مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (1) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (1) 2017

مقارنة بين أسلوبي الإخفاء في المجالين: الفراغي والترددي للصور الرقميَة

د. رياض ضاهر [*]
إيهاب عيسى صالح [**]

(تاريخ الإيداع 4 / 9 / 2016. قُبِل للنشر في 30/ 1 / 2017)

□ ملخّص □

تزداد أهمية أمن المعلومات هذه الأيام بازدياد تعقيد وسائل الاتصال و أنظمة الحواسيب، و على الرغم من الأمان الذي تحققه خوارزميات التشفير للأطراف المتراسلة، تبقى الرسالة المشفرة عرضة لأنواع من الهجمات المختلفة التي قد يكون أحد أهدافها تخريب كمالية المعطيات المتبادلة كتحريفها او إخفاء وجود بعض المعلومات فيها لذا كان من الأفضل إخفاء وجود بيانات سرية يتم تبادلها أصلاً، حتى و إن كانت مشفرة، مما يجعل المهاجم غير قادر على معرفة وجود اتصال سري بين الطرفين المتراسلين من عدم وجوده و عملية الإخفاء هذه لا تنتمي بشكل مباشر إلى علم التشفير Cryptography بل تندرج تحت مسمى علم الإخفاء Steganography .

يهدف علم الإخفاء إلى حجب وجود عملية تراسل للمعطيات و هو ما يتطلب وجود وسط مضيف حاملا للرسالة قد يكون أي ملف رقمي سواء كان صورة أو فيديو أو ملفات نصيّة أو اي ملف يمكننا استغلال وجود مساحات غير مستخدمة أو يمكننا استخدامها دون ترك أثر واضح مثير للشبهات على الملف المضيف.

يمكن استخدام عدة أساليب تقليدية للقيام بعملية الإحفاء ضمن الأوساط الرقميّة، إلا أن زيادة الاهتمام بمسألة حماية المعلومات و امنها أدى إلى اعتماد عدة خوارزميات متقدمة تعتمد على مفاهيم معالجة الإشارة و نظرية المعلومات و في هذا البحث كان التركيز على خوارزميات الإخفاء الحديثة المستخدمة في الصور الرقمية و التي تعتبر من أكثر الوسائط الرقمية التي تستخدم كوسيط حامل للرسالة السرية، و نقدم دراسة لعملية المقارنة بين أحدث الخوارزميات المتبعة وفق عدد من المعايير الرياضية مع مناقشة النتائج المستخلصة من هذه المقارنة.

الكلمات المفتاحية :DWT, DCT, LSB, PNSR, NC, MSE,

[*] أستاذ مساعد، قسم هندسة الحاسبات و التحكم الآلي، كلية الهندسة الميكانيكية و الكهربائية، جامعة تشرين، اللاذقية، سورية
[**] ماجستير هندسة حاسبات، قسم هندسة الحاسبات و التحكم الآلي، كلية الهندسة الميكانيكية و الكهربائية، جامعة تشرين، اللاذقية، سورية

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (1) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (1) 2017

A comparison between two hiding models: in the spatial domain and the frequency domain of the digital images

Dr. Reyad Daher [*]
Ehab Issa Saleh [**]

(Received 4 / 9 / 2016. Accepted 30 / 1 / 2017)

□ ABSTRACT □

Nowadays, the importance of information security is increasing according to the complexity of communication devises and their operating systems. Although of the safety that the encryption algorithms can provide between communication users, the encrypted messages may faces lot of attack types, which their purposes vandalism of data integrity such distorting or hiding some or all information, so it will be better to hide information transform existing, even though these information are encrypted, therefore the attacker will not know that there is a secret communication between communication users, this operation of hiding data doesn't belong directly to the *Cryptography* science, but it falls under *Steganography* science .

In general, Steganography science aim to hide the secret message exchanged between users, which requires a host milieu carrying the secret message, this host may be any file type such as audio file, video file, image file or any type of digital file we can exploit the existence of unused spaces of file, or any space we can use without doing any effect may lead the attackers to know where the message stay in file.

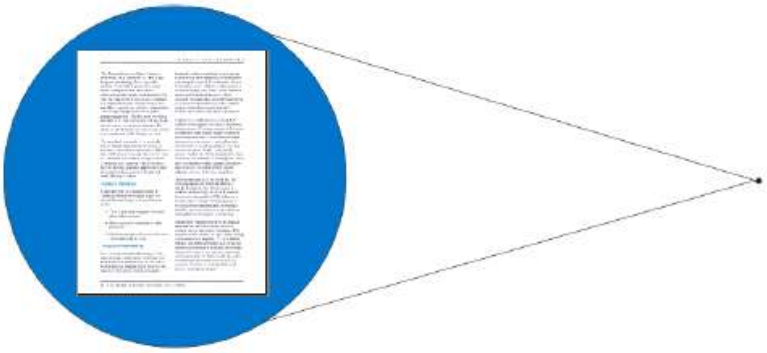
It could use some traditional ways to apply data hiding in digital medias, but due to the increment of interest with information safe and security, many advanced algorithms which depend on information theory and signal processing have been adopted, in this paper we concentrated on Steganography algorithms in image files, which considered as the most host files used to carry the secret message, and put a study of comparison process between the newest algorithms that use data hiding in digital images using some mathematical standards, with discuss the final results of this comparison.

Key words: MSE : Mean Square Error ; PSNR : Peak Signal to Noise Ratio; NC : Normalization Correlation; LSB : Least Significant Bit ; DCT : Discrete Cosine Transform; DWT : Discrete Wavelet Transform

[*] **Associated Prof ,Department Of Computers And Automatic Control Engineering, Faculty Of Mechanical And Electrical Engineering, Tishreen University, Lattakia, Syria.**
[**] **Master In Computers Engineering, Department Of Computers And Automatic Control Engineering, Faculty Of Mechanical And Electrical**

مقدمة :

إن مصطلح الإخفاء Steganography مشتق من عبارة اغريقية قديمة مكونة من كلمتين *steganos* و التي تعني التغطية أو الحماية و *graphein* والتي تعني الكتابة لتشكلان العبارة "تغطية الكتابة " او "الكتابة المخفية"، و قبل البدء بالحديث عن التطبيق الرقمي لعلم الإخفاء لابد من الاشارة إلى بعض استخداماتها في العصور القديمة و قبل بدء عصر الحاسبات و التمثيل الرقمي للبيانات ففي أثناء الحرب العالمية الثانية اتبع الألمان طريقة لإخفاء رسائلهم أو مخططاتهم السرية و هي النقاط الميكروية Microdots وهي عبارة عن نقط صغيرة مصنوعة من مادة ذات خصائص معينة تسمح بتصغير الرسالة التي قد تكون نصاً إلى حجم صغير جداً يقاس بـ ميلي متر ولن تتم رؤية محتوى النقطة الميكروية مالم يستخدم عدسات مكبرة، و الشكل(1) يبين نقطة ميكروية تمثّل رسالة سريّة مصغرة لا ترى بالعين المجردة [13].



الشكل(1) النقطة الميكرويّة، أحد اساليب الإخفاء التقليديّة.

و مع ظهور عصر الحواسيب و التمثيل الرقمي للبيانات انتقلت تقنيات الاخفاء إلى العصر الرقمي و كانت المهمة هنا إخفاء سلسلة البتات المعبرة عن الرسائل السرية ضمن بتات الوسط المضيف وفق أساليب و خوارزميات متعددة تعتمد بشكل أساسي على طبيعة هذا الوسط (ملف نصي ، صورة ، فديو ، صوت ، بروتوكول .....).

قد تتشابه بعض الأوساط المضيفة بخوارزمية الاخفاء المتبعة، كأن نطبق نفس خوارزمية الاخفاء المستخدمة للصور الرقمية على ملفات الفيديو نظراً للتشابه الكبير بين نظريات معالجة الصور الرقمية و الفيديو[1]، و قد يتم اتباع طرق عشوائية من أجل اخفاء مجموعة من البتات ضمن بتات الوسط المضيف.

أهمية البحث و أهدافه :

تأتي اهمية هذا البحث من الأهميّة المتزايدة لعلم الإخفاء و انتشار تطبيقاتها بشكل واسع في الوسائط الرقميّة، فقد استخدمت بشكل كبير في تأمين حقوق النشر و الملكيّة للكثير من المواد المتداولة، كذلك في تحسين وثوقيه النتائج عند القيام بعمليات البحث عن الصور المهمة في محركات البحث، فالعديد منا لديه بعض الشكوك في معرفة مصادر المعلومات و البيانات المنتشرة على الشبكة العنكبوتية فوسائل تعديل الصور و الملفات منتشرة بكثرة و بشكل تنافسي و حتى اثبات وجود علامة مائية الكترونية على السلعة أو المنتج لم يجعلها منيعة أمام وسائل العبث و التعديل لذلك

استخدمت خوارزميات الاخفاء في اثبات أصالة المنتج أو المعلومة المأخوذة من الانترنت بحيث أن تعديل جزء و لو ببسيط من البيانات سيظهر لدى الزبون أو المستثمر[1].

أما أهداف هذا البحث تتخلص بدراسة أهم خوارزميات الإخفاء في الصور الرقميّة و تحديد الخوارزمية الأمثل للاستخدام وفق النتائج النهائية لعملية المقارنة المتبعة في البحث و اقتراح أساليب المقاومة ضد الهجمات المحتملة التي قد يتعرض لها الملف المضيف الحامل للرسالة السرية.

طرائق البحث و مواده :

يبدأ هذا البحث بدراسة أساليب الإخفاء في الصور الرقميّة و التي يمكن تلخصيها و بشكل عام في المجال الفراغي و المجال الترددي للصورة، و من أجل تحديد الاختلاف بين هذين الأسلوبين لا بد من وجود أساليب معيارية من أجل حساب كفاءة نظام الاخفاء المستخدم و بما أننا هنا نتعامل مع الصور الرقمية بالتالي جميع المقاييس المستخدمة يجب أن تركز على حساب جودة الصورة ومن أهم هذه المقاييس المستخدمة في حساب جودة الصور الرقمية:

1. متوسط الخطأ التربيعي(Mean Square Error (MSE :

إن قيمة متوسط الخطأ التربيعي تشير إلى مقدار انحرافات مقدار معين عن القيمة الفعليّة و كلما انخفضت قيمة متوسط الخطأ التربيعي حصلنا على نتائج أفضل، و عند تعاملنا مع الصور الرقمية تكون علاقة متوسط الخطأ التربيعي MSE هي كالتالي [7] :

$$MSE=\frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(C(i,j)-S(i,j)\right)^2 \qquad (1)$$

حيث m , n هي أبعاد الصورة المستخدمة (الصورة الأصلية و الصورة بعد الإخفاء يجب أن تكونا نفس الحجم)، و C(i,j) هو بكسل الصورة الأصلية و S(i,j) هو بكسل الصورة بعد الإخفاء.

2. نسبة الإشارة إلى الضجيج Peak Signal to Noise Ratio(PSNR) :

إن نسبة ذروة الإشارة إلى الضجيج في جميع أوساط النقل الرقمية يشير إلى مدى تداخل الضجيج مع الوسط الناقل سواء أكان صورة أو اشارة لاسلكية [12]، تُقاس نسبة الإشارة إلى الضجيج بالديسبل (db) وكلما اقتربت القيمة من الصفر كلما كان تداخل الضجيج في الإشارة الأصلية أكبر، و بالتالي تعتمد نتائج المقارنة على كبر قيمة الـ PSNR، تعطى علاقة الـ PSNR بالنسبة للصور الرقمية كما يلي [7]:

$$\mathrm{PSNR} = 10 \times \log\left(\frac{MAXi^2}{MSE}\right) \qquad (2)$$

حيث *MAXi* هي أكبر قيمة لونية يمكن أن يمتلكها بكسل الصورة الرقمية، و عند التعامل مع الصور التي يتم تمثيل البكسل فيها بقيم 8Bit فإن الـ *MAXi* تأخذ قيمة 255 ، و بشكل عام إذا حجزنا لكل بكسل عدد بتات مساوي للرقم b تكون عندها أكبر قيمة هي :$2^b - 1$

3. الترابط الطبيعي Normalization Correlation (NC) :

يعتبر معامل الارتباط أو الترابط الطبيعي مقياسا لمدى التشابه بين متغيرين مستقلين، يقيس هذا المعامل الفرق بين الصورة الأصلية و الصورة الناتجة عن عملية الإخفاء و يعطى بالعلاقة التالية [7]:

$$NC = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(C(i,j)\times S(i,j)\right) / \sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(C(i,j)\right)^2 \times \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(S(i,j)\right)^2} \qquad (3)$$

عملياً، كلما اقتربت قيمة الترابط الطبيعي من الـ 1 كلما كان الفرق بين الصورتين C و S قريب جداً و بالتالي لا يكون لخوارزمية الإخفاء الكثير من التأثير على المعطيات الرقمية للصورة.

تم استخدام لغة الماتلاب (Matlab) من أجل حساب المقادير السابقة، كذلك من أجل رسم مخططات تدرجات ألوان الصورة (Histogram) و التي يمكننا من خلالها تحليل الأثر المرئي الناتج عن تضمين الرسالة ضمن الصورة الرقمية.

أما بالنسبة للرسالة التي سيتم إخفائها ضمن الصورة فهي عبارة عن نص مكتوب باللغة الإنكليزية، و ذلك لأن لغة الماتلاب لا تدعم إدخال أي نص من قبل المستخدم إلا في اللغة الإنكليزية، يعطى هذا النص كما يلي:

Nowadays, the importance of information security is increasing according to the complexity of communication devises and their operating systems. Although of the safety that the encryption algorithms can provide between communication users, the encrypted messages may faces lot of attack types, which their purposes vandalism of data integrity such distorting or hiding some or all information, so it's better to hide information transform existing, even if the information are encrypted, and therefore the attacker will not know that there is a secret communication between communication users.

يتم احتساب الفراغات و علامات التنقيط عند ترميز الرسالة السابقة قبل تضمينها ضمن الصورة، وعادة يتم ترميز هذه المحارف باستخدام الترميز ASCII الذي يسند لكل محرف بايت واحد له تسلسل محدد كما هو محدد في جدول الترميز الخاص بترميز ASCII، وعلى سبيل المثال إذا كانت الرسالة السريّة هي : **E1** يكون التمثيل الست عشري لهذين المحرفين وفق ترميز ASCII هو **31 45** و بتحويل العددين السابقين إلى الصيغة الثنائية تكون الرسالة السرية وفق الشكل التالي :**0001 0011 0101 0100** ، وبعد ذلك يتم تطبيق خوارزمية الاخفاء على كل بت من بتات الرسالة السرية بشكل متتالي، أسلوب إخفاء و طريقة التعديل على الصورة المضيفة يختلف حسب خوارزمية الاخفاء المتبعة و هو ما سيتم توضيحه لاحقاً.

أما بالنسبة إلى الصورة التي سيتم اختيارها كملف مضيف فهي الصورة المبينة في الشكل(2)، ويجب أن نأخذ بعين الاعتبار أن الصورة لها اللاحقة (.png) وسنذكر السبب عند مناقشتنا للنتائج فيما بعد.

الشكل(2) الصورة المضيفة الحاملة للرسالة السريّة.

الإخفاء ضمن الصورة الرقميّة:

تهدف جميع خوارزميات الإخفاء ضمن الصورة الرقميّة إلى تضمين التمثيل الرقمي للرسالة ضمن الصورة دون أن تترك عمليّة التضمين أي أثر مرئي يمكن أن يسبب كشف وجود تعديل متعمد على الصورة قد يقود إلى مكان وجود الرسالة السريّة، و من ناحية أخرى يجب أن يكون الأثر الناتج عن عمليّة الإخفاء لا يقلل من جودة الصورة المضيفة الحاملة للرسالة، و يتم التأكد من أثر عمليّة الاخفاء على الصورة عن طريق استخدام بعض المعايير الرياضيّة التي ذكرت سابقاً، و بشكل عام يمكننا القيام بعملية الاخفاء ضمن الصورة ضمن المجالين الفراغي و الترددي.

1- الإخفاء في المجال الفراغي Spatial domain :

إن إحدى الطرق المهمة المستخدمة في الإخفاء ضمن الصورة هي الإخفاء ضمن المجال الفراغي (الفيزيائي)، ويقصد به المجال الذي تظهر به الصورة للعيان بمعنى آخر الشكل النهائي للصورة و الذي يعبر عنه بمجموعة من السويات اللونيّة، وعند قيامنا بعمليّة الإخفاء ضمن هذا المجال فإننا نقوم هنا بالتعديل على القيم الممثلة لهذه السويات.

إن تضمين الرسالة السرية ضمن هذا المجال يعتبر من أسهل الطرق المتبعة في عمليّة إخفاء البيانات، و عند تعاملنا مع الصور كوسط مضيف لحمل الرسالة السرية فإن التأثير الذي تتركه عمليّة تضمين البيانات ضمن هذا المجال يكون كالأثر الذي يتركه الضجيج المتداخل مع الإشارة (الصورة المضيفة) [3]، و الذي يقل تأثيره كلما كان التعديل الذي تركه الضجيج على السويات اللونية لم يكن ذو أهميّة ملحوظة إحصائية أو مرئية، و كميّة البيانات التي يمكن تضمينها ضمن هذا المجال تتعلق بشكل أساسي مع كميّة البتات التي يمكن تغييرها من الملف المضيف(الصورة) مع أقل تأثير ممكن، مع الأخذ بعين الاعتبار أن زيادة عدد البتات التي يتم تعديلها من الوسط المضيف قد يترك أثر مرئي أو إحصائي يسهل على المهاجم اكتشاف وجود رسالة سريّة.

إن الخوارزميّات الأكثر استخداما في المجال الفراغي للصورة هي الخوارزميّات التي تعتمد على تعديل البت الأقل أهميّة (LSb) من كل بكسل من بكسلات الصورة المضيفة أو أقل و ذلك حسب كبر الرسالة المراد تضمينها[6].

إن تغيير البت الأقل أهمية من بكسل الصورة لن يؤثر بشكل كبير على قيمة الكثافة اللونية لهذا البيكسل، و عملياً يعتبر تبديل قيمة هذا البت من 0 إلى 1 هي بمثابة إضافة العدد 1 إلى القيمة العشرية للبيكسل، و بالعكس عند تغيير قيمة هذا البت من 1 إلى 0 هي بمثابة طرح العدد 1 من القيمة العشرية لهذا البيكسل، عملية الاضافة او الطرح تكون حسب قيمة بت الرسالة السرية المراد اخفاءه، و يجب التنويه هنا بأن ليست جميع عمليات التضمين يمكن أن تغير من قيمة البيكسل و هذا يعود إلى حدوث تطابق بين قيمة البت الأقل أهميّة للبيكسل و بين قيمة البت المراد إخفاءه، فعلى سبيل المثال إذا أردنا إخفاء البت ذو القيمة 0 في البيكسل الذي يأخذ القيمة العشرية 132 فنلاحظ عند تحويل قيمة البيكسل إلى ثنائية، و هي (1111110000001**0**)، أن قيمة البت الأقل أهمية متطابقة مع قيمة البت المراد اخفاءه و بالتالي عملية الاخفاء هنا لن تغير من قيمة البيكسل.

و بشكل عام يمكن تلخيص عمل خوارزمية الاخفاء في المجال الفراغي للصورة باستخدام البت الأقل أهمية من قيم البكسلات و فق الخوارزمية الرياضية التالية:

Algorithm *Lsb_Hiding* **is**
Input : Secret message bit stream ***S***, Host Image ***M***
Output: Host Image ***M***
*(Note: **(i,j)** is the index of host image pixels, **k** is the index of secret message bits)*
For Each bit **In** the message *S* **Do**
If S(k) = 0 **Then**

If *M(i,j)* **Mod** 2 ≠ 0
M(i,j) ← *M(i,j)* -1
Else
M(i,j) ← *M(i,j)*
Else If S(k) = 1 **Then**
If *M(i,j)* **Mod** 2 = 0
M(i,j) ← *M(i,j)* + 1
Else
M(i,j) ← *M(i,j)*
Return *M*

يعبر ***M*** في الخوارزمية السابقة عن الصورة المضيفة المستخدمة لإخفاء بتات الرسالة السرية ***S***، ونلاحظ أن عملية الاخفاء ستستمر من أجل جميع بتات الرسالة السرية، و يتم اختبار قيمة البت المراد إخفاءه في كل تكرار و من ثم تعديل قيمة البيكسل حسب قيمة هذا البت و فق الأسلوب المشروح سابقاً، و يجري التأكد من قيمة البت الأقل أهمية من البيكسل المختار لعملية الاخفاء عن طريق حساب باقي القسمة على العدد 2 فإذا كانت قيمة باقي القسمة مساوي للـ 0 يكون البت الأقل أهمية له القيمة 0، أما إذا كان ناتج باقي القسمة لا يساوي الصفر يكون البت الأقل أهمية له القيمة 1، و يعبر عن عملية حساب باقي القسمة في الخوارزمية السابقة بالعملية ***Mod***، و عندما تكون قيمة البت الأقل أهمية مساوية لقيمة البت المراد إخفاءه لن يحدث تغيير في قيمة البيكسل لكننا نكون قد قمنا بعملية إخفاء حقيقية لبت الرسالة المختار، و يعبّر ***(i,j)*** عن دليل بيكسل الصورة المُختار لعملية الاخفاء، بينما يمثل ***k*** دليل بت الرسالة المراد اخفاءه.

و بشكل مشابه يمكننا تلخيص أسلوب استخلاص الرسالة السرية التي تم اخفاءها في الصورة المُضيفة وفق الخوارزمية التالية :

Algorithm *Msg_Extracting* **is**
Input : Host Image ***M***
Output: Secret message bit stream ***S***
(Note: ***(i,j)*** *is the index of host image pixels,* ***k*** *is the index of secret message bits)*
For Each chosen pixel **In** the : Host Image *M* **Do**
If M(*i,j*) **Mod** 2 = 0 **Then**
S(k) ← 0
Else If M(*i,j*) **Mod** 2 ≠ 0 **Then**
S(k)← 1
Return *S*

يتم إيجاد قيمة البت الذي تم اخفاءه عن طريق تطبيق عملية باقة القسمة على العدد 2 لكل بيكسل تم اختياره في عملية الاخفاء، و طالما ان قيمة باقي القسمة مساوي للـ 0 تكون قيمة البت المخفي 0، بينما حصولنا على باقي القسمة غير معدوم يعني أن قيمة البت الذي تم اخفاءه مساوي للـ 1، و يتم تكرار هذه العملية من أجل جميع بكسلات الصورة المختارة في خوارزمية الاخفاء.

2 الإخفاء في المجال الترددي Frequency Domain :

يمكن تمثيل الصورة رياضيّاً بعد تحويلها إلى مجال نقل آخر غير المجال الفراغي كالمجال الترددي، و يوجد العديد من التحويلات الرياضيّة التي تنقل الإشارة من مجالها الفراغي إلى المجال الترددي وعند التعامل مع الصور كإشارة متقطعة ثنائيّة البعد(أو ثلاثيّة البعد بالنسبة للصور الملونة) فإن تطبيقات و أهداف نقل الصورة إلى المجال

الترددي متعددة، كتطبيقات الفلترة وترميم الصور و إزالة الضجيج وتحليل الصورة، وفي تطبيقنا هنا سنحاول الاستفادة من نقل الصورة إلى مجال التردد من أجل توظيف خصائص الصورة ضمن هذا المجال للقيام بعمليّة إخفاء للبيانات السريّة في هذا المجال، وبشكل عام يوجد ثلاثة تحويلات للصورة تنقلها من المجال الفراغي إلى مجال التردد وهي كما يلي:

1. تحويل فوريه المتقطع (Discrete Fourier Transform (DFT :

في هذا التحويل يتم استخدام تحويل فوريه المتقطع DFT ذو البعدين لنقل الصورة من المجال الفراغي إلى المجال الترددي، و من ثم تضمين بتات الرسالة السريّة ضمن معاملات التحويل، و بشكل عام يستخدم هذا التحويل علاقات رياضيّة معقدة و تستنفذ مدة زمنيّة أكبر في العمل لذا كان التوجّه الأكبر نحو التحويل DCT .

2. تحويل التجيب المتقطع (Discrete Cosine Transform(DCT :

في هذا التحويل يتم استخدام تحويل التجيب المتقطع DCT من أجل نقل الصورة من المجال الفراغي إلى مجال التردد، و يعتبر من التحويلات الشهيرة الأكثر استخداماً خاصة أنّه يستخدم علاقات رياضيّة بسيطة ذات فترة تنفيذ قصيرة، كذلك فإن معاملات التحويل قليلة مما يجعله أكثر استخداماً في عمليات ضغط الصورة، و هو بشكل عام أكثر استخداماً من التحويل DFT .

3. تحويل المويجة المتقطّع (Discrete Wavelet Transform (DWT :يعمل هذا التحويل على نقل الصورة إلى المجال الترددي و من ثم عزل العناصر ذات التردد الصغير من العناصر ذات التردد الأكبر، بعد ذلك يمكننا تضمين بتات الرسالة ضمن العناصر ذات التردد الكبير، و بالمقارنة مع التحويل DCT فإن هذا التحويل يوفر مساحة أقل من تلك التي يوفرها التحويل DCT .

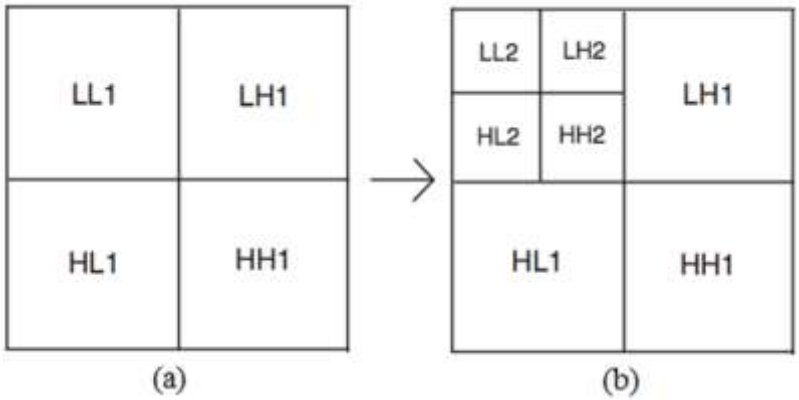
وبشكل عام فإنه يمكننا استخدام جميع التحويلات السابقة من أجل نقل الصورة إلى مجالها الترددي و من ثم تضمين الرسالة السريّة في هذا المجال و بعدها تطبيق عمليّة معاكسة للتحويل المستخدم من أجل العودة بالصورة(الحاملة للرسالة السريّة) إلى المجال الفراغي.

2-1 تحويل المويجة المتقطع (Discrete Wavelet Transform (DWT :

يعتبر تحويل المويجة المتقطع DWT من التحويلات القويّة و المستخدم بشكل واسع في معالجة الصورة الرقميّة، تتركز الفكرة الأساسيّة لهذا التحويل هي بتقسيم الصورة الأصليّة إلى أربعة اجزاء (LL1,LH1,HL1,HH1) بحيث يمثّل LL1 الجزء الحاوي على الترددات الدنيا أمّا الأجزاء المتبقيّة فتمثل الأجزاء الحاوية على الترددات العليا من الصورة الأصليّة لكن باتجاه أفقي(LH1) و شاقولي(HL1) و قطري(HH1)،كما هو مبين بالشكل(3)، ومن اجل تطبيق مستوى آخر من التحويل DWT يتم تطبيقه على الجزء LL1 فقط لنحصل على الأجزاء (LL2,LH2,HL2,HH2) وهكذا إذا أردنا الإكمال بمستوى ثالث من التحويل سنحصل على الأجزاء (LL3,LH3,HL3,HH3)، إن نقل الصورة إلى مجالات التردد هذه يتم باستخدام مرشحات التمرير [12] و من أشهر المرشحات المستخدمة هي مرشح Haar.

إن جميع الأجزاء السابقة من أجل جميع المستويات المستخدمة في التحويل تنتج صورة أخيرة تحتوي على ترددات الصورة الأصليّة، من التردد الأصغر و حتى التردد الأكبر الموجود في الصورة الأصليّة، وبما أن الصورة الأصليّة تحتوي على مجموعة من المناطق ذات التباينات العالية و المنخفضة فإن المناطق ذات التباينات المنخفضة تكون مناطق متصلة ببعضها البعض و تمتلك تقريباً نفس الكثافة اللونية [5]، و بعكسها تكون مناطق التباين العالي

تمثل تحولات في الكثافة اللونيّة للبكسلات كالحواف، و عند قيامنا بتحويل الـ DWT على الصورة فإن مناطق الحواف يتم تمثيلها في أجزاء التحويل ذات التردد العالي بينما الجزء الحاوي على الترددات المنخفضة تمثّل أغلب معلومات الصورة الأصليّة [11]، إن أهداف نقل الصورة باستخدام التحويل DWT متعددة في مجال معالجة الصورة كتحسين الصورة أو في عمليات ضغط الصورة أو ازالة الضجيج الداخل إلى الصور، إلا اننا هنا سنستغل أجزاء التحويل الحاوية على الترددات العالي في تضمين الرسائل السريّة فيها نظراً للتأثير الصغير الذي سينتج من التعديل في هذه الأجزاء طالما أنها تمثّل مناطق من الصورة ذات تباين عالي.



الشكل(3) تحويل المويجة المتقطع بمستوى وحيد(a)، مستويين (b).

تعطى علاقة تحويل المويجة المتقطع عند تعاملنا مع إشارة متقطعة $F(X)$ أحادية البعد بالعلاقات التالية[9]:

$$W_{\varphi}(j_0,k)=\frac{1}{\sqrt{M}}\sum_{x}F(x)\,\varphi_{j0,k}\,(x) \qquad (4)$$

$$W_{\psi}(j,k)=\frac{1}{\sqrt{M}}\sum_{x}F(x)\,\psi_{j,k}\,(x) \qquad (5)$$

حيث :

$W_{\varphi}(j_0,k)$ تحسب قيم معاملات التقريب.

$W_{\psi}(j,k)$ تحسب قيم معاملات التفاصيل.

$\varphi_{j0,K}$ و $\psi_{j,K}$ هي توابع ذات متحولات متقطعة.

بينما علاقة التحويل العكسي للتحويل السابق هي [9]:

$$F(x)=\frac{1}{\sqrt{M}}\sum_{k}W_{\varphi}(j_0,k)\varphi_{j0,K}\,(x)+\frac{1}{\sqrt{M}}\sum_{j=j0}^{\infty}\sum_{k}W_{\psi}(j,k)\,\psi_{j,K}\,(x) \qquad (6)$$

أما بالنسبة إلى الصور الرقميّة، و هي مجال بحثنا، فيمكننا اعتبارها إشارة متقطّعة ثنائية البعد، حتى بالنسبة إلى الصور الملونة التي تمثّل بمصفوفة ثلاثية الأبعاد يمكننا اعتبار كل بعد على أنه مصفوفة من المعلومات ثنائية البعد، و بالتالي عند تعاملنا مع الصور بالشكل السابق فإن تحويل المويجة المتقطع سيتم تطبيقه من أجل استخلاص المعاملات التقريبيّة من قيم الإشارة بشكل أفقي و بشكل عمودي، اما بالنسبة إلى معاملات التفاصيل يتم تطبيق التحويل بشكل أفقي لوحده ومن ثم بشكل عمودي لوحده و من ثم تطبيقه بالاتجاهين الأفقي و العمودي(السمات القطرية)، و بالنسبة إلى صورة ثنائية البعد لها الحجم $M\times N$ تكون علاقة التحويل و فق المعادلتين (7) و (8) [10]:

$$W_{\varphi}(j_0,k1,k2)=\frac{1}{\sqrt{M\times N}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}F(x,y)\,\varphi_{j0,k1,k2}\,(x,y) \qquad (7)$$

$$W_{\psi}^{i}(j,k1,k2)=\frac{1}{\sqrt{M\times N}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}F(x,y)\,\psi^{i}{}_{j0,k1,k2}\,(x,y) \qquad (8)$$

حيث i في المعادلة (8) تحدد الاتجاه الذي يتم فيه التحويل من اجل استخلاص معاملات التفاصيل (أفقي، عمودي، قطري).

اما بالنسبة إلى العلاقة الرياضيّة المستخدمة لاستخلاص الإشارة الأصليّة من العلاقتين السابقتين، و هي علاقة التحويل العكسي ثنائي البعد فتعطى بالعلاقة [10]:

$$F(x,y)=\frac{1}{\sqrt{M\times N}}\sum_{k1}\sum_{k2}W_{\varphi}(j_0,k1,k2)\varphi_{j0,k1,k2}\,(x,y)$$
$$+\frac{1}{\sqrt{M\times N}}\sum_{i}\sum_{j=0}^{\infty}\sum_{k1}\sum_{k2}W_{\psi}^{i}(j,k1,k2)\psi^{i}{}_{j0,k1,k2}\,(x,y) \qquad (9)$$

وكما ذكرنا سابقاً يمكننا تطبيق مستوى واحد من التحويل أو عدة مستويات، و هنا سنتعامل مع التحويل ذو المستوى الواحد للحصول على صورة أكثر وضوح و أكثر فهماً للقارئ و الشكل(4) يبين ناتج تحويل المويجة المتقطّع ثنائي البعد على الصورة الملونة المبينة في الشكل(2) .

الشكل(4) الصورة الأصليّة(a)، و تطبيق تحويل المويجة المتقطع بمستوى وحيد(b).

نلاحظ من الشكل(4) ناتج تحويل المويجة المتقطع DWT و المبينة في الجزء (b) من نفس الشكل، عمليّة إخفاء الرسالة السريّة يمكن أن تتم في أي جزء من أجزاء التحويل (LL,LH,HL,HH) إلا أن تضمين الرسالة السريّة في الأجزاء الحاوية على الترددات الأدنى للصورة يمكن أن يسبب تشوهات في الصورة الأصليّة عند استعادتها إلى المجال الفراغي، لذا ستنحصر خياراتنا في الأجزاء (LH,HL,HH)، وفي هذا البحث سنختار الجزء HH من أجل تضمين الرسالة السرية على اعتباره الجزء الحاوي على الترددات الأعلى للصورة المضيفة، و بالتالي عملية الإخفاء لن

تترك تأثير مرئي على الصورة الأصليّة كذلك الأمر بالنسبة إلى النتائج الإحصائية لقياس جودة الصورة ستكون ذات قيم أفضل إذا ما قارناها بالنتائج التي سنحصل عليها عند قيامنا بعمليّة الإخفاء في الأجزاء الأخرى من الصورة.

إن الآلية التي تم استخدامها من أجل القيام بعمليّة الإخفاء في المجال الترددي للصورة تختلف عن تلك المستخدمة في طريقة الإخفاء ضمن المجال الفراغي و السبب يعود إلى أن معاملات التفاصيل للتحويل DWT وهي المبينة في الأجزاء (LH,HL,HH) تمتلك قيم حقيقيّة و بالتالي لا يمكننا الاعتماد على طريقة الإخفاء باستخدام البتات الأقل أهميّة نظراً لوجود هامش خطأ عند قيامنا بكل تحويل DWT [4]، حتى وإن صغر هذا الخطأ قد يؤدي إلى تشوه الرسالة السريّة، و الطريقة الأفضل لتضمين الرسالة هي بإعطاء أوزان معينة لبتات الرسالة و تعديل معاملات التفاصيل في الجزء HH وفقاً لهذه الأوزان، و بدلاً من تعديل كامل الجزء HH وفقاً لبتات الرسالة السريّة نقوم فقط بتعديل المعاملات التي لا تمتلك قيم معدومة أي (0) و التي نراها في الجزء HH باللون الأسود بحيث نقوم بالتعديل على المعاملات التي تمتلك قيم مغايرة للصفر و التي تمثل معلومات الحواف، و عند استرجاع الصورة إلى مجالها الفراغي لن يكون هنالك تأثير مرئي للمراقب طالما أن التعديل قد تم على معلومات الحواف للصورة في مجالها الترددي.

وبفرض كان العدد (α) يمثل الوزن الذي سنمثل به بتات الرسالة السريّة ضمن معاملات الحواف القطرية (المغايرة للصفر)، و كان(β) يعبر عن بت الرسالة السريّة، يمكن تمثيل عمليّة الإخفاء ضمن معاملات الجزء HH رياضيّا بالعلاقة التالية:

$$HHi = \begin{cases} -1 \times |HHi| - \alpha, & \text{if } \beta = 0 \\ |HHi| + \alpha, & \text{if } \beta = 1 \end{cases} \qquad (10)$$

حيث $|$ ***HHi*** $|$ يعبر عن القيمة المطلقة لمعاملات الحواف، و بالتالي نستطيع استنتاج أن المعاملات السالبة هي الحاوية على البت ذو القيمة 0 من الرسالة السرية و المعاملات الموجبة هي الحاوية على البت ذو القيمة (1) من الرسالة السرية و بالتالي فإن علاقة استرجاع الرسالة الأصلية هي بتنفيذ عملية مقارنة على معاملات الجزء HH و مقارنتها مع العدد (0) وفق العلاقة التالية:

$$\beta = \begin{cases} 1, & \text{if} \quad HHi > 0 \\ 0, & \text{if} \quad HHi < 0 \end{cases} \qquad (11)$$

و الجدير بالذكر، ان قيمة الوزن (α) المعتبرة في هذا البحث هي 0.05 من أجل الصورة المبينة في الشكل(2).

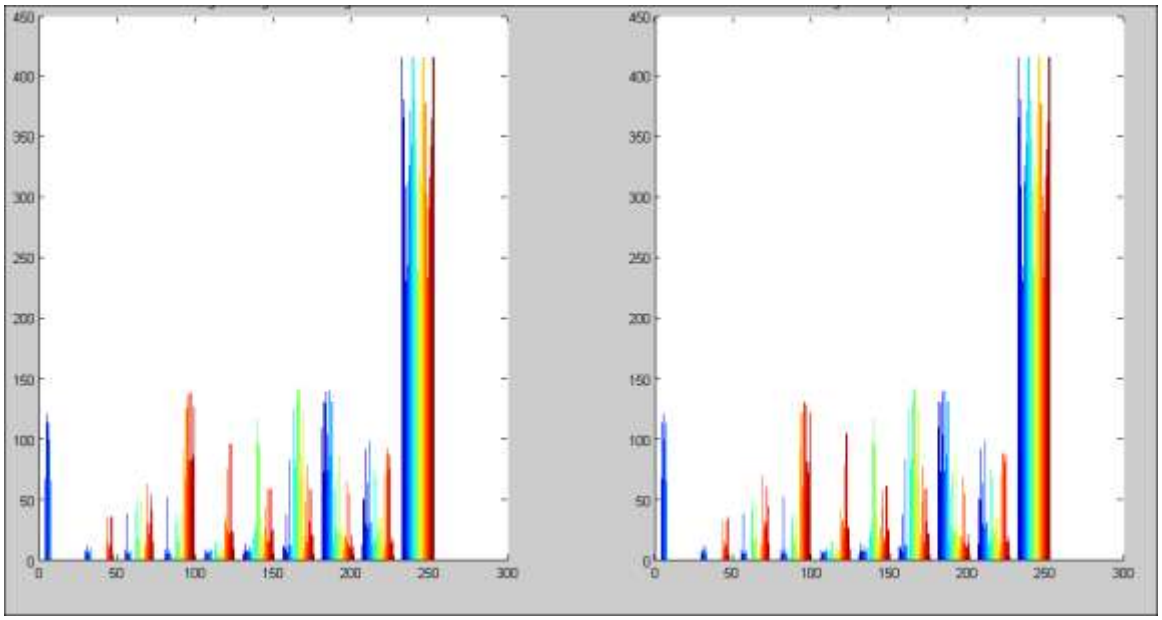
النتائج و المناقشة :

عند قيامنا بإخفاء الرسالة السرية ضمن الصورة المبينة في الشكل(2)، و باستخدام أسلوبي الإخفاء المشروحين في هذا البحث لم نلاحظ وجود تغيرات مرئيّة على الصورة الأصليّة يمكن أن تكشف وجود بيانات مخفية ضمن الصورة ، و الشكل(5) يبين الصورة الأصلية بعد تطبيق الإخفاء في المجال الفراغي باستخدام الخانات الأقل أهمية لبكسلات الصورة(LSB)، وفي المجال الترددي باستخدام تحويل المويجة المتقطع(DWT).

a b

الشكل(5) الصورة بعد إخفاء الرسالة، (a) باستخدام تقنية LSB،(b) باستخدام التحويل DWT.

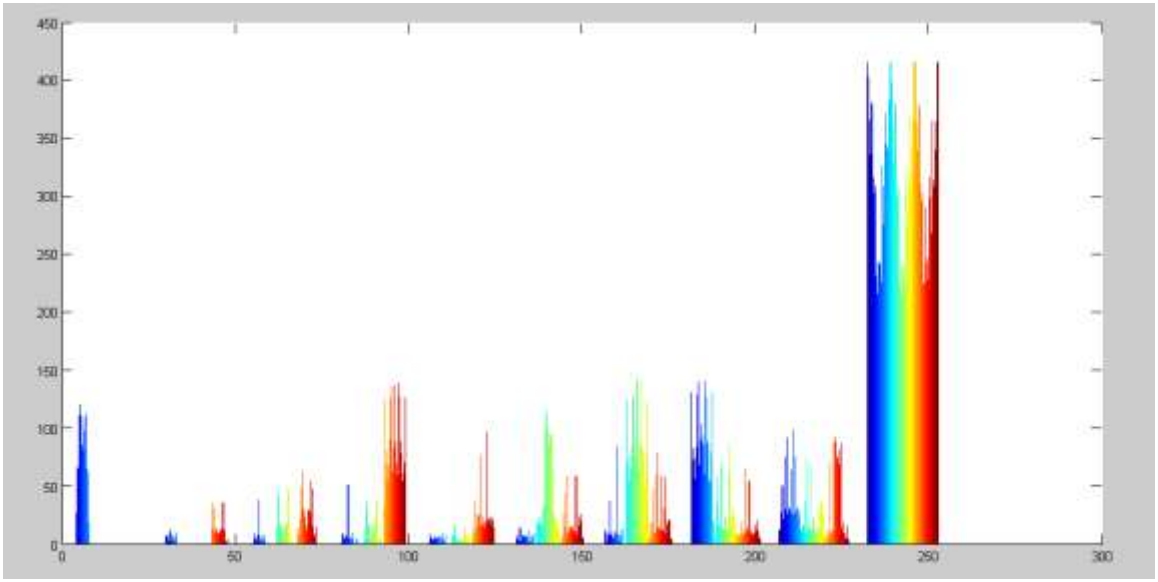
ونلاحظ من الشكل(5) وعند المقارنة مع الشكل(2) نرى انه لا مجال من المقارنة المرئية بين الصور قبل الإخفاء وبعده و بالتالي فإن اسلوبي الإخفاء لا يحققان تغييراً مهم على قيم السويات اللونية لبكسلات الصورة، اما بالنسبة إلى توزع السويات اللونية للصورتين بعد القيام بعملية الاخفاء فهو مبين في الشكل(6).



a b

الشكل(6) توزيع السويات اللونيّة للصورة بعد إخفاء الرسالة، (a) باستخدام تقنية LSB،(b) باستخدام التحويل DWT.

نلاحظ من الشكل السابق مدى التشابه بين مخططي الهستوغرام للصورتين بعد تطبيق الإخفاء، و الذي لا يختلف عن مخطط توزيع السويات اللونية للصورة الأساسية المبينة في الشكل(2)، و الشكل(7) يبين مخطط توزيع السويات اللونية للصورة الأساسية.



الشكل(7) مخطط توزيع السويات اللونية للصورة الأساسية.

أما بالنسبة إلى المقارنة الإحصائية لخوارزميتي الإخفاء، فسنعتمد على النتائج المستخلصة من العلاقات الرياضية(1) و (2) و (3)، و النتائج مبينة في الجدول(1).

الجدول (1) قيم معاملات الاختبار: MSE, PSNR, NC بالنسبة لأسلوبي الإخفاء : LSB وDWT .

خوارزمية الإخفاء	MSE	PSNR	NC
LSB	0.0016471	75.9637	1
DWT	0.1046	57.94	0.99997

نلاحظ من الجدول السابق أن تطبيق أسلوب الإخفاء في المجال الفراغي للصورة قد أعطى نتائج أفضل من تطبيقها في المجال الترددي، ويمكننا القول أن قيم كلا من المعاملين NC و MSE قد اقترب بشكل كبير من القيم المثالية عند استخدامنا لأسلوب الإحفاء باستخدام الخانات الأقل أهمية لبكسلات الصورة في المجال الفراغي و هو ما انعكس على قيمة PSNR وزادها بشكل أكبر بالمقارنة مع أسلوب الإخفاء في المجال الترددي باستخدام التحويل DWT.

و بالعودة إلى أسلوب الاخفاء المتبع في كلا الخوارزميتين تبدو النتائج المبينة في الجدول(1) منطقية، فعملية الاخفاء ضمن المجال الفراغي للصورة باستخدام البت الأقل أهمية لا تسبب تغيراً جزرياً في قيمة البيكسل بل يمكن أن لا تسبب أي تغير في حال تطابق قيمة البت المراد اخفاءه مع قيمة البت الأقل أهميّة من البيكسل المختار لعملية الاخفاء، بينما خوارزمية الاخفاء في المجال الترددي للصورة باستخدام التحويل DWT كانت باستخدام إضافة أوزان معينة إلى معاملات التفاصيل في الجزء *HHi* مع تعديل إشارة المعامل حسب قيمة البت المراد اخفاءه، و هذه العملية تم تطبيقها من أجل جميع بتات الرسالة المراد اخفاءها و بالتالي سيزداد أثر عملية التضمين بشكل أكبر من أثر تعديل البت الأقل أهمية لبكسلات الصورة، و بالمحصلة فإن كلا الخوارزميتين قدمتا نتائج مرئية جيدة كما هو مبين في الشكل(5) و الشكل(6) و لا يمكن تمييز وجود رسالة في الصورة بعد تطبيق عملية الاخفاء باستخدام الخوارزميتين.

الاستنتاجات و التوصيات :

من خلال تنفيذنا لعملية المقارنة بين أسلوبي الإخفاء، و بالنظر إلى النتائج الإحصائية المبينة في الجدول(1) يمكننا تحديد النتائج التالية:

1 - إن تطبيق أسلوب الإخفاء باستخدام تقنية الخانات الأقل أهمية لبكسلات الصورة في مجالها الفراغي يعطي نتائج إحصائية أفضل من أسلوب الإخفاء في المجال الترددي للصورة.

2 - قوة خوارزميّة الإخفاء في المجال الترددي باستخدام التحويل(DWT)، تكمن في عدم تأثر الرسالة السريّة لعمليات التعديل على الصورة كالتحكم بشدّة إضاءة الصورة (ضمن مجلات مسموح بها)، وعمليات الفلترة في المجال الفراغي و تعزيزها.

3 - خوارزميّة الإخفاء في المجال الفراغي للصورة باستخدام الخانات الأقل أهمية للبكسلات حساسة جدا لأي تعديل يطرأ على الصورة.

4 - يمكن اقتراح أسلوب عشوائي خلال تضمين بتات الرسالة السريّة عبر استخدام مفتاح مشترك و متفق عليه من قبل أطراف التراسل، كذلك يمكننا زيادة مستوى السريّة عبر تشفير بتات الرسالة باستخدام إحدى خوارزميات التشفير.

5 - النقطة الأهم هي أن صيغ الصور المتبعة يجب أن تكون تلك الصيغ التي لا تدعم ضغط الصورة أو على الأقل تدعم وجود ضغط لكن بنسب مسموح بها، بحيث أن أي عملية ضغط للصورة يمكن أن يؤدي إلى فقدان البيانات التي تم تضمينها سواء في المجال الفراغي أو الترددي للصورة الرقمية.

6 - يمكننا زيادة قوة خوارزميّة الإخفاء في المجال الترددي باستخدام التحويل DWT ضد عمليات ضغط الصورة باستخدام أكثر من تحويل ضمن المجال الترددي للصورة، بعض الأساليب المقترحة كأنت بتطبيق التحويل DCT على الجزء HH الناتج عن التحويل DWT و من ثم القيام بعملية الاخفاء ضمن معاملات التردد العليا.

المراجع

1. CHEDDAD,A ; CONDELL,J ; CURRAN,K ; MCKEVITT,P. *Digital Image Steganography: Survey and Analysis of Current Methods.* Signal Processing, Northern Ireland- United Kingdom, Volume 90, 2010, *727-752.*

2. HELAL,B. *A Modified Method of Information Hiding Based on Hybrid Encryption and Steganography*, IJCCCE, Vol.12, No.1, 2012.

3. SRAVANTHI,G.S; DEVI,B; RIYAZODDIN, S.M; REDDY, M. *A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method* . Global Journal of Computer Science and Technology Graphics & Vision,USA, 2012.

4. BHATTACHARYYA,S; SANYAL,G. *A Robust Image Steganography using DWT Difference Modulation (DWTDM),I. J. Computer Network and Information Security*,Vol 7,2012, 27-40.

5. MOHAMMED,S.A ; HASSAN,A .S ; HASHIM ,M.D. *wavelet transformation domain for sub image hiding based on the discrete wavelet transformdomain,* Al-Qadisiya Journal For Engineering Sciences, Vol. 5, No. 2, 166-184, 2012.

6. GOEL,S; RANA, A;KAUR,M. *A Review of Comparison Techniques of Image Steganography, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 6, Issue 1 (May. - Jun. 2013), 41-48.*

7. متراس، بان أحمد حسن ; عبو، أديبة خالد. *الإخفاء ضمن سلسلة(DNA) باستخدام مفتاح سري يعد بزرة (seed) لمولد أرقام عشوائية* ، المجلة العراقية للعلوم الإحصائيّة، العراق، العدد الخامس و العشرون، 2013، 430-440.

8. محمد، نادية معن. *الإخفاء الفوضوي للصور باستخدام DCT & DWT*، مجلة الرافدين لعلوم الحاسوب و الرياضيات، العراق- جامعة الموصل، المجلد(10)، العدد(3)،2013، 61-73.

9. ZAGADE,S; BHOSALE, S. *Secret Data Hiding in Images by using DWT Technique's*, International Journal of Engineering and Advanced Technology (IJEAT), Vol-3, Issue-5, June 2014.

10. PRABAKARAN,G; BHAVANI, R; SANKARAN, S; *Dual Wavelet Transform in Color ImageSteganography Method*, IEEEInternational Conference on Electronics and Communication System,2014.

11. PARUL; MANJU; ROHIL,H. *Optimized Image Steganography using Discrete Wavelet Transform (DWT)* . International Journal of Recent Development in Engineering and Technology, Haryana (India), 2014.

12. ABU,N.A; ADI,P.W; MOHD,O.*Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform*, International Journal of Video&Image Processing and Network Security ,VOL:14 No:02,2014.

13. Bhavisha,T; JOSHI,D, *survey on different steganography techniques*, international journal of engineering sciences & research technology, India, 2015.