

مقارنة لعملية إخفاء البيانات داخل الصورة الرقمية الملونة باستخدام خوارزمية البت الأقل أهمية المطورة استنادا على قنوات الألوان الثلاثة على الترتيب (2:2:4) و(2:3:3)

أ. ام السعد محمد الاميلس¹ عيسى عبد السلام زويد² محمد حسين أبو عزوم³

omu_alam2001@yahoo.com¹

كلية التقنية الصناعية – مصراته^[1-2-3]

استرجاع تلك البيانات بسهولة دون فقدان لأي من مكوناتها، فضلا عن أن عملية الاسترجاع هذه تتم دون الاستعانة بالصورة الأصلية أو الحاجة لإنشاء جدول يبين مواقع الإخفاء.

في هذا العمل تم الاعتماد على بيئة MATLAB في تصميم برنامج لإخفاء واستخلاص البيانات ومن ثم مقارنة النتائج في الحالتين بقياس جودة الصورة من خلال استخدام مقياس نسبة الإشارة إلى الضوضاء (PSNR) ومقياس مربع الخطأ (MSE) وكذلك مقياس معدل الخطأ في البتات (BER)، كما تم إظهار هيستوجرام الصورة والذي يبين الفرق في توزيع ألوان الصورة الأصلية والصورة الناتجة.

الكلمات المفتاحية: إخفاء البيانات Steganography، الصورة الغطاء Cover Image، الرسالة السرية Secret Message، تقنية البت الأقل أهمية المحسنة Improved LSB، نسبة الإشارة إلى الضوضاء PSNR، مقياس مربع الخطأ MSE، مقياس معدل الخطأ في البتات BER.

Abstract: The study aimed to define the concept of data hiding (steganography), which refers to hiding confidential information in other sources such as text, video, audio, image, etc.

In image steganography, the "cover image" is used as a carrier where the "secret message" is hidden, and the resulting image after concealment is known as the "Stego Image".

The work was based on the Enhanced Least Significant Bit technology (Improved LSB) by including information within the RGB color image in a way that does not affect the quality of the image after masking while

الملخص: هدفت الدراسة الي التعريف بمفهوم إخفاء البيانات (Steganography) وهو علم إخفاء المعلومات السرية في أحد المصادر الأخرى مثل نص، فيديو، صوت، صورة ... إلخ. وفي علم الإخفاء الصوري (Image Steganography) تستخدم الصورة الرقمية كغطاء (Cover Image) حيث يتم فيها إخفاء الرسالة السرية (Secret message)، وتعرف الصورة الناتجة بعد عملية الإخفاء باسم (Stego Image).

اعتمد العمل على تقنية البت الأقل أهمية المحسنة (Improved LSB) وذلك بتضمين معلومات داخل الصورة الملونة RGB بطريقة لا تؤثر علي جودة الصورة بعد الإخفاء مع توفير مساحة أكبر لإخفاء البيانات السرية. تتم عملية الإخفاء باستخدام نفس الخوارزمية ولكن بطريقتين الطريقة الاولى على الترتيب (2:2:4) والثانية على الترتيب (2:3:3) حيث تم بالترتيب الأول خزن 2 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأحمر R (البايت الأعلى أهمية)، 2 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأخضر G، وأخيرا 4 بت من البيانات السرية في الجزء الأقل أهمية من حزمة اللون الأزرق B. اما بالترتيب الثاني فتم إخفاء 3 بت في كل من قناة من قنوات اللون الأخضر والأزرق أما قناة اللون الأحمر فتم إخفاء 2 بت.

هذه الخوارزمية تأتي اعتمادا على نظرية الالوان Color Theory التي تنص على أن العين البشرية أكثر تحسنا للونين الأحمر والأخضر مقارنة باللون الأزرق، حيث نجحت هذه الخوارزمية في الحالتين في إخفاء البيانات دون حدوث حالة تشوه للصورة الأصلية، أو إمكانية ملاحظة التغيرات الحاصلة فيها جراء عملية الإخفاء، وتم

فظهرت وسائل حماية متنوعة مثل وضع كلمات سرية، أو استخدام التشفير (Cryptography) وكذلك تقنيات إخفاء أو تغطية البيانات (Steganography) ، وتتلخص عملية التشفير بتحويل الرسائل والبيانات السرية إلى صيغة لا يمكن قراءتها وذلك باستخدام مفتاح سري (Secret Key) ويتم استرجاعها باستخدام ذلك المفتاح [1].

أما إخفاء البيانات فيتم من خلال وضع البيانات داخل ملفات الوسائط بحيث لا يمكن ملاحظتها أو كشفها أو إدراك وجود معلومات منقولة من خلال تلك الملفات وإنما تبدو كملفات عادية، حيث يتم فيها المحافظة على الشكل العام للملف الناقل، ويكون الإخفاء على صنفين، الصنف الأول العلامة المائية (Watermarking)، وفيه يتم إخفاء المعلومات القليلة مثل التوقيع أو علامة الشركة أو ختم المؤسسة وذلك لتوثيق المستندات المرسله بطريقة يصعب التلاعب بها أو محوها من خلال عمليات المعالجة الصورية مثل الترشيح أو التحويلات الهندسية أو إضافة الضوضاء. والصنف الثاني هو إخفاء البيانات (Steganography) حيث يتضمن إخفاء أكبر ما يمكن من المعلومات المهمة (وثيقة، رسالة، صور) داخل ملفات نصوص أو صور أو صوت أو فيديو بطريقة لا تثير الفضول وإنما تبدو كصور إعلان أو نصوص عادية [2].

1.1 مشكلة البحث

تكمن مشكلة البحث الأساسية في أن حماية البيانات عن طريق التشفير قد يجذب انتباه البعض لمهاجمة البيانات المشفرة (Encrypted Data) كما أن شكل الرسالة والبيانات الناتجة بعد عملية التشفير يثير الشك لظهور محتواها بشكل غير مرتب وظهور ألفاظ من غير اللغة المستخدمة مما يلفت انتباه المتطفلين أو قرصنة المعلومات إلى العبث بالرسالة إن لم يتمكنوا من فك الشفرة.

في المقابل توجد طريقة أخرى لإخفاء المعلومات وهي بأن نقوم بتضمينها داخل وسيط ما وتحت غطاء معين بحيث لا تظهر هذه الرسالة لمن يستعرض الوسيط الأساسي

providing more space to hide confidential data.

Masking process is done in two ways by using the same algorithm, the first one is in order (2:2:4) and the second one in order (2:3:3). In the first order, 2 bits of confidential data are stored in the least important part of the red color channel R (the most important byte), 2 bits of confidential data in the least important part of the green color channel G, and finally 4 bits of confidential data in the least important part of the blue color channel B. In the second order, 3 bits are hidden in each of the green and blue channels; either the red color channel is 2 bits hidden.

This order of insertion was chosen depending on the color theory that says red and green are equivalently sensitive to human eye and are more sensitive as compared to blue. The proposed method successfully and easily retrieved data from the carrier image without losing it, as well as completing this retrieval process without restoring the original image or using a hiding table.

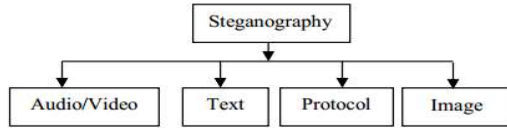
In this work, the MATLAB environment used to design a program for data masking and extraction, and then compare the results of two ways by measuring image quality, signal-to-noise ratio (PSNR) and square error (MSE) as well as a measure of bit error rate (BER). The image histograms also show the difference in the color distribution of the original image and the resulting image.

Keywords: Steganography, Cover Image, Secret message, Improved LSB, PSNR, MSE, BER.

1. المقدمة:

في الاتصالات الرقمية بات من السهل اعتراض المعلومات المرسله عبر شبكات الاتصال المختلفة أو الدخول الي الحاسبات سواء أكانت مرتبطة أو مستقلة عن الشبكة بقصد الاطلاع على محتوياتها أو سرقة معلوماتها أو العبث بها، وفي ضوء ذلك يتوجب تأمين الحماية والموثوقية والمصادقية للمعلومات والمحافظة عليها

بفحصه، يوضح الشكل (1) تصنيفات الإخفاء وفقاً لنوع الناقل [3].



الشكل 1. تصنيفات الإخفاء وفقاً لنوع الناقل

1.2 الإخفاء بالنص Text Steganography

يمكن استخدام المستندات النصية لإخفاء المعلومات عن طريق إضافة مسافات بيضاء في نهاية أسطر المستند. وهذا النوع من الإخفاء فعال لأن الفضاء الأبيض يحدث بشكل طبيعي وغير مرئي للعين البشرية على الإطلاق وذلك في معظم برامج تحرير النصوص، وعند استخدام هذه التقنية فلا توجد طريقة للاشتباه في وجود أي بيانات مخفية [4].

2.2 الإخفاء بالصورة Image Steganography

يعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الاستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء، ويتم تطبيق هذه النوع من الإخفاء باستخدام العديد من الطرق منها الإخفاء باستخدام التحويل الزاوي المتقطع DCT، والإخفاء باستخدام التحويل الموجي DWT، وكذلك الإخفاء باستخدام الإدخال في البت الأقل أهمية LSB وهي أكثر الطرق شيوعاً [4].

3.2 الإخفاء بالصوت Audio Steganography

هناك العديد من التقنيات المستخدمة في إخفاء المعلومات داخل الملف الصوتي؛ التقنية المستخدمة عادة في إخفاء المعلومات داخل الملفات الصوتية هي تشفير بت منخفض يشبه LSB في ملفات الصور، ولكن باستخدام ترميز بت منخفض، وتعد هذه الطريقة محفوفة بالمخاطر لأنه عادة ما تكون ملحوظة للأذن البشرية. هناك طريقة أخرى تستخدم لإخفاء المعلومات داخل ملف صوتي وهي (Spread Spectrum)، وتعمل بإضافة ضوضاء عشوائية للإشارة، وتنتشر المعلومات عبر طيف التردد للملف الصوتي. طريقة أخرى لإخفاء المعلومات داخل ملف صوتي هي إخفاء بيانات (Echo) وتعمل هذه

سواءً كان (صورة أو صوت أو فيديو) لأنها مخفية تماماً داخله.

2.1 منهجية البحث

لكي تتم عملية الإخفاء يتم أولاً تحويل البيانات السرية إلى سلسلة من البتات ومن ثم إخفائها في كل حزم الصورة اللونية بطريقتين الأولى علي الترتيب (2:2:4) وذلك بتوزيعها كالآتي 2 بت في كل من حزم اللون الأحمر R والأخضر G وذلك في الجزء الأقل أهمية من كل حزمة أو قناة لونية، و 4 بت في الجزء الأقل أهمية لقناة اللون الأزرق B، أما الترتيب الثاني وهو (2:3:3) فيتم بإخفاء 2 بت بالجزء الأقل أهمية لحزمة اللون الأحمر، و 3 بت بالجزء الأقل أهمية لكل من حزمة اللون الأخضر والأزرق علي التوالي، وفي هذه الخوارزمية يمكن إخفاء كمية أكبر من البيانات حيث أن التلاعب بقيم البتات الأقل أهمية لا يؤثر على جودة الصورة أو قيمة اللون في كل قناة مما يجعل من الصعب على العين البشرية ملاحظة التغيير في الصورة الناتجة بعد الإخفاء.

3.1 أهداف البحث

الهدف الأساسي في أي عملية إخفاء هو الحفاظ على جودة الغطاء سواء كان صورة أو فيديو أو صوت مع إخفاء أكبر قدر من البيانات السرية. وفي هذا البحث تم إنشاء تطبيق يقوم بإخفاء البيانات واسترجاعها باستخدام خوارزمية البت الأقل أهمية المحسنة Improved LSB والتي من خلالها يتم إخفاء 8 بت في كل بكسل من بكسلات الصورة بدلاً من إخفاء 3 بتات كما في خوارزمية LSB الأساسية.

2. تصنيفات الإخفاء وفقاً لنوع الناقل

الناقل هو ملف البيانات الذي يتم فيه إخفاء البيانات السرية وذلك من خلال إجراء التعديلات عليه مثل ملفات الصور والمستندات وملفات الفيديو والملفات الصوتية والبروتوكول ويجب على الناقل أن يعمل بنفس طريقة الناقل الأصلي غير المعدل، وأن يظهر بشكل طبيعي لأي شخص يقوم

حيث:

I_{max} : هي القيمة القصوى للإشارة الموجودة في الصورة الأصلية.

MSE: هو متوسط الخطأ التربيعي بين الصورة الأصلية أو صورة الغطاء cover image وبين الصورة الناتجة بعد عملية الإخفاء Stego image [9].

2.3 مقياس مربع الخطأ MSE

كما ذكر سابقا فإن حساب قيمة نسبة الإشارة إلى الضوضاء (PSNR) يتطلب قياس مربع الخطأ (MSE) ويكون للصورة الرمادية حسب المعادلة التالية:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (CI(i, j) - SI(i, j))^2 \quad (2)$$

حيث:

M, N عدد الصفوف والأعمدة للصورة الغطاء والصورة الناتجة.

CI (i, j): هي قيمة البيكسل في الصورة الغطاء cover image (قبل الإخفاء) عند النقطة (i, j).

SI (i, j): هي قيمة البيكسل في الصورة الناتجة Stego image عند النقطة (i, j).

أما بالنسبة للصور الملونة، يتم حساب (MSE) بطريقتين الأولى بتحويل الصورة الملونة الى رمادية عبر استدعاء الدالة (rgb2gray) ومن ثم استخدام القانون السابق، أو بحساب (MSE) على كل قيم البيكسل لكل قناة لونية على حدة ويتم حساب متوسطها بعدد قنوات الصورة الملونة والتي تحتوي على ثلاث قيم RGB لكل بكسل حسب المعادلة التالية:

$$MSE = \frac{1}{C \cdot M \cdot N} \sum (i_1 - i_2)^2 \quad (3)$$

حيث:

i_1, i_2 : قيمة البيكسل للصورتين الغطاء Cover Image والناتجة Stego Image
C : عدد قنوات الالوان [6].

الطريقة على إخفاء المعلومات ببساطة عن طريق إضافة صوت إضافي إلى صدى داخل الملف الصوتي [5].

4.2 الإخفاء بالفيديو Video Steganography

عادة يتم إخفاء المعلومات داخل الفيديو باستخدام طريقة DCT، التي تعمل من خلال إجراء تغيير على كل صورة من صور الفيديو وذلك بتغيير القيم بأجزاء معينة من الصورة، لذلك لا تلاحظها العين البشرية، وإخفاء المعلومات في مقاطع الفيديو مشابهة لتلك الموجودة في الصور، بحيث يكون جزء من المعلومات مخفيا في كل إطار من الفيديو [6].

5.2 الإخفاء بالبروتوكول Protocol

Steganography

يشير مصطلح " الإخفاء في البروتوكول " إلى تقنية تضمين المعلومات داخل الرسائل وبروتوكولات التحكم في الشبكة المستخدمة [7].

3. مقاييس الأداء

يعتبر استخدام مقاييس أو معايير الأداء في تطبيقات تحسين الصور الرقمية له أهمية كبيرة في معرفة كفاءة التحسين الحاصلة لها، من ضمن هذه المقاييس مقياس نسبة الإشارة إلى الضوضاء Peak Signal-to-Mean Noise Ratio (PSNR)، مقياس مربع الخطأ Mean Square Error (MSE)، مقياس معدل الخطأ في البتات Bit Error Rate (BER) وكذلك مقارنة هيستوجرام الصورة الأصلية والناتجة (Histogram) بعد عملية الإخفاء [8].

1.3 مقياس نسبة الإشارة إلى الضوضاء PSNR

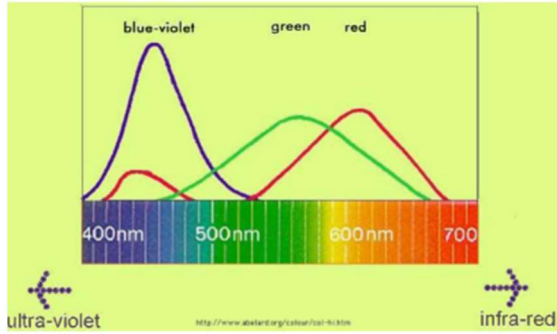
يتم تطبيق هذا المصطلح على الصور كمقياس للجودة، وهو يشير الي نسبة الإشارة إلى الضوضاء حيث يعبر عن النسبة بين القيمة القصوى الممكنة للإشارة وقوة الضوضاء المشوهة التي تؤثر على جودة تمثيلها ويتم التعبير عن (PSNR) عادةً من حيث مقياس ديسيبل لوغاريتمي (dB) كما في المعادلة:

$$PSNR = 10 \log_{10} \left(\frac{I_{max}^2}{MSE} \right) dB \quad (1)$$

أفضل تأثير لإخفاء المعلومات هو عندما يكون حجم الصورة كبير، ويكون عدد البتات المطلوب إخفاؤها أقل، وكما أن إخفاء المعلومات في كل صفوف الصورة أفضل من إخفاءها في صف واحد من الصورة، حيث أن تأثير إخفاء المعلومات في النطاقات الملونة غير متساوٍ.

4. نظرية الألوان Color theory

تفسر هذه النظرية كيفية إدراك العين البشرية للألوان، وكيفية دمجها سواء كانت متشابهة أو مختلفة. يشير مصطلح رؤية اللون (Color vision) الي قدرة العين علي تمييز الأجسام اعتمادا على أطوال موجات الضوء (wavelengths) المنعكس عليها، ويميز الجهاز العصبي اللون بمقارنة استجابات الأنواع المختلفة من الخلايا المخروطية في العين للضوء حيث تكون هذه الخلايا حساسة لأجزاء مختلفة من الطيف المرئي، يوضح الشكل (2) أن هناك درجة من التداخل بين استجابات الخلايا المخروطية، حيث يتراوح الطيف المرئي للبشر تقريبا من 380 إلى 740 نانومتر، في هذا النطاق يكون اللونان الأحمر والأخضر أكثر حساسية للعين البشرية مقارنة بالأزرق [12].



الشكل.2 التداخل في الاطوال الموجية للألوان

تعتبر مجموعة الألوان الأساسية بأنها مجموعة الألوان التي يمكن دمجها للحصول على تشكيلة واسعة من الألوان الأخرى. لكن أشهرها هو RGB، الذي يعتمد على الألوان الأحمر والأخضر والأزرق، والتي تدمج للحصول على بقية الألوان المختلفة بتدرجاتها جميعاً، وهو النموذج اللوني المستخدم بكثرة في شاشات التلفاز والحواسيب وآلات التصوير وغيرها [11].

3.3 مقياس معدل الخطأ في البتات BER

معدل الخطأ في البتات هو عدد أخطاء البتات لكل وحدة زمنية. وتقاس نسبة الخطأ البتات بعدد أخطاء مقسوماً على العدد الإجمالي للبتات المنقولة خلال فترة زمنية معينة، وهي مقياس بدون وحدة.

في الإرسال الرقمي يكون عدد أخطاء البتات هو عدد البتات المستقبلية لتدفق البيانات عبر قناة اتصال تم تغييرها بسبب الضوضاء أو التداخل أو التشوه أو أخطاء التزامن في البتات، يتم حساب معدل الخطأ حسب المعادلة التالية:

$$BER = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_b}{N_0}} \right) \quad (4)$$

حيث :

E_b : عدد البتات الخاطئة

N_0 : عدد البتات الكلي

كمثال، افترض تسلسل البتات المنقولة كالتالي:

1 1 0 1 0 0 0 1 1 0

وتسلسل البتات التي تم استقبالها كالتالي:

1 0 0 1 0 1 0 1 0 0

في هذه الحالة يكون عدد أخطاء البتات هو 3 بتات غير صحيحة مقسومة على 10 بتات تم نقلها، مما يؤدي إلى معدل BER يبلغ 0.3 أو 30% [10].

4.3 مقياس الهستوجرام Image Histogram

الهستوجرام لأي صورة ملونة هو شكل بياني يوضح نسبة وجود الألوان فيها، بحيث يكون المحور الأفقي مبينا نسبة هذه الألوان بشكل متدرج بينما المحور العمودي هو القيمة الإجمالية لظهور ذلك اللون في الصورة، وبالنسبة لصور اللون الرمادي فيكون الهستوجرام هو تمثيل بياني لمستويات الرمادي المختلفة في الصورة. وعلى هذا فلكل لون (أو قيمة رمادية) قيمة عددية تمثل في الشكل البياني وهي قيمة حدوثه في الصورة، وبمعالجة نسب الالوان والتدرجات يمكن عمل تأثيرات كثيرة على الصورة [11].

من المقاييس الأخرى التي كان لها دور في تحسين جودة الصورة طول النص وكذلك حجم صورة الغطاء حيث أن

الاختلاف في الألوان فيها. من مساوى هذه الدراسة أنها تعاني من فقدان البيانات عند الاسترجاع ولكنها تمتاز بجودة عالية بالإضافة الى إخفاء كمية كبيرة من البيانات [14].

في العام 2010م قدمت دراسة (p. Halanka & Athawale) والتي اقترحت تحسين طريقة الخانة الثنائية الأقل أهمية لزيادة سعة التضمين والدقة، وهذه الطريقة يمكن تطبيقها على الصورة ذات الحجم 24 خانة ثنائية، وتم استخدام مفتاح سري طوله 8بت، وقبل أن تتم عملية التضمين تجري عملية (XOR) للمفتاح السري والخانات الثنائية في الرسالة وكل نقطة في الصورة وهذه الطريقة لها مميزات منها زيادة السعة لتضمين المعلومات مع جودة وأداء أفضل [14].

6. خوارزمية البت الأقل أهمية المحسنة على

الترتيب (2:2:4) والترتيب (2:3:3) لكل قناة

لونية RGB

في هذه الورقة تم العمل على خوارزمية البت الأقل أهمية المحسنة لإخفاء نص داخل صورة رقمية ملونة على الترتيب (2:2:4) مرة، والترتيب (2:3:3) مرة أخرى وذلك لكل قناة لونية RGB حيث يمكن في الحالة الاولى أن تستبدل البت الثنائية الأقل أهمية الأولى والثانية في قناتي اللونين الأحمر والأخضر وكذلك البتات الثنائية في الاربعة من الجزء الأقل أهمية في قناة اللون الأزرق، أما الترتيب (2:3:3) فيتم فيه إخفاء 2 بت في قناة اللون الأحمر و3 بتات في كل قناة من قنوات اللون الأخضر والأزرق على الترتيب مع بقاء العين البشرية غير قادرة على تمييز الفرق بين الصورتين فيما يلي مثال لطريقة الإخفاء على الترتيب (2:2:4) كما بالشكل (3) و الترتيب (2:3:3) كما بالشكل (4).

وبما أن نظرية الألوان تنص على أن العين البشرية أقل تحسناً للون الأزرق من اللونين الآخرين وهما الأحمر والأخضر، فقد تم في هذا البحث اختيار طريقة إخفاء البيانات في الصورة الملونة بناء على هذا الأساس.

5. الدراسات السابقة لخوارزمية البت الأقل

أهمية LSB (Least Significant Bit)

أجريت العديد من الدراسات والأبحاث التي كانت تحاول تطوير وتحسين تقنية LSB تحت اسم Improved LSB ومن هذه الدراسات، الدراسة التي قدمها (A. A. AWAD) حول إخفاء المعلومات متعدد المستويات في العام 2003 ف، حيث يتم في المستوى الأول وضع الرسالة النصية في صورة من الأبيض والأسود، والمستوى الثاني يأخذ من خرج المستوى الأول كمدخل الى صورة RGB. وكانت نتيجة هذه الدراسة أن الإخفاء متعدد المستويات له فوائد محتملة، حيث أنه يؤدي الي تعزيز سرية المعلومات باستخدام مستويين من الإخفاء ولكن مع اضافة المزيد من التعقيد في عملية إخفاء المعلومات من خلال تطبيقه في مستويين [13].

في العام 2008م قدمت دراسة من قبل B.B. (G.S. ISouvik) & (Indradip) حيث ادرجت فكرة المفتاح السري للمصادقة عند كلا الطرفين وذلك باستخدام الترميز عند كلا الطرفين من أجل تحقيق مستوى عال من الأمن، وبالتالي يتم تنفيذ العملية العكسية لاسترجاع المعلومات الأصلية. وقد اضاف هذا النموذج مستوي عال من السرية، حيث أن الغطاء لا يدعو للشك بوجود رسالة ما داخله لأنها تبدو مشابهة الي الكائن الأصلي سواء كان الكائن صورة أو صوت أو فيديو [14].

أما في العام 2009م فقد قدمت دراسة من قبل (R.R. Koppola) وكان الهدف منها هو اقتراح تقنية جديدة مبنية على طريقة LSB لإخفاء كمية كبيرة من البيانات، وهذه التقنية تسمح بإخفاء صورة داخل صورة أخرى لها نفس الحجم وذلك بتقليل حجم الرسالة السرية قبل الإخفاء لإخفاء كمية أكبر من البيانات، ويتم إخفاء البيانات في مناطق من الصورة والتي لا تستطيع العين إدراك

قبل عملية الإخفاء

قناة اللون الأزرق	قناة اللون الأخضر	قناة اللون الأحمر
11100101	11011010	10101101
قيمة البايت في كل قناة Initial Pixel Bytes		
11011101		
البيانات المراد إخفاؤها Data to be Embedded		

بعد عملية الإخفاء Channels in which Data is Embedded

قناة اللون الأحمر Red Channel	قناة اللون الأخضر Green Channel	قناة اللون الأزرق Blue Channel
11010111	11011010	11101101
إخفاء 2 بت في قناة اللون الأحمر		
إخفاء 2 بت في قناة اللون الأخضر		
إخفاء 4 بت (في قناة اللون الأزرق)		

الشكل 3. طريقة LSB المحسنة على الترتيب (2:2:4)

قبل عملية الإخفاء

قناة اللون الأزرق	قناة اللون الأخضر	قناة اللون الأحمر
11100101	11011010	10101101
قيمة البايت في كل قناة Initial Pixel Bytes		
11011101		
البيانات المراد إخفاؤها Data to be Embedded		

بعد عملية الإخفاء Channels in which Data is Embedded

قناة اللون الأحمر Red Channel	قناة اللون الأخضر Green Channel	قناة اللون الأزرق Blue Channel
11010111	11011011	11101101
إخفاء 2 بت في قناة اللون الأحمر		
إخفاء 3 بت في قناة اللون الأخضر		
إخفاء 3 بت في قناة اللون الأزرق		

الشكل 4. طريقة LSB المحسنة على الترتيب (2:3:3)

1.6 خطوات عملية الإخفاء في خوارزمية البت الأقل أهمية المحسنة على الترتيب (2:2:4)

1. قراءة الصورة الرقمية الملونة cover image وتحديد أبعادها M, N وهل هي مناسبة بالحجم لإخفاء الرسالة السرية .
2. تحويل كل بكسل من الصورة الغطاء Cover Image إلي ASCII Code ومن ثم إلى الصيغة الثنائية binary.
3. إدخال النص المراد إخفاءه ومن ثم تحويل كل حرف الي ASCII CODE ومنه إلي الصيغة الثنائية binary.
4. يتم تخزين بتات النص في مصفوفة احادية (كأجزاء مكونة من 8 بت).
5. وضع قيمة عداد المقاطع $I = 1$ والخاص بحساب عدد مقاطع بتات النص المراد إخفاءه.

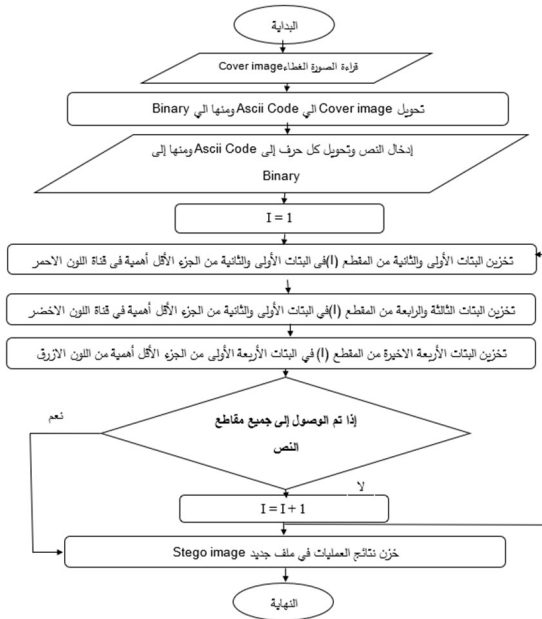
6. تخزين البتات الأولى والثانية من المقطع I في البتات الأولى والثانية من الجزء الأقل أهمية في قناة اللون الأحمر.

7. تخزين البتات الثالثة والرابعة من المقطع I في البتات الأولى والثانية من الجزء الأقل أهمية في قناة اللون الأخضر.

8. تخزين البتات الأربعة الأخيرة من المقطع I في البتات الأربعة الأولى من الجزء الأقل أهمية في قناة اللون الأزرق.

9. إذا تم الوصول الي جميع المقاطع اذهب الي الخطوة (10) وإلا قم بزيادة العداد $I = I + 1$ واذهب الي الخطوة (6).

10. خزن ناتج العمليات السابقة في ملف جديد بنفس نوع ملف الغطاء وهو ملف Stego image. يوضح الشكل (5) المخطط الانسيابي لخطوات عملية الإخفاء.



الشكل 5. المخطط الانسيابي لخطوات عملية الإخفاء

2.6 خطوات عملية الاسترجاع في خوارزمية البت

الأقل أهمية المحسنة على الترتيب (2:2:4)

1. قراءة ملف الصورة الناتجة Stego image الذي يحتوي على البيانات المخفية بداخله.

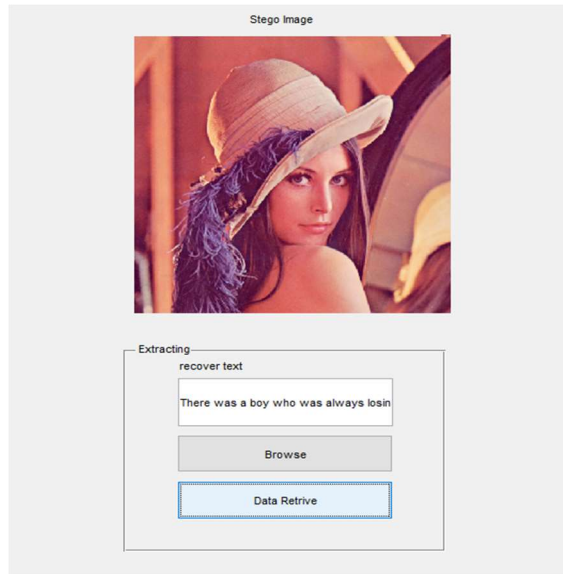
في الترتيب الثاني تم اتباع نفس الخطوات عندما كان ترتيب الاخفاء على الطريقة (2:2:4) ولكن مع اختلاف الترتيب ليكون على النحو التالي (2:3:3).

7. تصميم وتنفيذ البرنامج

تم في هذه المرحلة تصميم الواجهة الرئيسية للبرنامج، حيث تحتوي هذه الواجهة على خيارات يتم فيها إظهار الصور الاصلية cover image والصور التي تم إخفاء النص داخلها Stego image، كما تحتوي على خيارات ترتيب إخفاء النص أو إظهار النص المخفي، كذلك تحتوي الشاشة على مجموعة من المقاييس التي يتم حسابها بالبرنامج بالإضافة الي زر يقوم بإظهار هيستوجرام الصورة قبل وبعد الإخفاء، كما هو موضح بالشكل (7). كما يظهر الشكل (8) خيار إخفاء النص داخل الصورة.



الشكل 7. الواجهة الرئيسية للبرنامج

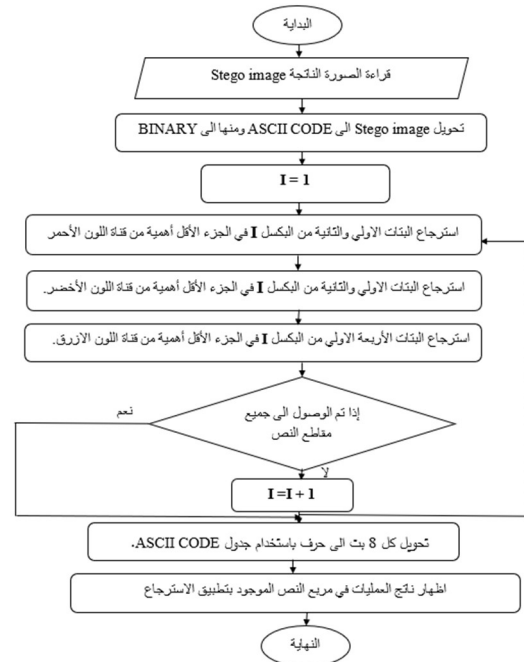


الشكل 8. واجهة إخفاء نص داخل صورة

2. تحويل كل بكسل من الصورة الي ASCII Code ومن ثم إلى الصيغة الثنائية binary.
3. وضع قيمة عداد المقاطع = 1 للخاص بحساب عدد مقاطع بتات النص المراد استرجاعه
4. استرجاع البتات الأولى والثانية من البكسل I في الجزء الأقل أهمية من قناة اللون الأحمر.
5. استرجاع البتات الأولى والثانية من البكسل I في الجزء الأقل أهمية من قناة اللون الأخضر.
6. استرجاع البتات الأربعة الأولى من البكسل I في الجزء الأقل أهمية من قناة اللون الأزرق.
7. إذا تم الوصول الي جميع بتات مقاطع النص المراد استرجاعه اذهب الي الخطوة (8) والاقم بزيادة العداد $I = I + 1$ والذهاب الي الخطوة (4).

8. تحويل كل 8 بت الي حرف باستخدام جدول ASCII CODE.

يوضح الشكل(6) المخطط الانسيابي لخطوات عملية الاسترجاع.



الشكل 6. المخطط الانسيابي لخطوات عملية الاسترجاع

تم في البرنامج استخدام عدد من الصور ذات الامتداد (.JPG) كما موضحة بالشكل (9).



الشكل 9. الصور المستخدمة كغطاء

8. النتائج

تم اختبار الصور بمقاييس جودة الصورة وهي نسبة الإشارة الي الضوضاء (PSNR)، معدل الخطأ (MSE) وأخيرا معدل الخطأ في البتات (BER) ومقارنة النتائج في الحالتين كما بالجدول (1) والجدول (2).

جدول (1) نتائج اختبار مقاييس الأداء عند الترتيب (2:2:4)

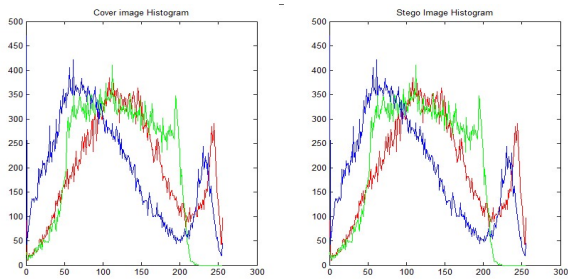
مقاييس الأداء			اسم الصورة
BER	MSE	PSNR	
0.050	0.16	54.83	Baboon
0.049	0.17	61.92	Lena
0.050	0.16	56.13	Balloons
0.049	0.16	56.85	Boat

جدول (2) نتائج اختبار مقاييس الأداء عند الترتيب (2:3:3)

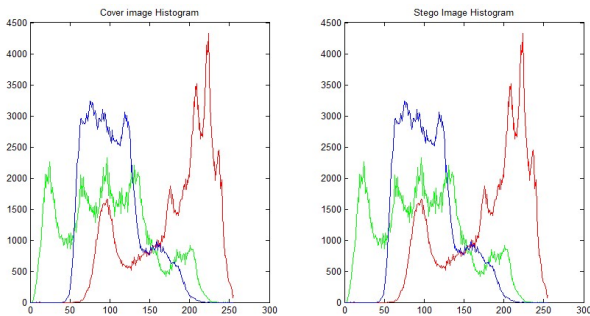
مقاييس الأداء			اسم الصورة
BER	MSE	PSNR	
0.050	0.17	53.99	Baboon
0.048	0.18	61.32	Lena
0.051	0.16	55.80	Balloons
0.050	0.16	56.55	Boat

نستنتج من جداول النتائج السابقة ان الخوارزمية علي الترتيبين (2:2:4) و (2:3:3) قد أعطت نتائج مقاربة جدا في مقاييس الأداء مع وجود اختلاف بسيط حيث تم الاخفاء بالجزء الأقل أهمية لقناة اللون الأزرق بفارق 4 بت عند اختيار الترتيب (2:2:4) بدلا من 3 بتات بالترتيب (2:3:3) وبالتالي تأتي جودة الصورة بالنسبة للعين البشرية بعدم ملاحظة أي تأثير أو اختلاف في صورة الغلاف بالدرجة الأولى، بحيث يمكن أن تتم عملية الإخفاء دون ملاحظة وجود أي بيانات داخلها، وذلك اعتمادا على نظرية الألوان color theory التي تنص على أن قدرة العين البشرية للتمييز بين التدرجات الرقمية القريبة الضعيفة فضلا على قدرتها علي التمييز في التدرجات الغامقة، وحسب نظام الرؤية البشرية HVS فإن العين البشرية أقل تحسسا للون الأزرق من اللونين الآخرين (الأحمر والأخضر).

بالنسبة لمخطط الهستوجرام فقد تم الحصول على مخططات الألوان الموجودة بكل صورة وذلك قبل وبعد عملية الإخفاء كما بالأشكال (10) (11) (12)، والتي توضح أن توزيع الألوان كان متطابقا لكل صورة قبل وبعد التعديل عليها.



الشكل 10. هيستوجرام صورة baboon



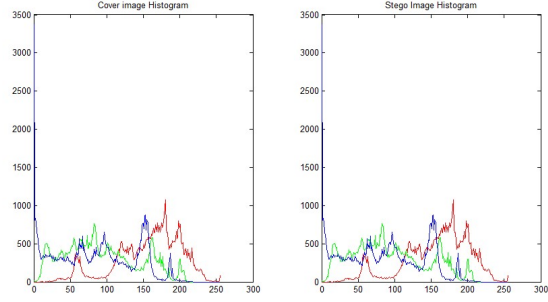
الشكل 11. هيستوجرام صورة Lena

11. الخلاصة :

تم في هذه الورقة العمل على إخفاء بيانات نصية في صورة رقمية ملونة باستخدام خوارزمية البت الأقل أهمية المحسنة (Improved LSB) وذلك على الترتيبين (2:2:4) و (2:3:3) بت في كل قناة لونية RGB، فقد تم بالترتيب الأول تجزئة البايت المراد إخفاؤه الي ثلاث أجزاء يحتوي الجزء الأول والثاني علي 2 بت وتم إخفاؤها في الجزء الأقل أهمية من بايت كل قناة من الألوان (الأحمر والأخضر) بينما تم إخفاء الأربع بتات الأخيرة في الجزء الأقل أهمية من بايت قناة اللون الأزرق، اما بالترتيب (2:3:3) فقد احتوي الجزء الأقل أهمية لقناة اللون (الأحمر) علي 2 بت، بينما احتوي الجزء الأقل أهمية للقنوات اللونية (الأخضر والأزرق) على 3 بتات لكل قناة، وقد كانت النتائج متقاربة الي حد ما مع وجود اختلاف بسيط جدا في قراءة المقاييس والذي يرجع الي اختلاف الترتيب . وقد تبين ان هذه النتائج تعطي إمكانية إخفاء كميات كبيرة من البيانات داخل الصورة بحيث لا يحدث تغير في الصورة من ناحية جودة الأداء.

12. المراجع

- [1] Wang, Y., Tang, M., & Wang, Z. "High-capacity adaptive steganography based on LSB and Hamming code". *Optik*, 213, 164685. (2020).
- [2] Devi, M., & Sharma, N. "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images". *IEEE, Recent Advances in Engineering and Computational Sciences (RAECS)*, pp. 1-5. Vol 34. No.7. (2014) .
- [3] Hegde, R., & S, J. " Design and Implementation of Image Steganography by Using LSB Replacement Algorithm and Pseudo Random Encoding Technique". *International Journal on Recent and Innovation Trends in Computing and Communication*, pp.4415 - 4420. Vol 3. No.7. (2015, July).



الشكل. 12 هيستوجرام صورة Balloons

9. الاستنتاجات

- أ- أعطت الخوارزمية في الترتيبين نتائج جيدة من ناحية مقاييس الأداء وكذلك جودة الصورة، حيث أن مقياس (PSNR) أعطى قيم عالية والذي يوضح نسبة الإشارة إلى الضوضاء مما يعني أن الصورة الناتجة كانت قريبة من الصورة الأصلية.
- ب- مقياس (MSE) أعطى قيم ضئيلة جدا في نسبة التغير بين الصورة الأصلية والناتجة.
- ت- مقياس (BER) فقد أعطى أيضا قيم ضئيلة جدا في عدد أخطاء البتات.
- ث- بالنسبة الي هيستوجرام الصور الأصلية والناتجة فقد أظهر توزيعا متقاربا في الألوان قبل وبعد عملية الإخفاء.
- ج- عند استخدام صور عالية الجودة يمكن الحصول علي نتائج أفضل .

10. التوصيات

- أ- يمكن استخدام ترتيب آخر للبيانات مثل (1:3:4).
- ب- قد يعطي استخدام صور بامتداد من نوع آخر كصورة غطاء نتائج مختلفة.
- ت- يمكن إخفاء صورة داخل صورة أو صوت أو فيديو، كما يمكن إخفاء البيانات في غطاء آخر بدلا من الصورة مثل الصوت أو الفيديو.
- ث- لزيادة لأمن والحماية بالإمكان تشفير البيانات قبل عملية الإخفاء.

12. World Scientific and Engineering Academy and Society,(2008).

[15] Bhattacharyya, Souvik. "Data hiding through multi-level steganography and SSCE." Journal of Global Research in Computer (Science 2.2 2011).

[4] Koppola, Rajinikanth Reddy. "A High-Capacity Data-Hiding Scheme in LSB-Based Image Steganography". Diss. University of Akron, (2009).

[5] Kuo, W. C., Wang, C. C., & Hou, H. C. "Signed Digit Data Hiding Scheme". Information Processing Letters, pp. 15-26. Vol 5. No.2. (2015, August).

[6] Jarno, M. "LSB Matching Revisited. IEEE, Signal Processing Letters, pp. 285- 287. Vol 13 No.5. (2006, May)

[7] Marwa al-Bayati, Mudhafar M. Al-Jarrah, "The Hiding of Multimedia Secret Files in Dual RGB Cover Images Using LSB Steganography Techniques", Computer Science (2016).

[8] Rita, C. & Deepika, B. "An Improved DCT based Steganography Technique", International Journal of Computer Applications, pp. 46-49. Vol 102. No.14. (2014, September)

[9] أم السعد محمد الاميلس وفائزة إسماعيل الجروشي " استخدام الصور الرمادية للمقارنة بين طرق الإخفاء المعتمدة على قيمة البكسل و البيت الأعلى أهمية " Third International Conference on Technical Sciences (ICST2020), 28-30 November 2020, Tripoli – Libya

[10] Kekre, H. B., Archana Athawale, and Pallavi N. Halarnkar. "Increased Capacity of Information Hiding in LSBs Method for Text and Image." International Journal of Electrical, Computer and Systems Engineering 2.4 (2008).

[11] Pan, H. K., Tseng, Y. C & Chen Y. Y. A "Secure Data Hiding Scheme for Binary Images". IEEE Trans. Commun., pp. 1227-1231.Vol. 50.No.8. (2002, August).

[12] Alqadi, Z., Zahran, B., Jaber, Q., Ayyoub, B., & Al-Azzeh, J. "Enhancing the Capacity of LSB Method by Introducing LSB2Z Method". International Journal of Computer Science and Mobile Computing, 8(3), 76-90. (2019).

[13] <http://www.abelard.org/colour/col-hi.htm>

[14] Al-Najjar, Atef Jawad. "The decoy: multilevel digital multimedia steganography model." WSEAS International Conference Proceedings. Mathematics and Computers in Science and Engineering. No.