Authentication of data hiding using co-occurrence matrix

Melad jader saeed **Ghada thanoon**

meladjader@uomosul.edu.iq Ghadathanoon@uomosul.edu.iq

University of Mosul/ College of Computer Science and Mathematics

Received on : 28/3/2011 Accepted on :21/6/2011

ABSTRACT

This research is considered one of the steps aiming to deal with one of the most important challenges facing communicators via Internet, as a means for ensuring information security and verifying the authenticity and credibility of the received message. The research designs and implements proposed system for verifying the authenticity of retrieved information which are ciphered and hidden inside colored images. This is done through utilizing the capabilities and features that the process of image texture analysis offers, using the co-occurrence matrix. The message authenticity is verified by comparing the co-occurrence matrices before sending and after receiving in order to assure non infiltration.

Results of applying this system on image files with different extensions, and on text messages with different sizes too, have shown supremacy in fighting spam.

Keyword: data hiding, authentiacation, co-occurrence,cipher.

وثوقية البيانات المخفية في الصور الملونة باستخدام مصفوفة حدوث المشاركة

ميلاد جادر سعيد **غادة ذنون يونس**

كلية علوم الحاسوب والرياضيات

جامعة الموصل

تاريخ الاستلام: 2011/3/28 **تاريخ القبول: 2011/6/21**

الملخص

يمثل هذا البحث احد الخطوات الهادفة لمعالجة واحدة من أهم التحديات التي يواجهها المتراسلون عبر الشبكة كوسيلة لضمان سرية المعلومات والتحقق من وثوقية ومصداقية الرسالة المستلمة.

اشتمل هذا البحث تصميم وتمثيل نظام مقترح للتحقق من وثوقية المعلومات المسترجعة والتي تكون مشفرة ومخفية بداخل الصور الملونة من خلال الاستفادة من الإمكانيات والمميزات التي توفرها عملية تحليل نسيج الصورة باستخدام مصفوفة حدوث المشاركة co-occurrence matrix. إذ تم التأكد من الوثوقية من خلال مقارنة مصفوفتي حدوث المشاركة قبل الإرسال وبعد الاستلام للتأكد من عدم الاختراق. أظهرت النتائج المطبقة على ملفات صورية ذات امتدادات مختلفة ورسائل نصية بأحجام مختلفة أيضا قوة في مقاومة التطفل.

الكلمة المفتاحية: إخفاء البيانات ، التوثيق ، حدوث المشترك ، التشفير.

1. المقدمة

من المعايير الأساسية لأمن البيانات والتي من الواجب أن تتوفر في نظم المعلومات هي الوثوقية authentication . في البداية لابد من التمييز مابين الوثوقية Authentication، التخويل Authorization

والتحكم في النفاذ Access Control يقصد بالوثوقية: الإجرائية التي يقر النظام بمقتضاها وصول المستخدم إلى المعلومات، وذلك بأن يقارن اسم المستخدم وكلمة سره بمحتوى قائمة المخولين، فإن كان هنالك تطابق، منح المستخدم حق النفاذ إلى الحد المحدد له في قائمة السماحيات. أما التخويل فهو الحق الممنوح لشخص ما بالنفاذ إلى النظام والمعطيات المخزنة فيه. أما التحكم في النفاذ فهو آليات الحد من النفاذ إلى بنود معينة من المعلومات [1].

ولكي يؤمن النظام الآمن تكاملية البيانات المخزنة فيه، أي حماية البيانات المخزونة فيه من عمليات الحذف والتخريب. من خلال مجموعة من الأساليب توفرها نظم قواعد المعطيات كقوائم النفاذ والصلاحيات بالإضافة إلى علاقات الترابط Referential Integrity مابين البيانات المخزنة فيه. كما يؤمن النظام الآمن تكامل البيانات المرسلة لمعرفة فيما إذا تم تعديل أو حذف أي جزء منها أو أنها غير مكررة، وتحقيق ذلك يمكن أن يتم من خلال توليد خلاصة (توقيعٍ) للرسالة المرسلة، باستخدام بعض الخوارزميات، مثل خوارزمية MD5 أو خوارزمية SHA، وتضمين هذه الخلاصة مع كل رسالة ترسل عبر الشبكة، وبالتالي التأكد من أن الرسالة صحيحة ولم يتم العبث بها. أما في بحثنا فقد تم الاستفادة من تحليل نسيج الصورة للتحقق من وثوقية الصورة المستلمة التي تحوي على الرسالة المخفية. يمكن تحقيق سرية وخصوصية نقل المعلومات من خلال تضمينها داخل وسط حامل لها وهناك عدة اتفاقيات وتقنيات تضمين تمكننا من إخفاء المعلومات في شيء معين وجميع الاتفاقيات والتقنيات يجب أن تحقق عددا من المتطلبات لكي يمكن تطبيق نظرية إخفاء المعلومات بصورة صحيحة, وفي أدناه مجموعه من المتطلبات الرئيسية.[1]

1- الإكمال الصحيح للمعلومات المخفية لدى تضمينها داخل الغطاء الحامل, بحيث أن الرسالة السرية يجب أن لا تتغير إذ أن تغيير البيانات المضمنة يعني فشل العملية.
2- الوسط الناقل الذي يغطي الرسالة السرية يجب أن لا يتغير أيضا وعلى الأقل أن لا تكون تغييراته ظاهرة للعيان, وفي حالة كون التغييرات على الوسط الحامل كبيرة وظاهرة للعيان،فان الشخص الذي يشاهدها سوف يعلم بوجود معلومات مخفيه داخله فيحاول أن يفتحها أو يدمرها.
3- يؤخذ بنظر الاعتبار دائما أن المهاجم على علم بوجود معلومات مخفية داخل الغطاء الحامل.

وإن تكنولوجيا الكومبيوتر والانترنيت أعطت حياة جديدة لعلم إخفاء المعلومات والطرائق المبتكرة لخدمتها ويمكن أن تخفى المعلومات في أوساط متعددة. إذ يمكن الإخفاء داخل نص text أو الإخفاء داخل البرامج software أو الإخفاء في مساحة القرصDisk space والإخفاء في الصوت Audio أو الإخفاء في الصور Image.

ففي الصور, يمكن أن تخفى المعلومات بطرائق مختلفة ويمكن إخفاء المعلومات مباشرة بحيث يتم حشر كل مرتبة ثنائية من المعلومات في الصورة أو تضمن المعلومات اختياريا في المساحات المشغولة التي تكون اقل إدراكا. وقد تتبعثر المعلومات بصورة عشوائية أو تتكرر بضع مرات في كل مكان من الصورة. ويمكن الإخفاء في الصور الثنائية Binary Image ، والصور ذات التدرج الرمادي (Gray level Images) والصور الملونة (Color Images): والتي تم اعتمادها في هذا البحث إذ انه منذ ظهور الصور الملونة ومع مرور الزمن زاد عرض اللون، وزاد عدد التدرجات التي يمكن عرضها لكل لون, لكن بقي المبدأ الأساسي لتمثيل الصور كما هو, إذ تتكون كل (pixel) عن طريق تجميع الألوان الرئيسة الثلاثة الأحمر (red)، الأخضر (green)، والأزرق(blue)، وبدمج شدة الإضاءة لهذه الألوان الثلاثة يتم تشكيل اللون المطلوب(RGB). [2,1]

2- طرق الإخفاء:

هناك عدد كبير من طرائق الإخفاء في الصور من أشهرها: [3]

- تقنية تغير البت الأقل أهمية Least Significant Bit Replacement Technique
- تقنية تغير البت الوسطي Moderate Significant Bit Replacement Technique

في هذه التقنية يتم تغير البتات الأخيرة لكل نقطة (pixel) في الغطاء الصوري أي 4bits، ولقد تم الاستفادة من هذه الفكرة في بحثنا في مرحلة إخفاء الرسالة المراد إرسالها داخل صورة باستخدام البت الخامس والسادس والسابع من كل نقطة .إذ أن المعلومات المخفية في هذه المواقع تكون أكثر مقاومة للتهديدات التي تحاول تغييرها أو إزالتها. وكما هو معلوم إن هذا التغيير يؤدي إلى ظهور تشوهات في الصورة ولقد تم تجاوز هذه النقطة بتنفيذ الخطوتين التاليتين:

- القيام بعملية إخفاء البيانات في إطار الصورة فقط وقد تم البدء من التدرج الأحمر ثم الأخضر ثم الأزرق.
- تحسين الصورة الناتجة من عملية الإخفاء

ومن خلال تطبيق النقطتين السابقتين تم إنتاج صورة لا تحوي أي تشوه ممكن أن يثير الشك للمتطفل.

3- الأعمال السابقة:

من خلال قراءة عدد من البحوث تم استنباط أفكار عدة ومن ثم دراستها وتطوير البعض منها للوصول إلى النتائج الموضحة، ففي البحث [3] تم إخفاء نص داخل صورة ملونة باستخدام طريقة الإخفاء بتغير البتات الوسطية وتحسين الصورة الناتجة باستخدام median filter، أما [4] فقد تم استخدام مصفوفة حدوث المشاركة لتمييز الجلد بين الأشخاص، في حين أن [5] قد استخدم طريق TOPAZ لإخفاء نص داخل صورة ملونة واعتمد على أحجام ثابتة للنص والصورة، أما [6] استخدم طرائق مختلفة للإخفاء بداخل الصور باستخدام بت واحدة أو اثنين أو ثلاثة أو أربعة ودراسة مميزات كل طريقة.

4- تحويل فوريير السريع Fast Fourier Transformation:

هو احد أنواع التحويلات (Transformation) التي تنقل الصورة من صيغة إلى أخرى ولكي تعالج الصورة أو الإشارة على الحاسوب يجب أن يتم تحويلها إلى القيم غير المستمرة (Discrete) أي ثابتة أو متقطعة ، إذ أن أساس عمل فوريير السريع هو تجميع صفات الصورة حسب الخواص الترددية لها لغرض تسهيل عملية المعالجة، ويتم حسابه حسب المعادلة الآتية [2]:

$$F(u) = \int_{-\infty}^{\infty} F(x) e^{-j2\Pi ux} \quad ...(1)$$

5- تحسين الصور الرقمية Digital Image Enhancement

يعرف التباين بأنه تدرج و توزيع قيم وحدات الصورة الرقمية على المقياس من 0 إلى255 المستخدم بواسطة الحاسوب ، و بمعنى أوضح هو التدرج من المناطق المظلمة في الصورة إلى المناطق المضيئة ، و يعبر عنه رياضيا بالمعادلة التالية:

$$C = (Imax - Imin) / (Imax + Imin) \quad ...(2)$$

حيث أن C تمثل التباين و I_{max} و I_{min} تمثلان شدة الإضاءة القصوى و الدنيا على التوالي .

وحتى يسهل تفسير الصورة يتم تحسينها إما بتغيير التباين ليشمل التدرج الرمادي أو تحويل التدرج الرمادي إلى تدرج لوني [7, 2].

و لإجراء تحسين لهذا التباين أو للوضوح الإشعاعي للصورة هنالك تقنيات متعددة و جل هذه التقنيات تنطلق من مبدأ تمديد التدرج الرمادي أو توزيع الأعداد الرقمية لوحدات الصورة بحيث تغطي كل المدى الممكن، أي من السواد الداكن إلى البياض الناصع أو من العدد الرقمي 0 إلى العدد الرقمي 255 ، كما و أن هنالك تقنيات يتم فيها تحويل التدرج الرمادي في الصورة إلى ألوان زائفة، كل ذلك الغرض منه تسهيل عملية تفسير الصورة واستنباط المعلومات.

ومن التقنيات المعتمدة في هذا المجال: تمديد التباين الخطي Linear contrast stretch

إن الفكرة الأساسية هي زيادة مدى الأعداد الرقمية في الصورة، فبدل أن تكون الأعداد الرقمية لوحدات الصورة كلها محصورة في نطاق ضيق t تكون الصورة المرئية قاتمة كلها أو ناصعة البياض فإن الهدف هو توزيع الأعداد الرقمية للصورة لتشمل جميع المدى المتاح وهو من 0 إلى 255 ، حتى يكون هنالك مدى تباين واسع بين وحدات الصورة و يسهل من عملية تفسير الصورة المرئية.

إن الدالة المستخدمة في هذه الطريقة هي دالة خطية يمثلها النموذج التالي [7]:

$$DNo = 255\ [(DNi - DNmin) / (DNmax - DNmin)] \quad \ldots(3)$$

حيث أن DN_o = العدد الرقمي المخرج لوحدة صورة

DN_i = العدد الرقمي الأصلي (المدخل) لوحدة الصورة

DN_{min} = أقل عدد رقمي في البيانات المدخلة

DN_{max} = أقصى عدد رقمي في البيانات المدخلة

ولأنها تستخدم على صور أحادية ولما يتطلبه العمل البحثي فقد تم تطبيق هذه المعادلة على جزء الأحمر من الصورة ثم الأخضر وبالتالي الأزرق وبعد ذلك تم دمج الأجزاء الثلاثة في صورة واحدة لينتج صورة ملونة وبالتالي تم تحسين الصورة الملونة باستخدام هذه الطريقة التي أثبتت أنها لا تسبب فقداناً بالمعلومات أثناء إجراء عملية التحسين. [7, 2]

6- خواص مستندة إلى النسجة Texture Based Features:

إن النسجة (texture) واحدة من أكثر الخواص التي تستخدم لتحليل الصور وتفسيرها، فالنسجة هي مقياس لاختلاف كثافة السطح، وتحدد بعض خواص الصورة، وقد طبق العديد من الأساليب لتحليل النسجة وتصنيفها ومنها الطول المتواصل والأبعاد الكسورية للصورة وتحويل الموجة المنفصلة ومصفوفات حدوث المشاركة والتي تعد من أكثر الأساليب استخداماً بسبب قدرتها العالية على ملاحظة الترابط المكاني وتحديده (spatial dependence) للمستويات الرمادية التي تساعد على إدراك خواص النسجة.

6-1 مصفوفة حدوث المشاركة Co-occurrence matrix:

إن هذه المصفوفات اقترحها العالم Haralick في عام 1973، وهي مصفوفة ثنائية الأبعاد (معتمدة على المستويات الرمادية)، تستخدم بشكل أساسي في تحليل النسجة بسبب قدرتها العالية على تحديد الترابط المكاني لقيم

المستويات الرمادية في الصورة، إذ تعمل مصفوفة حدوث المشاركة (P) بوصفها جامعاً تراكميا (accumulator) وكل خلية فيها (P[i,j]) عدداً لعدد أزواج النقط الصورية التي تمتلك الكثافة (i) و (j)، ويعرف كل زوج للنقطة الصورية بالبعد والاتجاه الذي يمكن أن يمثل بمتجه الإزاحة (d=(dx,dy))، و(dx) تمثل إزاحة النقطة الصورية من المحور السيني (x-axis) و(dy) يمثل إزاحة النقطة الصورية من المحور الصادي (y-axis)، ومن اجل تحديد الاعتماد المكاني لقيم المستوى المكاني تم حساب عدد من خواص النسجة ، المذكورة في الجدول (1) والتي اعتمدت للتأكد من وثوقية الصورة المرسلة [4]، وهي:

جدول (1). خواص النسجة

ت	الصفة	الصيغة العامة
1	العشوائية Entropy	$\sum_{i}^{M}\sum_{j}^{N} \mathrm{P}[i,j]\log \mathrm{P}[i,j]$
2	الطاقة Energy	$\sum_{i}^{M}\sum_{j}^{N} \mathrm{P}^2[i,j]$
3	التباين Contrast	$\sum_{i}^{M}\sum_{j}^{N} (i-j)^2 \mathrm{P}[i,j]$
4	التجانس Homogeneity	$\sum_{i}^{M}\sum_{j}^{N} \frac{\mathrm{P}[i,j]}{1+\lvert i-j \rvert}$
5	المتوسط Mean	$\frac{1}{2}\sum_{i}^{M}\sum_{j}^{N} (ip[i,j]+jp[i,j])$
6	الاختلاف Variance	$\frac{1}{2}\sum_{i}^{M}\sum_{j}^{N} ((i-\mu)^2 p[i,j]+(j-\mu)^2 p[i,j])$
7	الارتباط Correlation	$\sum_{i}^{M}\sum_{j}^{N} \frac{(i-\mu)(j-\mu)p[i,j]}{\sigma^2}$
8	عزم الاختلاف المعكوس Inverse difference moment	$\sum_{i}^{M}\sum_{j}^{N} \frac{p[i,j]}{\lvert i-j \rvert^k} i \neq j$

7- التكميم الخطي والتشفير Quantize & encode:

تتم عملية تكميم خطي وتشفير للبيانات الحقيقية المدخلة من نوع floating point وإخراجها على شكل بيانات من نوع integer . فكرة هذه الطريقة تعتمد على تكميم المصفوفة المدخلة التي تحوي على بيانات حقيقية وتشفيره كبيانات من نوع integer باستخدام level quantity 2^n ومبدأ عمل الخوارزمية:

إن مدى البيانات المدخلة يكون ما بين [v , v-] الذي سيقسم على 2^n وسينتج منه فترة محددة بحيث أن المخرجات الناتجة من عملية التكميم الخطي يجب أن تقع ضمن أول فترة حصلنا عليها من عملية التقسيم وتستمر عملية التكميم الخطي والتقسيم حتى نصل إلى البيانات المطلوبة، وان العملية تكون معاكسة في حالة dequantize encode.[8]

8- الخوارزمية المقترحة في الإرسال:

المدخلات: النص المطلوب إرساله للطرف الآخر، صورة ملونة بامتداد Bmp, Jpg, Gif

1. البداية.
2. تجزئة الصورة إلى المكونات الأساسية (الأحمر والأخضر والأزرق) .
3. تحويل النص إلى نظام الاسكي ومن ثم الثنائي.
4. إخفاء النص بإطار الجزء (الأحمر) من الصورة ابتداءً من الأعلى ثم الأسفل ثم الأيسر ثم الأيمن وباستخدام طريقة (تغير البتات الأخيرة) ولقد تم استخدام البت 5 و6 و7.
5. إجراء عملية تحسين على الصورة الناتجة من عملية الإخفاء باستخدام linear streach على الصورة الملونة من اجل القضاء على أي تشوه يحدث على الصورة جراء عملية الإخفاء.
6. إجراء عملية طرح بين الصورة التي تحوي الإخفاء و الصورة بعد التحسين لينتج صورة جديدة.
7. إجراء عملية ترميز على الصورة الجديدة باستخدام Quantization encoding لينتج الصورة المرمزة.
8. إجراء عملية تحويل للصورة المحسنة إلى النظام فورير السريع FFT.
9. دمج نقاط الصورة المرمزة مع الصورة المحولة إلى FFT وإنتاج صورة مبهمة المعالم.
10. حساب مصفوفة حدوث المشاركة للصورة الناتجة.
11. تجزئة الصورة إلى المكونات الأساسية (الأحمر والأخضر والأزرق).
12. إخفاء قيم مصفوفة حدوث المشاركة بإطار الجزء (الأزرق) من الصورة ابتداءً من الأسفل ثم الأعلى ثم الأيسر ثم الأيمن و باستخدام طريقة (تغير البت الوسطي).
13. ومن ثم إرسال الصورة الأخيرة.
14. النهاية.

الشكل (1) يوضح المخطط الصندوقي للخوارزمية المقترحة.

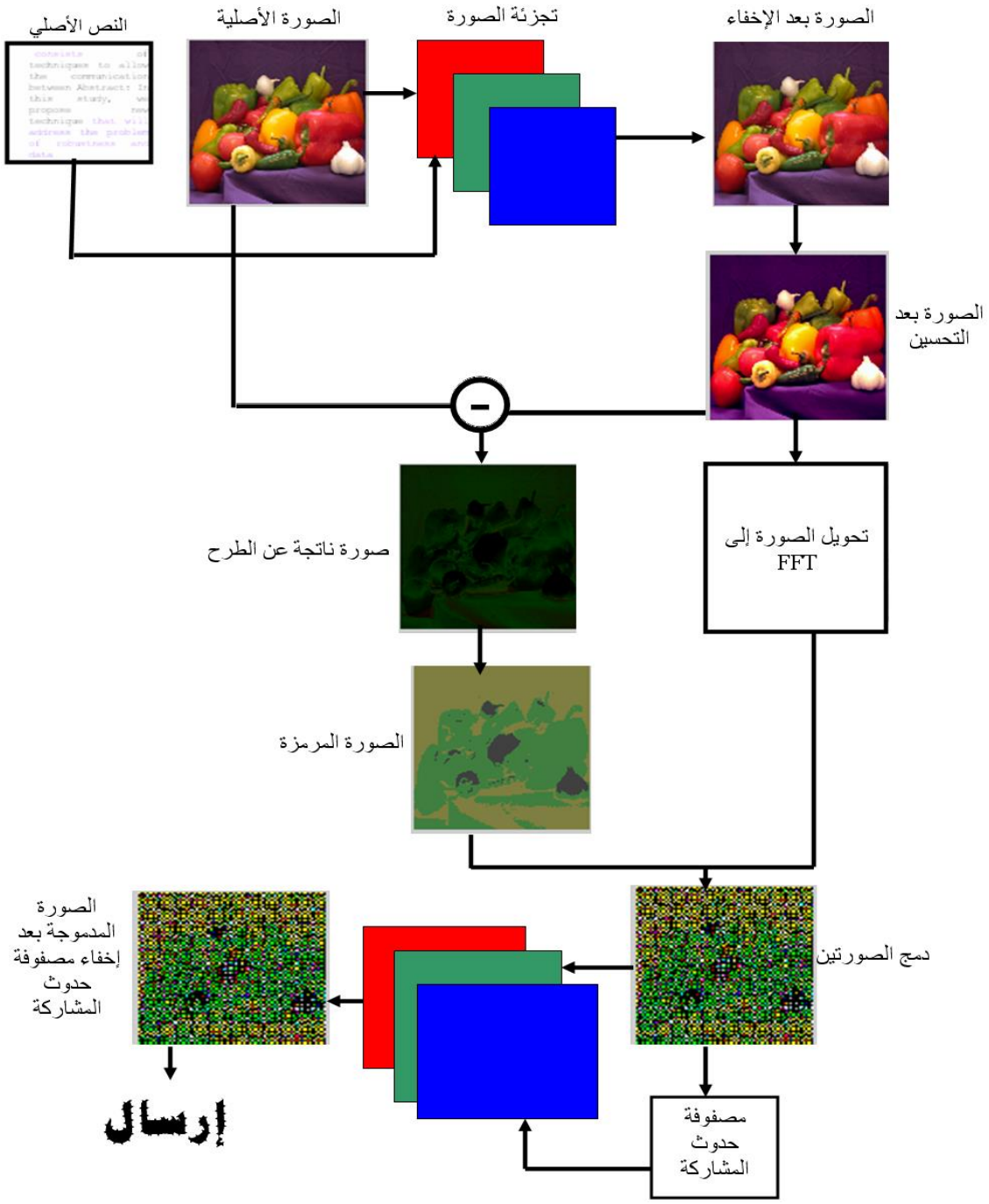
9- الخوارزمية المقترحة في الاستلام:

المدخلات: الصورة المدموجة بعد إخفاء مصفوفة حدوث المشاركة فيها.

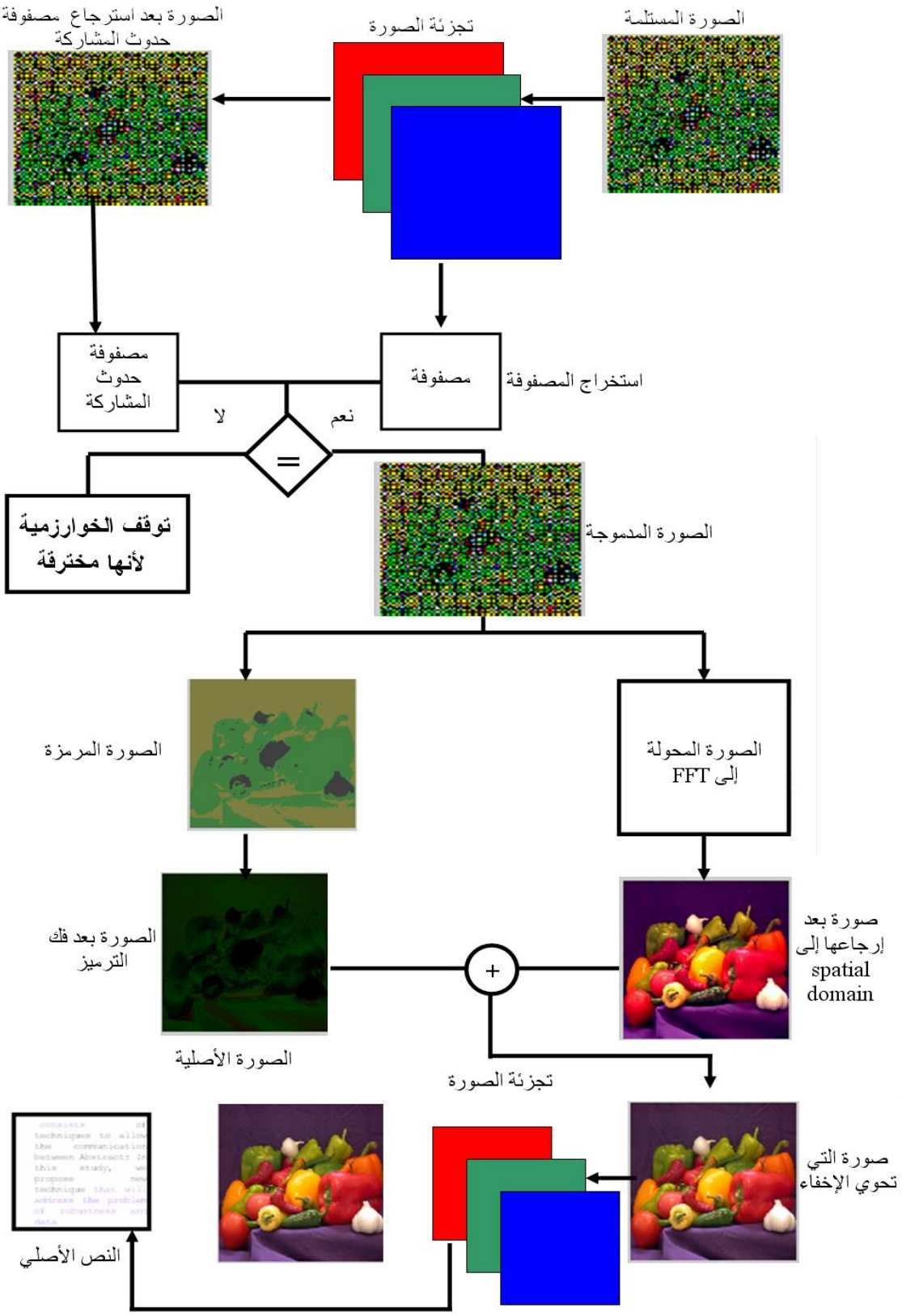
1. البداية.
2. استلام الصورة المدموجة والحاوية على مصفوفة حدوث المشاركة التي سوف تستخدم للتحقق من الوثوقية.
3. تجزئة الصورة إلى المكونات الأساسية (الأحمر والأخضر والأزرق).
4. استرجاع المعلومات المخفية الموجود في إطار الصورة الأزرق لإنتاج مصفوفة حدوث المشاركة.
5. حساب مصفوفة حدوث المشاركة للصورة الناتجة بعد استرجاع المعلومات المخفية.
6. مقارنة مصفوفتي حدوث المشاركة الناتجتين بالخطوات السابقة ، في حالة التساوي دليل على الوثوقية وإلا فان الصورة محرفة وسوف تتوقف الخوارزمية.
7. فك دمج الصورتين عن طريق توزيع النقاط الفردية لتمثل الصورة المحولة إلى FFT ، والنقاط الزوجية لتمثل الصورة المرمزة.
8. تحويل الصورة المحولة إلى النظام المكاني Spatial Domain باستخدام inverse Fast Fourier transform والتي تمثل الصورة المحسنة.
9. فك رمز الصورة المرمزة باستخدام Dequantization decoding.

10. جمع الصورة المحسنة مع الصورة بعد فك الترميز منها لتنتج الصورة التي تحوي الإخفاء.
11. تجزئة الصورة إلى المكونات الأساسية (الأحمر والأخضر والأزرق).
12. استرجاع المعلومات المخفية الموجودة في إطار الصورة الأحمر لينتج الرسالة المراد إرسالها.
13. النهاية.

المخرجات: الرسالة، الصورة الحاملة للرسالة. الشكل (2) يوضح المخطط للخوارزمية المقترحة للاستلام.



شكل (1). مخطط يمثل الخوارزمية المقترحة للإرسال



شكل (2). مخطط يمثل الخوارزمية المقترحة للاستلام

10- مناقشة النتائج:

من خلال تطبيق الخوارزمية على أكثر من صورة تختلف بالنوعية والامتداد أثبتت الخوارزمية نجاحها من خلال مقاييس الكفاءة التي تم اعتمادها وهي [2] :

1. مقياس مقدار التشوه: وهو قيمة الكفاءة المستخدمة لقياس مدى التشوه في الصورة الناتجة من عملية الإخفاء باعتماد المعادلة الآتية:

$$PSNR=10\log_{10}(\frac{C_{\max}^2}{MSE}) \quad \ldots(4)$$

$C_{\max}$: أعلى قيمة لونية في الصورة.

$$MSE=\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy}-C_{xy})^2 \quad \ldots(5)$$

M, N : أبعاد الصورة.

S_{xy} : تمثل الصورة الأصلية (الغطاء).

C_{xy} : تمثل الصورة التي تحوي المعلومات المخفية.

2. معامل الارتباط Correlation Function:

تستخدم هذه الدالة لغرض إجراء مقارنة بين مصفوفتين وملاحظة مدى التقارب بينهما فكلما كانت القيمة الناتجة قريبة من الواحد كان ذلك دليلاً على درجة الوضوحية وقلة وجود التشوه [2].

القانون العام لها

$$A=corr2(p1,p2) \quad \ldots(6)$$

P1: الصورة الأصلية (الغطاء).

P2: الصورة التي تحوي المعلومات المخفية.

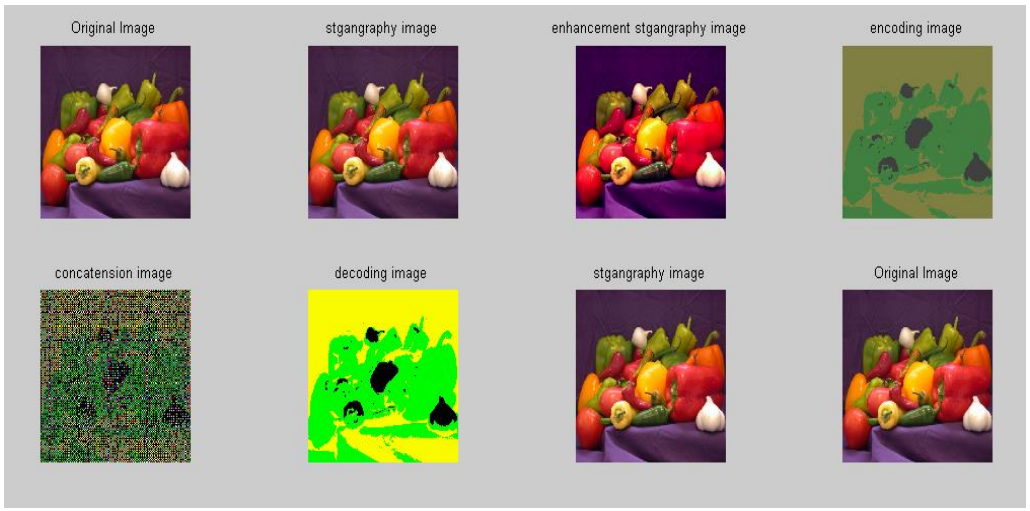
- فيما يلي بعض الأمثلة العملية التي توضح خطوات الخوارزمية المقترحة وقيم المقاييس المستخدمة، وفي جميع الحالات تم إرجاع النص الأصلي بدون تحريف وكان النص الأصلي:

consists of techniques to allow the communication between Abstract: In this study, we propose new technique that will address the problem of robustness and data

ويمكن تحديد حجم النص الذي ممكن إخفاؤه داخل الصورة المستخدمة كغطاء من خلال المعادلة التالية:

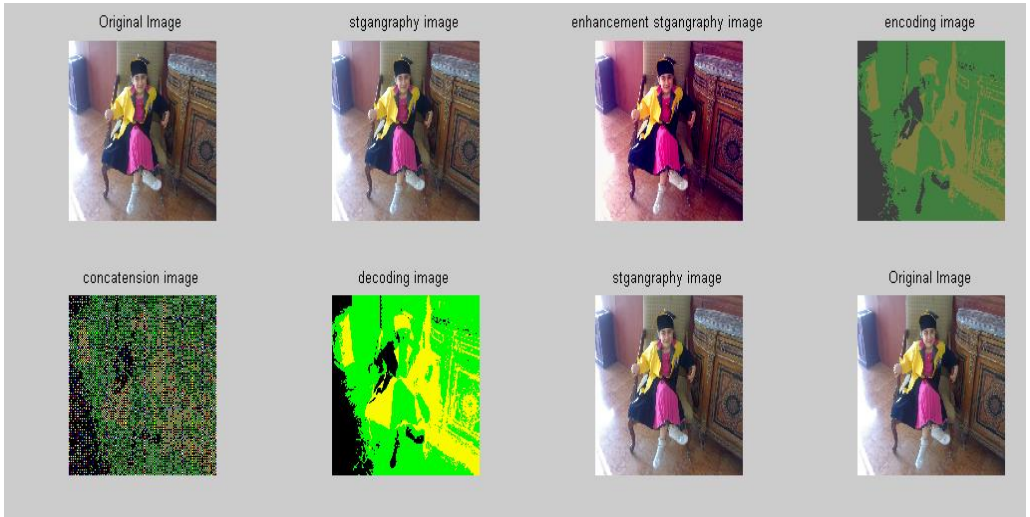
$$No.\ of\ letter\ in\ message = (size\ of\ image * 11 * 3)/8 \quad \ldots(7)$$

وذلك لأنه الإخفاء يكون في إطار الصورة الأحمر في الأعلى ثم الأسفل ثم الأطراف يليه إطار الصورة الأخضر بنفس التسلسل ومن ثم إطار الصورة الأزرق الجزء العلوي والأطراف فقط لان الأسفل يكون لإخفاء مصفوفة حدوث المشاركة، ولأنه في كل بايت يمكن إخفاء ثلاثة بتات فقد تم الضرب في ثلاثة ومن ثم التقسيم على ثمانية لإنتاج عدد الحروف التي يمكن إخفاؤها بداخل تلك الصورة.



شكل (3). صورة الفواكه

شكل (4). صورة سلة الورد



شكل (5). صورة البنت

جدول (2). مقاييس كفاءة

اسم الصورة	نوعها	قيمة PSNR	قيمة Correlation	نسبة استرجاع النص
صورة الفواكه	JPG	65.7340 db	1	%100
صورة سلة الورد	JPEG	59.6248 db	1	%100
صورة البنت	BMP	58.6763 db	1	%100

11- الاستنتاجات :

أثبتت النتائج العملية كفاءة الخوارزمية المقترحة من ناحية الوثوقية وان المعلومات المخفية لم يحدث لها أي تغير أو تشوه على الملف الصوري الذي يعد غطاء ، إذ تم قياس مدى صلاحية ووضوحية الصورة الناتجة بعد التضمين فكانت قيمة (PSNR) peak signal to noise Ratio = تتراوح بين (58.6763 db) – (65.0734db) لمجموعة الصور التي أخذت كعينات، وكذلك قيمة Correlation كانت مساوية للـ (1) في جميع الحالات.

أما من ناحية أخرى فقد امتازت هذه الخوارزمية بالسعة العالية إذ أن عملية إخفاء في 3bits من كل byte في الصورة أمكننا من إخفاء نص يحوي عدد كبير من الأحرف وحسب ما موضح بالمعادلة رقم 7.

إضافة إلى السرية العالية إذ انه في هذه الطريقة لا يتم إرسال الصورة التي تحوي النص المخفي مباشرة stego-imag ولكن يمر بعدد من المراحل للتغير ومن ثم إرساله.

12- التوصيات:

1. تشفير النص المراد إرساله قبل إخفائه بأحدث الطرق ومن أشهرها T-code.
2. الاستفادة من خصائص الخوارزمية الجينية أو الشبكات العصبية وإدخالها ضمن هذه الخوارزمية.

المصادر

[1] الحمامي، علاء حسين،العاني، سعد عبد العزيز، (2007)، تكنولوجيا أمنية المعلومات وأنظمة الحماية.

[2] Gonzalez, Rafael C.&woods, Richardv E., 2002,"digital image processing", pearson Education. ISBN 81-7808-629-8.

[3] Babita A. Manpreet K., Manav R. 2009, " High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering ,vol. 1, No. 1, may 2009.

[4] Khalil I. and shaimaa M. ,2010," Skin classification based on co-occurance matrix" , Raf. J. of comp. & math s., vol. 7, no. 3, third scxienfific conference information technology.

[5] Ibrahim A., Zabian A.,2009 ,"Algorithm for Text Hiding in Digital Image for information Security", IJCSNS International Journal of computer Scince and Network Security, VOL. 9 NO.6, june 2009.

[6] Namita T. & Dr. Madhu S., 2010, " Evaluation of variious LSB based of image steganography on GIF file format ", international journal of computer applications (0975-8887) volum 6-no.2, septembar.

[7] Ismat M.,2007, " Digital Alimage processing in remote sensing", final research report no 6/427.

[8] The mathworks, Inc, 2009.

Email: webmaster@mathworks.com