفير، وخوارزمية البت الأقل أهمية LSB (Least Significant Bit) للإخفاء. وستطبق هاتان الخوارزميتان باستخدام لغة VB.Net على مجموعة مختلفة من الصور ونصوص مختلفة الطول، للوقوف على قدرة هذه

الآلية على زيادة حماية البيانات من المتطفلين عند إرسالها بين المستخدمين، واسترجاعها فيما بعد بشكل يحافظ على النص الأصلي كما هو بدون تغيير.

4. أمن المعلومات (Information Security):

يشمل أمن المعلومات ثلاثة مكونات وهي (قنديلجي، وآخرون، 2012 الصفحات 175-176):

أ. سرية المعلومات: ويشمل هذا الجانب كافة التدابير اللازمة لمنع اطلاع الأشخاص غير المصرح لهم على المعلومات الحساسة أو السرية.

ب. سلامة وأمان المعلومات: أي اتخاذ التدابير اللازمة لحماية المعلومات من التغيير.

ج. ضمان الوصول إلى المعلومات والموارد الحاسوبية: أي توفر المعلومات بشكل دائم للمخولين بالوصول إليها.

ويمكن اعتبار النظام آمنًا أو غير آمن إذا حقق الخصائص الرئيسية للمعلومات عند تداوله لهذه المعلومات، والتي في مجملها لها علاقة بحماية المعلومات من الاختراق بهدف سرقتها أو التلاعب بها، ومن هذه الخصائص الإتاحة أو التوفر (Availability)، والدقة (Accuracy)، والوثوقية أو الصحة (Authenticity)، والسرية (Confidentiality)، السلامة والتكامل (Integrity). (Whitman, et al., 2012).

5. الهجمات الأمنية (Security Attacks):

يتم إرسال البيانات من المصدر (source) لتصل إلي الهدف (destination) وهذا يعرف بالتدفق الطبيعي للبيانات (Normal Flow). ولكن من الممكن أن يقوم بعض المهاجمين (hackers) باختراق الشبكة لغرض الوصول أو تعديل البيانات الأصلية، وهذا ما يعرف بالهجمات الأمنية، حيث يمكن للمهاجم مقاطعة هذا التدفق الطبيعي للبيانات بتنفيذ تقنيات الاختراق المختلفة على البيانات والشبكة الناقلة، مثل المقاطعة (Interruption)، والاعتراض (Interception)، والتعديل (Modification)، والتلفيق أو الفبركة (Fabrication). جميع هذه الأنواع من الهجمات حال حدوثها تجعل النظام غير آمن، وبالتالي يصبح غير قادر على تحقيق الخصائص الرئيسية للمعلومات.

في ظل وجود هذه الاختراقات الأمنية التي تحاول تغيير البيانات الأصلية، تصبح حماية البيانات من الاختراق مهمة مستمرة لأي مؤسسة أو فرد يقوم بإرسال البيانات، وذلك بتنفيذ عدة مقاييس أو طرق أمنية تتضمن الوقاية، والاكتشاف، والاستجابة، والاستعادة.

6. طرق منع الهجمات الأمنية:

توجد طرق منهجية مختلفة لمنع الهجمات الأمنية، وهي كالتالي:

1.6 التشفير (Cryptography):

"كلمة التشفير (Cryptography) مشتقة من اللغة الإغريقية وتتألف من مقطعين crypto تعني السرية وgraphy وتعني الكتابة، أي الكتابة السرية" (حسين، 2010 صفحة 43). ويعرف التشفير بأنه: "عملية ترميز الرسالة حتى يكون معناها غير مفهوم" (الحمامي، وآخرون، 2007). وبالتالي هي عملية خلط أو تشويش للنص الأصلي وذلك بإعادة ترتيب واستبدال النص الأصلي وتنظيمه ليظهر بشكل غير قابل للقراءة من قبل الآخرين، فهو طريقة فعالة لحماية المعلومات المرسلة خلال شبكة الاتصال.

علم التشفير (Cryptology) هو العلم المختص بالتشفير وتحليل المشفر. فالتشفير هو منهجية لإرسال الرسائل بشكل سري وآمن إلي الهدف. أما تحليل المشفر فهو طريقة الحصول على النصوص الأصلية من الرسائل المضمنة بها تلك النصوص (Whitman, et al., 2012).

بشكل عام، التشفير هو إرسال البيانات من المصدر إلي الهدف بعد تعديلها باستخدام شفرة برمجية أمنية. وتستخدم نظم التشفير كلاً من النص الأصلي ومفتاح سري (Secret Key) كإدخال وتوليد نص مشفر (Cipher Text) باستخدام خوارزمية تشفير محددة.

أهم عناصر نظم التشفير هي:

أ. النص الأصلي (Plain text): هو الجزء الأصلي من المعلومات المطلوب إرسالها للهدف.

ب. خوارزمية التشفير (Encryption algorithm): هي المفتاح الأساسي لأي نظام تشفير، حيث تقوم خوارزمية التشفير بتعريض النص الأصلي لعدة استبدالات وتحويرات.

ج. المفتاح السري (Secret key): يعطى بواسطة المستخدم، ويمثل إدخالاً لخوارزمية التشفير، التي تنفذ العديد من الاستبدالات والتحويرات بشكل مختلف بناءً على هذا المفتاح.

د. النص المشفر (Cipher text): يمثل مخرجات (output) خوارزمية التشفير. وهو نص مختلط، ويختلف في كل مرة حسب المفتاح السري الممنوح لخوارزمية التشفير.

يرتبط عمل التشفير بإيجاد خوارزميات تستخدم لتحقيق الآتي:

- إخفاء محتوى الرسائل عن الجميع عدا المخولين لتوفير الخصوصية والسرية.
- التحقق من صحة الرسائل لدى المستلم أي التخويل.

1.1.6 خوارزميات التشفير (Cryptographic Algorithms):

توجد عدة خوارزميات تشفير تختلف حسب نوع التشفير المستخدم، ويمكن تقسيمها حسب معيار التشفير المستخدم إلى نوعين (Stallings, 2013):

أ. خوارزمية التشفير الغير تماثلي (Asymmetric encryption algorithm):

يعرف بتشفير المفتاح العام (Public key encryption). وفيه تتم عمليتي التشفير وفك التشفير بمفتاحين مختلفين، مفتاح للتشفير ومفتاح آخر لفك التشفير.

في التشفير الغير متماثل، البيانات المشفرة بمفتاح عام (Public Key) يمكن فك تشفيرها فقط باستخدام نفس الخوارزمية، والرسالة المشفرة باستخدام مفتاح خاص (Private Key) يمكن فك تشفيرها فقط باستخدام المفتاح العام المطابق.

المشكلة الرئيسية للتشفير الغير متماثل هي مفاتيح التشفير (Cipher Keys). فكلما أراد شخصان مختلفان تبادل البيانات في نفس الوقت باستخدام التشفير الغير متماثل فإنهما يحتاجان معاً لأربعة مفاتيح مختلفة (اثنان لكل واحد منهما). فيصبح الأمر أكثر إرباكاً، حيث أن كل ملف يحتاج للمفتاح المطابق ليتم فتحه.

ب– خوارزمية التشفير التماثلي (Symmetric encryption algorithm):

هو تشفير يتم باستخدام مفتاح وحيد ويعرف بالتشفير التقليدي (Conventional Encryption)، كما يعرف بتشفير المفتاح الخاص (Private Key Cryptography). بشكل عام خوارزمية التشفير المتماثل تستخدم نفس المفتاح للتشفير وفك التشفير. كما يعتمد مستوي أمان هذا النوع من التشفير على طول المفتاح، فهو يزداد بزيادة طول المفتاح.

أنواع خوارزميات التشفير التماثلي:

- **التشفير القياسي للبيانات (DES) (Data Encryption Standard):**

هذه الخوارزمية تستخدم مفتاح طوله 56 بت، وبالتالي من غير الممكن تحليله من قبل المخترق. عليه فإن مشكلة تحليل المشفر يتم تجنبها عند استخدام هذه الخوارزمية. ولكن ما يعوق هذه الخوارزمية هو هجوم القوة الغاشمة (Brute-force attack).

- **التشفير القياسي المتقدم – ريجنديل (Rijndael - AES) (Rijndael-Advanced encryption standard):**

خوارزمية ريجنديل تتم بإعادة تشفير كتلة تبعاً لحجم الكتلة وطول المفتاح. وفيها يتم استخدام كتل ذات أحجام 128 بت مثلاً كمدخلات، وينتج عنها كتل مشفرة بنفس الحجم أي 128 بت. تدعم كتل ومفاتيح ذات أحجام مختلفة مثل مفاتيح 128، 192 و256 بت. يكون عدد البتات وتعقيد النص المشفر حسب حجم مفتاح التشفير المستخدم، والنص المشفر الناتج وسط عملية الإعادة يسمى حالة (State)، وهي عبارة عن مصفوفة مربعة من أربع صفوف وعدد أعمدة يساوي طول الكتلة مقسوماً على 32. بالمثل فإن مفتاح التشفير له نفس شكل المصفوفة المربعة المكونة أيضاً من أربع صفوف وعدد أعمدة مساوٍ لطول المفتاح مقسوماً على 32. كما موضح بالجدول(1)، كما يوضح الشكل (1) هيكلية خوارزمية ريجنديل.

جدول(1) دورات AES حسب طول المفتاح (Kevin, 2015)

AES المستخدم	طول المفتاح	حجم الكتلة	عدد الدورات
AES–128	4	4	10
AES–192	6	4	12
AES–256	8	4	14

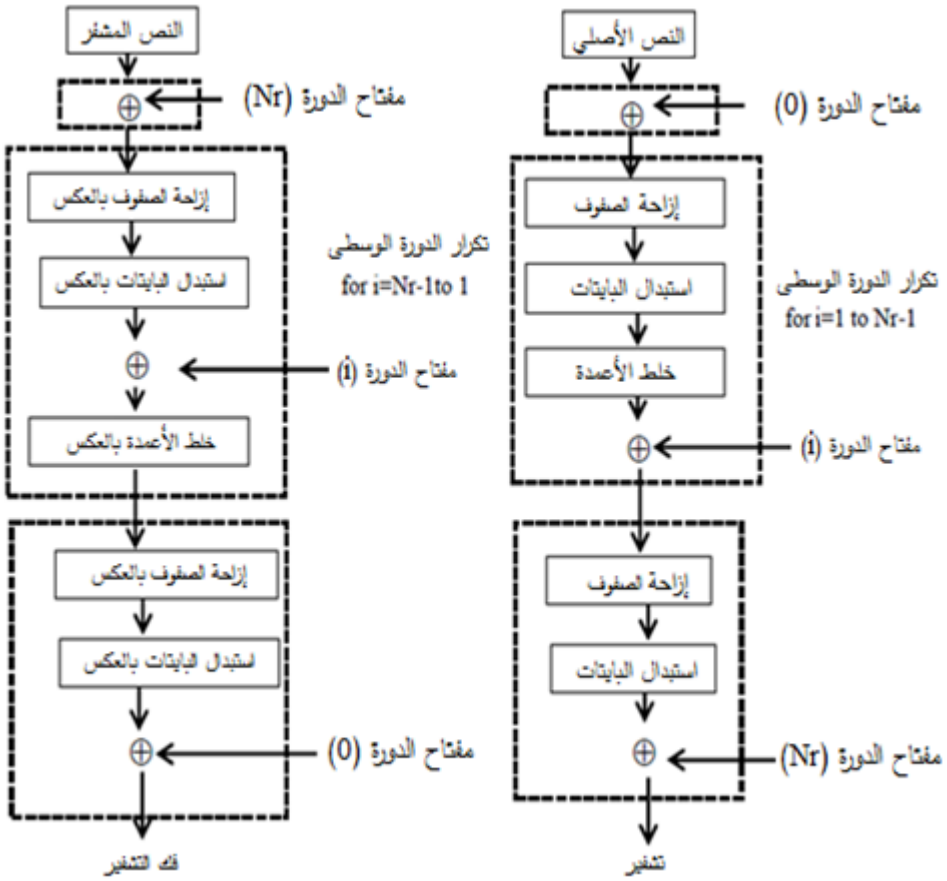
توجد أربع خطوات رئيسية تتم في كل دورة لخوارزمية ريجنديل كما يوضح الشكل (2) وهي:

أ. استبدال بايت (Sub Byte).

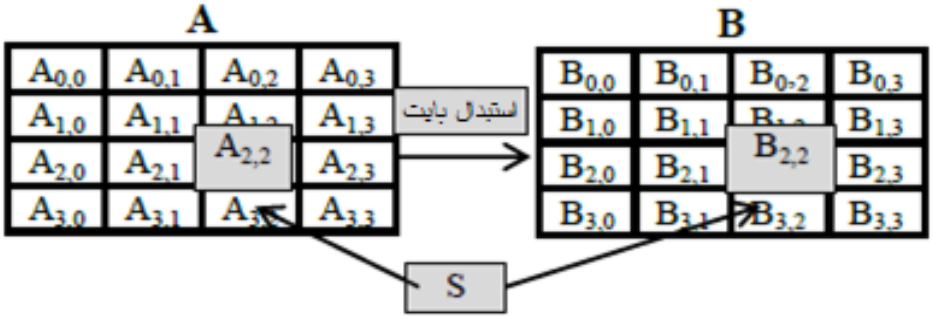
ب. إزاحة سطر (Shift Row).

ج. خلط عمود (Mix Column).

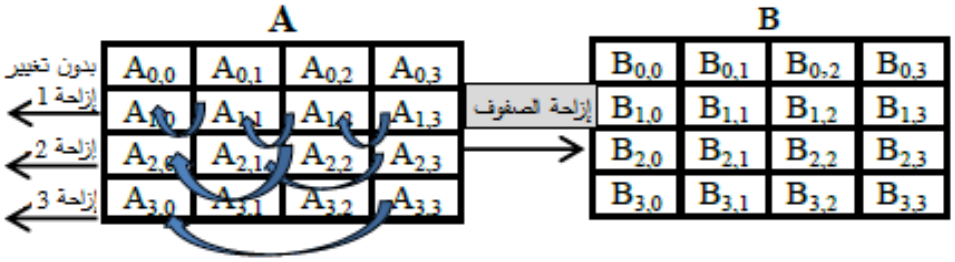
د. إضافة مفتاح الدورة (Add Round Key).



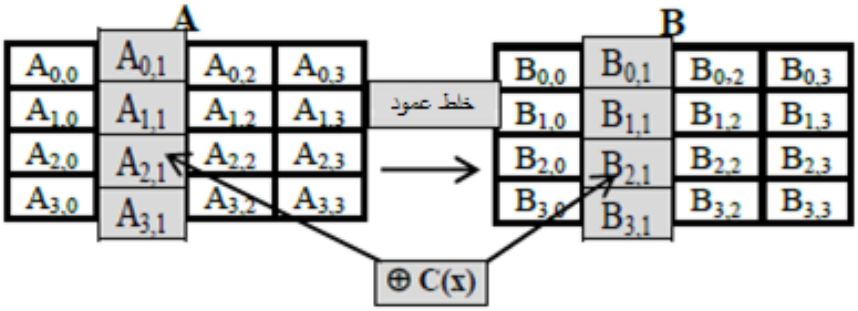
شكل(1) هيكلية خوارزمية ريجنديل (Joye, 2004).



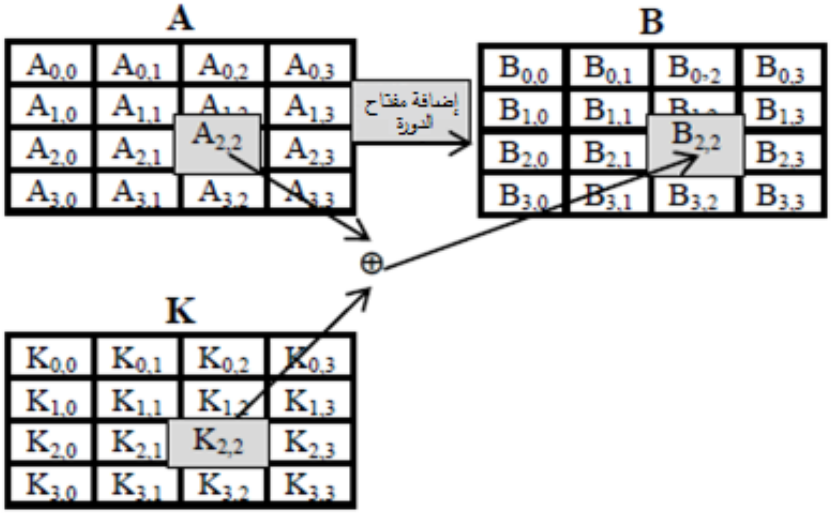
شكل(2–أ) دالة استبدال البايت (Felicisimo, et al., 2015).



شكل (2–ب) دالة ازاحة الصف (Sumathy, et al., 2012).



شكل (2–ج) دالة خلط العمود (Sumathy, et al., 2012).



شكل (2–د) دالة إضافة مفتاح الدورة (Sumathy, et al., 2012).

تحظى خوارزمية ريجنديل بقبول على نطاق واسع بسبب ما تمتاز به من التشفير القوي، والمعالجة المعقدة ومقاومتها لهجوم القوة الغاشمة.

2.1.6 أنماط كتل التشفير (Block Cipher Modes):

وهي تحدد نمط كتلة التشفير ليتم استخدامها في تشفير البيانات. وتوجد العديد من الأنماط لكتل التشفير أهمها وأكثرها استخداماً كتلة التشفير المتسلسلة CBC (Cipher Block Chaining) وهي تعمل كما يلي:

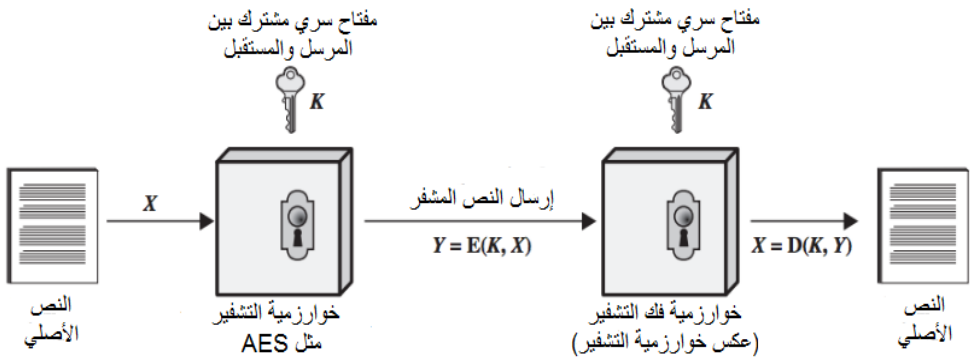
أ. قبل تشفير الكتلة الأولى من النص الأصلي يتم ضمها مع نص عشوائي ابتدائي IV (Initialization Vector) بتنفيذ عملية XOR عليها.

ب. قبل تشفير كل كتلة من النص الأصلي يتم ضمها مع النص المشفر للكتلة السابقة بتنفيذ عملية XOR عليها.

ج. إذا كان النص الأصلي به عدة كتل معروفة أو مكررة فإن كل كتلة سيتم تشفيرها إلي كتلة نص مشفر مختلفة عن مثيلاتها.

3.1.6 خوارزمية فك التشفير (Decryption algorithm):

وهي عكس عملية التشفير. حيث تأخذ كلاً من النص المشفر والمفتاح السري كمدخلات وينتج عنها النص الأصلي كمخرجات. الشكل (3) يوضح النموذج العام لنظام التشفير.



شكل (3) النموذج العام لنظام التشفير.

2.6 الإخفاء أو التغطية(التضمين) Steganography:

الإخفاء أو التغطية(Steganography) كلمة يونانية تعني الكتابة المغطاة (covered writing). وهو عملية إخفاء معلومة ما داخل مصدر معلومات آخر مثل: نص، صورة، ملف صوت أو فيديو، بالتالي تكون غير مرئية وغير ظاهرة للعيان. توجد عدة تقنيات لإخفاء البيانات تعتمد على الوسط الناقل(Carrier).

الإخفاء أو التغطية (Steganography) كلمة يونانية تتألف من مقطعين (Steganos) تعني مغطاة أو سرية، و(Graphy) تعني الكتابة أو الرسم، وهذان المقطعان معاً يعنيان مصطلح الكتابة السرية (Security Writing) أو الكتابة المغطاة (Covered Writing)" (Abdullah, 2009).

يمكن تعريف إخفاء المعلومات بأنها "عملية إخفاء معلومات سرية أو حساسة داخل وسط ناقل آخر بطريقة لا يستطيع أي شخص باستثناء المستخدمين المخولين أن يكتشف وجود رسالة سرية داخله" (Whitman, et al., 2012). وبالتالي هي عملية إخفاء معلومة ما، داخل مصدر معلومات آخر مثل: نص، صورة، ملف صوت أو فيديو، لتكون غير مرئية وغير ظاهرة للعيان. توجد عدة تقنيات لإخفاء البيانات تعتمد على الوسط الناقل(Carrier).

الإخفاء يدعم أنواع مختلفة من الأشكال الرقمية التي تستخدم لإخفاء البيانات مثل ملفات الصور، والصوت، والفيديوء، تعمل كنواقل لإرسال الرسائل الخاصة والمهمة إلى المستلم للقضاء على الثغرات الأمنية. يمكن تنفيذ تقنيات الإخفاء باستخدام أشكال مختلفة من الملفات مثل: ملفات الصوت (mp3.، wmv....الخ)، الفيديو (dat،.mpeg. ...الخ) ، والصور (bmp،.jpeg. ،...الخ).

ومع ذلك، فإن الصور لازالت الملفات الأكثر استخداماً في تقنيات الإخفاء. وتوجد في الوقت الحالي، العديد من الخوارزميات التي تساعد في تنفيذ تطبيقات الإخفاء عليها.

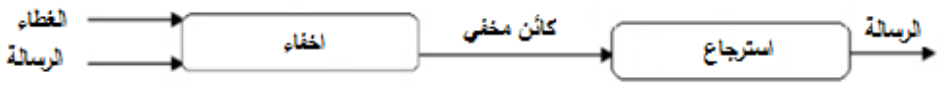
يستخدم كلاً من التشفير والإخفاء معاً لغرض إرسال البيانات بشكل آمن. الطريقة المتبعة في الإخفاء هي نفسها الموجودة في التشفير من حيث المراحل، التشفير وفك التشفير والمفتاح السري. الاختلاف هو أنه في الإخفاء يتم الاحتفاظ بالرسالة بشكل آمن دون أي تغييرات فيها، ولكن في التشفير المحتوي الأصلي للرسالة يختلف باختلاف المراحل مثل التشفير وفك التشفير.

1.2.6 أنواع الإخفاء:

توجد أنواع مختلفة من تقنيات الإخفاء وهي (Abdullah, 2009):

ا– الإخفاء المجرد (Pure Steganography):

هو عملية تضمين البيانات في الكائن بدون أية مفاتيح خاصة، ويعتمد هذا النوع من الإخفاء بشكل كبير على السرية، كما هو موضح بالشكل (4).

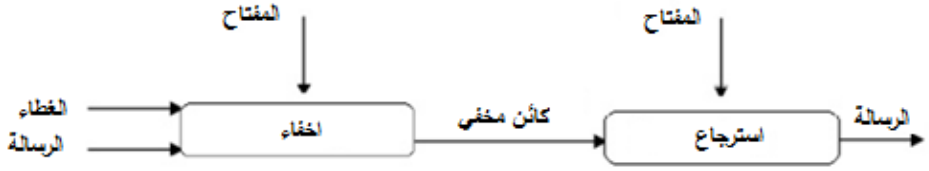


شكل (4) الإخفاء المجرد

هذ النوع من الإخفاء لا يوفر أمناً كافياً بسبب سهولة استرجاع الرسالة إذا تعرف الشخص الغير مخول على طريقة التضمين. ولكن إحدى مزاياه أنه يقلل من صعوبة مشاركة المفتاح.

ب– إخفاء المفتاح السري (Secret Key Steganography):

هو نوع آخر من أنواع الإخفاء التي تستخدم نفس الإجراء عدا استخدام المفاتيح السرية. يستخدم هذا النوع مفتاح فردي (مستقل) لإخفاء البيانات داخل الكائن والذي يشبه المفتاح المتماثل. ويستخدم الاسترجاع نفس المفتاح المستخدم في الإخفاء، كما هو مبين بالشكل (5).

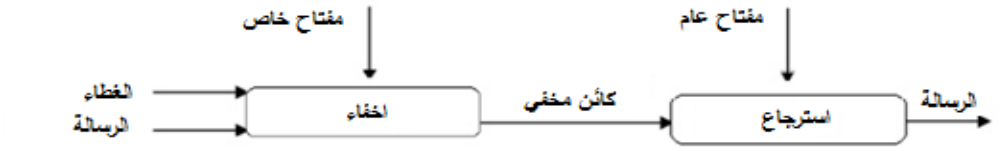


شكل (5) إخفاء المفتاح السري.

هذا النوع من الإخفاء يعتبر أكثر أماناً مقارنة بالإخفاء المجرد، أما مشكلته الرئيسة فتكمن في مشاركة المفتاح السري، فإذا تعرف المخترق على المفتاح سيكون من السهل عليه الاسترجاع والوصول للمعلومات الأصلية.

ج– إخفاء المفتاح العام (Public Key Steganography):

يستخدم نوعين من المفاتيح. الأول مفتاح خاص للإخفاء والآخر مفتاح عام للاسترجاع ويخزن في قاعدة بيانات عامة، كما هو مبين بالشكل (6).



شكل (6) إخفاء المفتاح العام

2.2.6 خوارزميات الإخفاء:

يوجد العديد من الخوارزميات المستخدمة في إخفاء البيانات منها (Andrews, et al., 2013):

أ. خوارزمية الإخفاء JSteg (JSteg Algorithm).

ب. خوارزمية F5.

ج. خوارزمية البت الأُقل أهمية (LSB) (Least Significant Bit Algorithm).

د. خوارزمية الإخفاء والبحث: الأسلوب العشوائي Hide & Seek: The Randomised Approach.

هـ. خوارزمية OutGuess 0.1.

و. خوارزمية F3.

سيتم في هذا البحث استعراض الخوارزميات الثلاث الأولى.

أ– خوارزمية الإخفاء J (JSteg Algorithm):

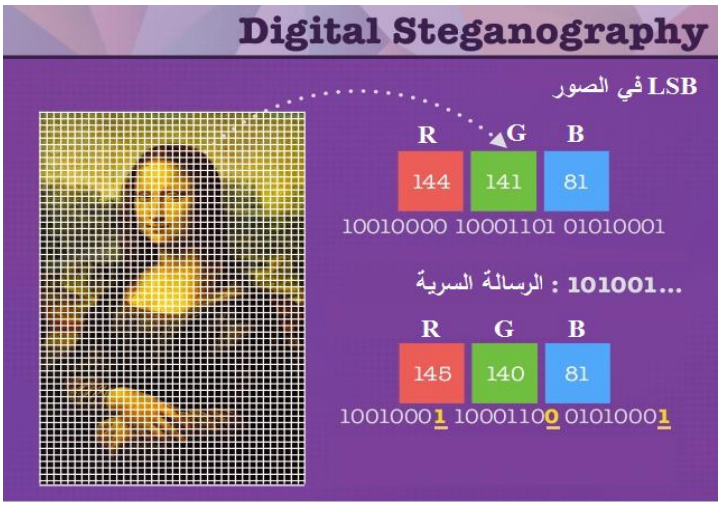
تستخدم خوارزمية JSteg لتضمين الرسائل في صور JPEG ذات الضغط الخفيف loosy، حيث أنها لها سعة تضمين عالية تصل 12%. وهي خوارزمية مقاومة للهجمات البصرية ولكنها أقل مناعة للهجمات الإحصائية. وهذه الخوارزمية تضمن فقط داخل صور JPEG حيث أن محتوي هذه الصور محور في صورة معاملات التردد ذلك لإنجاز التخزين في شكل مضغوط جداً.

ب– خوارزمية F5 (F5 Algorithm):

ابتكرها باحثان ألمانيان هماPfitzmann وWestfeld لتجنب مشكلة الأمن عند تضمين البيانات في صور JPEG، حيث يتم فيها تضمين الرسالة في معاملات (DCT) (Discrete Courier Transform) المختارة عشوائياً. وتستخدم مصفوفة للتضمين تقلل من التغييرات التي تطرأ على طول الرسالة. توفر هذه الخوارزمية سعة إخفاء عالية، وتمنع الهجمات البصرية ومقاومة للهجمات الإحصائية، حيث أنها لا تستبدل البتات.، ولها سعة تضمين أعلى من 13%، وتدعم صيغ صور JPEG،BMP،TIFF وGIF.

ج– خوارزمية البت الأُقل أهمية (LSB) (Least Significant Bit Algorithm):

استبدال البت الأقل أهمية (LSB) هي عملية تعديل البت الأقل أهمية لنقاط الصورة الناقلة (Pixels)، وهي طريقة مبسطة لتضمين الرسالة داخل الصورة. طول الرسالة المدخلة في LSB يختلف تبعاً لعدد بتات الصورة، فمثلاً الصورة ذات 8 بت، يتم تغيير البت الثامن لكل بكسل بالصورة ببت من الرسالة السرية. أما لو كانت الصورة ذات 24 بت، فإنه يتم تغيير ألوان كل نقطة RGB (أحمر، أخضر، أزرق) حيث أنه يتم تغيير البت الثامن لكل لون ببت من الرسالة السرية، كما هو مبين بالشكل (7). LSB فعال عند استخدام صور BMP حيث أن ضغط صور BMP أقل فقداً. ولكن خوارزمية LSB تحتاج لصورة ذات حجم كبير ليتم استخدامها كغطاء. يمكن استخدام استبدال LSB على صور GIF كذلك، ولكن المشكلة هي أن في صورة GIF كلما يتم تغيير LSB فإن اللون بكامله يتغير، ويمكن تجنب هذه المشكلة فقط باستخدام صور GIF ذات التدرج الرمادي والذي يحتوي على 256 ظلاً والتغييرات ستتم تدريجياً بالتالي سيكون من الصعب اكتشافها. أما عن صور JPEG، فإنه لا يمكن استخدامها مع تقنيات الإخفاء ذات الاستبدال المباشر، لأنها سوف تستخدم الضغط مع الفقد في البيانات.



شكل(7) توضيح LSB في الصور الملونة.

فعالية وأداء الخوارزميات السابقة يختلف بحسب نوع الصورة الغلاف أو المصدر الذي تضمن به البيانات. الجدول (2) يعرض مقارنة بين تلك الخوارزميات:

جدول (2) مقارنة بين الخوارزميات

خوارزمية الإخفاء	السرعة	جودة الإخفاء	الأمن
LSB	**عالية**	**جيدة**	**أقل**
F5	**عالية**	**الأعلى وتصل إلى 13.4%**	**عالية وقوية**
JSteg	**معتدلة**	**سعة التضمين تصل إلى 12%**	**أقل**

3.6 العلامة المائية الرقمية (Digital Watermarking):

"هي عملية تُخفي بيانات العلامة المائية في كائن متعدد الوسائط (Multimedia Object) بحيث يمكن ملاحظة العلامة المائية وتمييزها عن بيانات الكائن لتأكيد حقوق ملكيته أو التحقق من تكامله"(Stallings, 2013) . يوجد نوعان من تقنيات العلامة المائية، إحداهما هي العلامة المائية المتينة (robust)، والثانية هي العلامة المائية الهشة (fragile). العلامة المائية المتينة تستخدم بشكل أساسي

لغرض حماية حقوق النشر أو التأليف لقوتها مقابل جميع أنواع المعالجات في الصور. أما النوع الثاني (الهش) فيستخدم لتوفير وثوقية أفضل والتحقق من السلامة لمنع أية تعديلات من قبل الغير مخولين.

7. مراحل تصميم نظام إخفاء النص بالصورة:

يعتمد نظام إخفاء النص بالصورة على ثلاث مراحل أساسية كالتالي:

1.7 مرحلة الإخفاء (Embedding Phase):

تستخدم هذه المرحلة نوعين من الملفات لإجراء عملية الإخفاء، الأول هو البيانات السرية المطلوب إرسالها بشكل سري، والآخر هو الملف الناقل وهو ملف صورة، وفيها يتم تضمين البيانات بعد تشفيرها في الصورة باستخدام خوارزمية البت الأقل أهمية LSB، التي تقـــوم باستبدال البت الأقل أهمية لنقاط ملف الصورة ببتات البيانات المرسلة. أي يتم دمج بتات البيانات المشفرة مع بتات الملف الناقل، وينتج عنها صورة الغطاء. بهذا الإجراء تقوم خوارزمية LSB بالمساعدة في تأمين أصالة الصورة والحفاظ على نقائها.

2.7 مرحلة الإرسال (Transmission Phase):

ويتم فيها إرسال البيانات إلي الهدف بشكل آمن؛ لأنه ينتج عن مرحلة الإخفاء الصورة الغطاء المضمن أو المخفي بها البيانات، وهذه الصورة مؤمنة بمفتاح سري، وعادة ما يتم استخدام البريد الإلكتروني أو الوب لإرسال البيانات، فإذا نجح شخص ما باختراق البريد الإلكتروني أو الوب وحصل على الصورة، فإن المفتاح السري يساعد في منع الكشف عن النص وإجراء التعديلات الغير مصرح بها.

3.7 مرحلة الاسترجاع (Extraction Phase):

وهي عكس مرحلة الإخفاء، ويتم فيها استخدام الصورة الناقلة للبيانات (الصورة الغطاء) كإدخال، وتستخدم نفس كلمة السر المستخدمة في الإخفاء لحماية البيانات من الوصول غير المخول. بعد إعطاء كلمة السر الصحيحة تقوم مرحلة الاسترجاع باستخدام خوارزمية البت الأقل أهمية **LSB** والتي تقوم باسترجاع البتات من الصورة للحصول على البيانات المضمنة بها.

وكما تم مناقشته سابقا بأن التشفير ينقسم إلى نوعين:

أ. التشفير التماثلي (Symmetric Encryption).

ب. التشفير الغير تماثلي (Asymmetric Encryption).

حيث أن نمط التشفير يعتمد على نوع التشفير المستخدم. ففي هذا البحث تم استخدام التشفير التماثلي، وفيه مفتاح وحيد للتشفير وخوارزمية ريجينديل للتشفير والشكل (8) يوضح مراحل النظام المقترح.

8. الإجراء المتبع في إخفاء البيانات في النظام المقترح:

أ. أولاً يقوم المرسل باستخدام تطبيق الإخفاء لإخفاء النص داخل الصورة بعد تشفيره.

ب. للتشفير يكتب النص المراد اخفاؤه ثم يُحمل المرسل الصورة المراد إخفاء النص فيها، ثم كلمة السر في المكان المخصص لهما.

ج. يقوم المرسل بضغط إخفاء ومن هنا تبدأ عملية التشفير استخدام خوارزمية ريجنديل، وتشمل تشفير كلمة السر وإنتاج مفتاح يستخدم لتشفير النص لينتج عنه في النهاية الرسالة المشفرة.

د. يقوم البرنامج بإخفاء الرسالة المشفرة في الصورة باستخدام خوارزمية **LSB** لإنتاج صورة الغطاء، ويمكن تلخيص مراحل عملية الإخفاء في النقاط الآتية:

- قراءة ملف الغطاء وقراءة الملف المراد إخفاؤه.
- تحويل الملف المراد إخفاءه إلى الصيغة الثنائية.
- حساب البت الأقل أهمية في ملف الغطاء وتحديده.
- تبديل البت الأقل أهمية في ملف الغطاء ببت من الملف المراد إخفاءه واحد بواحد.
- تخزين الناتج في ملف جديد بنفس نوع ملف الغطاء (صورة أو صوت أو فيديو).

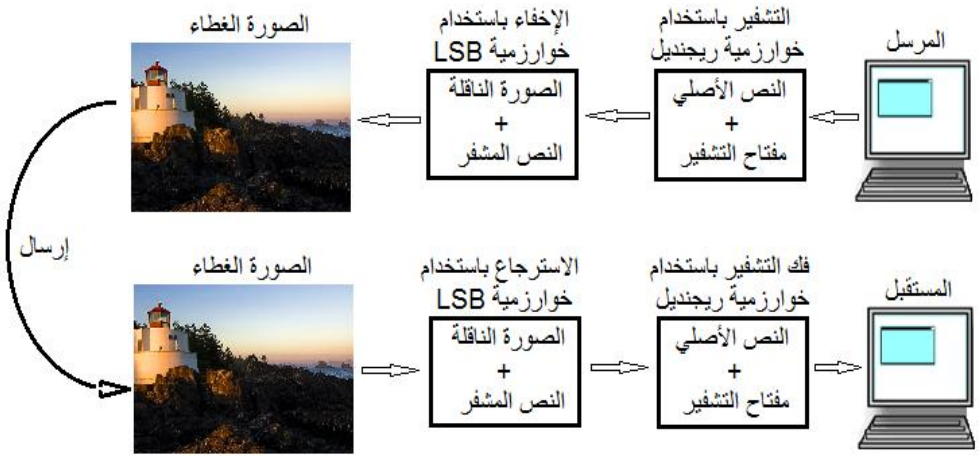
هـ. يقوم البرنامج بتنبيه المرسل بانتهاء عملية الإخفاء ويسمح له بتخزينها في ملف صورة حسب اختياره.

و. ترسل الصورة إلي الهدف أو المستلم خلال وسط إرسال كشبكة الإنترنت أو شبكة محلية باستخدام البريد الالكتروني أو أحد تطبيقات المحادثة المتوفرة على الإنترنت أو وسائط التخزين كالفلاش والقرص الضوئي.

ز. تبدأ مرحلة فك التشفير باستلام الرسالة من قبل الشخص المستلم، ويقوم باستخدام البرنامج بتحميل ملف الصورة المستلمة وإدخال كلمة السر لاسترجاع النص.

ح. يضغط المستلم على استرجاع ليقوم البرنامج ببدء عملية استرجاع الرسالة وفك تشفيرها وعرضها للمستلم، ويمكن تلخيص عملية الاسترجاع في النقاط الآتية:

- قراءة ملف الغطاء.
- حساب البت الأقل أهمية في ملف الغطاء وتحديده.
- استرجاع البت الأقل أهمية في ملف الغطاء.
- تحويل مجموعة البت إلى صيغتها الرقمية (في حالة النص مثلا كل 8 بت تحول إلى حرف وهكذا).



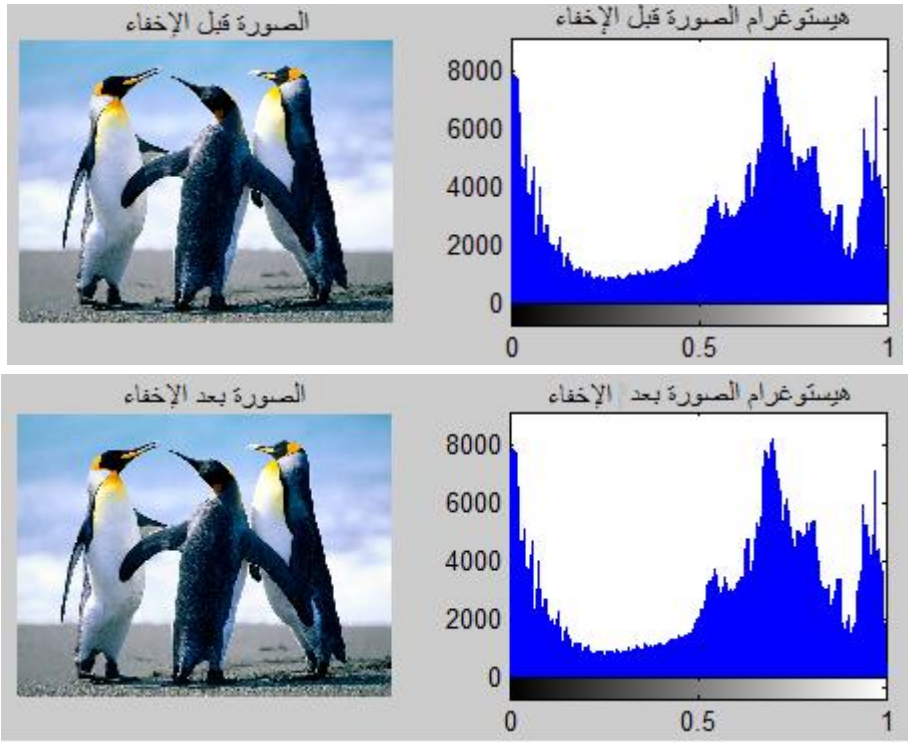
الشكل (8) مراحل النظام المقترح.

الشكل (9) يوضح أنموذجا لعملية إخفاء عبارة "يسم الله الرحمن الرحيم" داخل صورة ملونة.

الشكل (9) مثال لإخفاء رسالة في صورة ملونة.

9. التقويم:

عملية تقويم الأداء التي تمت في هذا البحث قامت على إجراء عدة اختبارات تجريبية للتحقق من عدم ملاحظة البيانات المرسلة والتأكد من أداء النظام المقترح. تم التقويم بالاعتماد على الملاحظة المرئية من خلال مقارنة الصورة الغطاء قبل إخفاء الرسالة السرية فيها بنفس الصورة بعد عملية الإخفاء، ولزيادة التأكد من عدم وجود فوارق ملحوظة بين الصورتين أُستخرج الهيستوغرام (histogram) للصورتين ومقارنتهما. ومن خلال تجربة صور مختلفة ورسائل مختلفة اتضح أنه يتعذر على العين البشرية إدراك وجود اختلاف بين الصور وهيستوغرام الصور قبل وبعد الإخفاء. الشكل (10) يعرض إحدى التجارب التي تمت على النظام المقترح، الصورة تُخفي رسالة مشفرة تتكون من 720 حرفا.



الشكل (10) مثال لإحدى التجارب التي أجريت على النظام المقترح

10. الاستنتاجات:

من المهم حماية البيانات في العالم الرقمي؛ وذلك لزيادة التهديدات الأمنية بسب التوسع الكبير في استخدام وسائل الاتصال الرقمية في تبادل البيانات، ومن خلال هذا البحث والتجارب التي أجريت على النظام المقترح، توصل الباحثان للنتائج الآتية:

أ. يمكن تشفير الرسائل السرية وإخفاؤها داخل صور ملونة لحمايتها من الاختراق واسترجاعها بشكل يضمن سلامتها.

ب. لا يمكن للعين البشرية إدراك وجود رسالة نصية مخفية داخل الصورة المرسلة، لأن النظام يستطيع دمجهما، بحيث لا يوجد خطر من إرسالهما عبر قناة غير آمنة، فدقة عرض الصورة لا تتأثر بالتغييرات عند تضمين الرسالة بها بشكل يمكن ملاحظته بالعين المجردة ، والصورة محمية بكلمة سر مشفرة، بالتالي من الصعب الحصول على المعلومات من قبل الغير مخول لهم.

ج. عدم قدرة العين المجردة على وجود اختلاف في هيستوغرام الصورة قبل وبعد الدمج يزيد من كفاءة ومتانة النظام المقترح.

د. حتى لو تمكن قراصنة البيانات بطريقة ما من معرفة وجود رسالة مخفية داخل الصورة، فإنه يصعب عليهم قراءة الرسالة لأنها مشفرة بكلمة سر.

11. المراجع

المراجع العربية:

1. حسو، شهد. إخفاء النصوص المكبوسة في ملف صوتي، مجلة الرافدين لعلوم الحاسوب والرياضيات، المجلد (10) العدد (1)، (عدد خاص بوقائع المؤتمرالعلمي الخامس في تقانة المعلومات). – 2013.
2. قنديلجي، عامر إبراهيم و آخرون. شبكات المعلومات والاتصالات، عمان : دار المسيرة، 2012.
3. حسين، عبدالأمير خلف. طرق التشفير للمبتدئين ، عمان : دار وائل للنشر والتوزيع، 2010.
4. الحمامي، علاء حسين و العاني، سعد عبدالعزيز. تكنولوجيا أمنية المعلومات وأنظمة الحماية، عمان : دار وائل للنشر والتوزيع، 2007.

المراجع الأجنبية:

1. Abdullah Sadoon Hussein**,** Steganography Methods and some application (The hidden Secret data in Image) , Mosul : University of Mosul, 2009.

2. Andrews Chinchu Elza and Joseph Iwin Thanakumar, An analysis of various stegnographic algoritms, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE). - Volume 2, Issue 2, February 2013.

3. Felicisimo V. W., Bobby D. G. and Bartolome T. T. Modified AES Algorithm using Multiple S-Boxes". Proceedings of the Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA) , Manila, Philippine, 2015.

4. Fouad Mohamed M, Enhancing the Imperceptibility of Image Steganography for Information, The Federated Conference on Computer Science and Information Systems, 2017. - pp. pp. 545–548.

5. Jeffrey A Bloom, Digital watermarking and steganography, Morgan Kaufmann publications, 2008.

6. Joye M., Cryptographic Hardware and Embedded Systems-CHES, New York, 2004.

7. Kevin L., Advanced Encryption Standard (AES) Selection Process- How Rijndael Won, MIDN 1, 2015.

8. Kobayashi L, Furuie S and Barreto P, Providing Integrity and Authenticity in DICOM Images: A novel Approach, IEEE Transactions on Information Technology in Biomedicine. - 2009. - pp. pp. 582-589.

9. Koduri Nani, Information Security Through Image Steganography Using Least Significant Bit Algorithm, London : University of East London, 2011.

10. Stallings W., Cryptography and Network Security:Principles and Practice : Prentice Hall, 2013.

11. Sumathy V. and Navaneethan C., Enhanced AES Algorithm for Strong Encryption, International Journal of Advances in Engineering & Technology (IJAET). - 2012.

12. Whitman M E and Mattord H J, Principles of information security, Thomson, 2012.

13. Zinaly Elham and Naghipour Avaz, Audio Steganography to Protect the Confidential Information: A Survey, International Journal of Computer Applications. - July 2017. - pp. 22-29.