الإخفاء باعتماد الخوارزميات المتوازية

نغم ثروت سعيد

قسم علوم الحاسوب / كلية التربية

جامعة الموصل

الاستلام	القبول
٢٦ / ٠٩ / ٢٠١٠	١٥ / ٠٩ / ٢٠١١

Abstract

In this research a simulation parallel algorithm for data hiding and data retrieval in gray digital image files were used.

A simulation for this algorithm was applied on star network type. The secret image and the covered image was segment in equal number of parts (four parts) then was applying the suggested algorithm on each part in synchronized form using Matlab Parallel Processing Tools.

The proposed algorithm was applied to retrieve the secret image from the covered one in synchronized form too. Measurement of time needed by the algorithm was compared with one used serial algorithm for hiding and retrieving by using substitution techniques.

The proposed algorithm shows higher performance than the serial type in consuming time.

الملخص

تم في هذا البحث محاكاة لخوارزمية متوازية لإخفاء واسترجاع البيانات في ملف صوري رمادي اللون تم بناء محاكاة لهذه الخ وارزمية على شبكة معالجات بشكل (Star Network) وتم تقطيع كل من صورة الإخفاء وصورة الغطاء إلى عدد متساوي من الأجزاء (أربعة أجزاء) وتنفيذ الخوارزمية المقترحة على كل جزء من هذه الأجزاء بشكل متزامن باستخدام Matlab Parallel Processing Tools.

تم تنفيذ الخوارزمية المقترحة لاسترجاع الصورة المخفية من صورة الغطاء بشكل متزامن أيضا وقياس الوقت المستغرق لهذه الخوارزمية ومقارنته بالوقت المستغرق على خوارزمية متسلسلة ولكل من خوارزمية الإخفاء والاسترجاع وتم استخدام تقنية الإبدال في عملية الإخفاء والاسترجاع ، أظهرت الخوارزمية المقترحة كفاءة أفضل من الخوارزمية المتسلسلة من حيث الوقت المستغرق.

١- المقدمة:

ان امن الحاسوب يلعب دورا مهما في حماية مواردنا الاستراتيجية المهمة وهي المعلومات . واحدة من افضل الطرائق في حماية انظمة الحاسوب هي استخدام تقنية التشفير . حيث انه يركز اساسياً على المعلومات ووثوقيتها وتوافقها ومصدر مصداقيتها، في حين ان خوارزميات التشفير توفر مستوى عالي من الحماية لأنظمة الحاسوب.

في الوقت الحالي يوجد العديد من خوارزميات التشفير المستخدمة لدعم انظمة الحاسوب بمختلف انواع الحماية لكن الهيكل العام لخوارزميات التشفير متسلسلة بخطواتها في الية معالجة البيانات، بينما المعالجة المتوازية لاستخدام تقنية المعالجات المتعددة اصبحت شائعة لذلك يوجد فرق واضح بين خوارزميات التشفير المتسلسلة ومستقبل الحاسوب التي تحوي اكثر من معالج داخلي

يقترح البحث تقليل الفرق بين المعالجات المتعدد ة ذات الكفاءة العالية وخوارزميات التشفير الحالية ذات الهيكل المتسلسل عن طريق تسليط الضوء على الاستخدام الامثل من المعالجات المتعددة. عليه تم كتابة خوارزمية متسلسلة تعمل على اكثر من معالج يعملون بشكل متزامن وبصورة متوازية.

٢- البرمجة المتوازية: Parallel Programming

هي ايجاد نمو ذج متوازي يتكون من عدد من حاسوب Von Neuman ويكون عام لكثير من تطبيقات الحاسوب المتوازي يمتلك ميّزتين اساسيتين هما (البساطة والواقعية)، البساطة تعني امكانية معالجة الحاسوب للبيانات والبرمجة لها ، والواقعية هي ضمان تنفيذ النماذج البرم جية لها بكفاءة معقولة على حاسوب واقعية وفي ما يلي بعض المفاهيم الخاصة بالبرمجة المتوازية .[1]

٢-١ التوازي: Parallelism

هو مجموعة من المعالجات التي بإمكانها العمل بصورة متوازية او تعاونية (cooperatively) لحل مسالة حسابية ما، ويعد التوازي في بعض الاحيان منطقة غريبة ونادرة للبرمجة لكنها مثيرة لاهتمام عدد غير قليل من المبرمجين وبخاصة في دراسات التطبيقات ومعمارية الحاسوب والشبكات فأصبح التوازي واسع الانتشار وأصبحت البرمجة المتوازية اساسا للتقدم العلمي والبرمجي.[7]

٢-٢ الخوارزمية المتوازية: Parallel Algorithm

يقصد بالخوارزمية المتوازية عبارة عن مجموعة من المهام (Tasks) والتي يمكن تنفيذها بوقت واحد وبشكل متوازي . كل مهمة (Sub Task) بواسطة معالج متسلسل (Sequentially) لتعطي ناتجا كاملا لها ثم تجمع هذه الحلول من المهام جميعها لتعطي الحل والناتج الرئيسي للخوارزمية المتوازية .[4]

٢-٣ تصنيف الحاسوب المتوازية : Parallel Computer Classification

ان الحاسوب سواءً كانت تسلسلية أم متوازية تعمل على تنفيذ مجموعة من الايعازات على مجموعة من البيانات التي تمثل ادخال الخوارزمية والتي تستخدم في عمل الايعازات وبالاعتماد على هذه المجاميع من الايعازات والبيانات تصّنف الحاسوب الى اربعة انواع: [١٤]

حاسوب **SISD** : يحوي حاسوب هذا الصنف على وحدة معالجة واحدة بحيث تستقبل ايعازاً واحداً وتقوم بتنفيذه على معلومة واحدة، وهو النوع الذي يطلق عليه بالحاسوب التسلسلية (Sequential).

حاسوب **MISD** : ان هذا الصنف من الحاسوب هناك عدد من المعالجات وكل معالج له وحدة سيطرة خاصة به عن طريقها تقوم المعالجات باستلام مجاميع من الايعازات وجميع هذه المعالجات لها وحدة ذاكرة مشتركة أي جعل المعالجات تقوم بتنفيذ ايعازات مختلفة وبالوقت نفسه على المعلومة نفسها.

حاسوب **SIMD** : تحتوي هذه الحاسوب على عدد من المعالجات وكل واحدة من هذه المعالجات تعمل على الجزء الداخلي للذاكرة الخاص به (الذاكرة المحلية Local Memory) وهو مكان خزن كل من البرامج والبيانات، كل هذه المعالجات تعمل على نفس الايعاز الصادر من وحدة السيطرة المركزية وتعمل هذه المعالجات بصورة متوازية بتنفيذ نفس الايعاز على بيانات مختلفة.

حاسوب **MIMD** : يعد هذا النوع من الحاسوب اكثر شيوعا وكفاءة وقوة في تنفيذ التطبيقات العامة (General Purpose) في موضوع الحاسوب المتوازية، اذ تكون فيها مجموعة الايعازات ومجموعة البيانات مختلفة.

وان هناك عدة اشكال وأساليب لربط المعالجات المستخدمة في الحاسوب المتوازية:

١. الربط المتكامل (Fully Connected): ان كل معالج مرتبط مع باقي المعالجات ربطا متكاملاً.
٢. شبكة قناة نقل (Bus Network): ان جميع المعالجات ترتبط بقناة (ناقل) واحدة فقط.
٣. الشبكة الحلقية (Ring Network): ان جميع المعالجات ترتبط ربطاً حلقياً.
٤. الشبكة النجمية (Star Network): يتم من خلالها ربط جميع المعالجات بمعالج مركزي وسطي.
٥. مصفوفة خطية (Linear Array): ترتبط جميع المعالجات ربطاً خطياً.
٦. شبكة مصفوفة حلقية (Ring Array Network): يتم ربط المعالجات بشكل حلقي مستطيل.

٢-٤ مقاييس تقييم الخوارزمية المتوازية:Parallel Algorithm Measurements

عند صياغة خوارزمية جديدة للحاسوب المتوازي يجب الاخذ بنظر الاعتبار مقاييس التقييم لهذه الخوارزمية[1]، وهذه المقاييس تشمل:

١- وقت التنفيذ (Running Time):

بما ان عملية تسريع التنفيذ لمختلف التطبيقات هو الغرض الرئيسي لبناء الحاسوب المتوازي، فان أهم مقياس لتقييم الخوارزمية المتوازية هو وقت التنفيذ وهو الوقت الذي تستغرقه الخوارزمية منذ لحظة ابتداءها بالعمل الى لحظة انتهاءها وتوقفها، وفي حالة كون المعالجات لا تبدأ او تنتهي في الوقت نفسه فان وقت التنفيذ يساوي الوقت المستغرق لبدء أول معالج بالعمل ولغاية توقف أخر معالج عن العمل.

٢- عدد الخطوات (Counting Steps):

وهي عملية حساب عدد العمليات او الخطوات (Operation or Steps) التي يتم تنفيذها بواسطة الخوارزمية بأسوأ حالاتها . ففي الحا سوب الاعتيادي وحاسوب SISD يقاس وقت التنفيذ بعدد من وحدات الوقت تدعى (Cycle) بينما في باقي الانواع من الحاسوب المتوازي فيقاس عدد خطوات التنفيذ بمقياسين هما الخطوات الحسابية

(Computational Steps) وعدد الخطوات التي يتم فيها نقل البيانات من معالج الى اخر من خلا ل ذاكرة مشتركة او شبكة ربط وهذا ما يدعى بـ (routing steps).[١٤]

٣- التسريع (Speed Up):

ان مقياس التسريع للخوارزمية المتوازية M والتي هي تطوير عن خوارزمية متسلسلة MI باستخدام P من المعالجات لتنفيذ M هو

$$SP= \frac{TP}{TS} \quad \ldots\ldots\ldots (1)$$

حيث Sp تمثل التسريع، Tp وقت التنفيذ لM باستخدام p من المعالجات، M خوارزمية متوازية. وان Ts وقت التنفيذ لMi باستخدام معالج واحد وان Mi تمثل خوارزمية متسلسلة.

٤- عدد المعالجات (Number of Processors):

ان ثاني اهم مقياس لتقييم الخوارزمية هو عدد المعالجات المستخدمة في حل هذه الخوارزمية . فكلما زاد عدد المعالجات المستخدمة زادت الكلفة المالية للحصول على النتائج أي بمعنى الزيادة في الكلفة لأسعار المعالجات المستخدمة والكلفة لصيانتها والكل فة الزمنية للتنفيذ . فان عدد المعالجات المطلوبة لحل مسألة ما باستخدام خوارزمية متوازية هو دالة لـ n يرمز لها بـ p(n). [١]

٥- الكلفة (Cost):

تعرف كلفة الخوارزمية المتوازية بانها حاصل ضرب المقياسين السابقين:

الكلفة = وقت التنفيذ × عدد المعالجات

أي ان الكلفة هي عدد الخطوات المنفذة من قبل جميع المعالجات المستخدمة في حل مسالة معينة ذات حجم n فتكون كلفة التنفيذ هي[4] [14].

$$C(n) = p(n) \times t(n) \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

حيث (P) تمثل عدد المعالجات ، (T) تمثل وقت التنفيذ

٣- الاخفاء:Information Hiding

إن إخفاء المعلومات يعني إخفـاء معلومات في معلومات أخرى ظاهرها لا يدعو إلى الشك ولا يلفت الانتباه، وتكون غير مدركة من قبل المتطفلين والمهاجمين، ولذلك لن تكون المعلومات

مشاعة لمستخدمي الشبكة، بل يبقى محتواها حكرا على الجهات ذات العلاقة، والتي تكون على دراية بكيفية استخراج هذا المحتوى.[3]

إن الغاية من إخفاء المعلومات ليست منع الآخرين من معرفة المعلومات المخفية فقط، بل لإزالة الشك أصلا في وجود معلومات مخفية، والشيء المميز في تقنيات إخفاء المعلومات أنها تواكب التقنيات الحديثة، ويمكن استخدامها في جميع الوسائط الحاسوبية من صور، نصوص، صوت، فيديو وحزم الشبكة.

ان تزايد تطبيقات التعامل مع الوسائط المتعددة ومحتويات الشبكة العالمية خلال السنوات الأخيرة جعل الكتابة المغطاة تتصدر تقنيات الأمنية والاتصال السري . لذلك كان لابد من ظهور وسائل تعمل على توفير امن لهذ هالوسائط لحمايتها من السراق والمتطفلين من العبث بها وتحريفها أو سرقتها و نشر المعلومات الحساسة منها . ومن هنا ظهرت الحاجة إلى توفير وسائل أمنية البيانات، ومن هذه الوسائل علم التشفير Cryptography لكن مع ازدياد شبكات التناقل وشبكة المعلومات العالمية Internet أصبح من الصعب المحافظة على هذه البيانات ، ولاسيما انها تكون دائما في متناول الجميع عبر شبكة الانترنت في صيغة غير واضحة تبعث على الشك والاهتمام لدى المتطفل والسارق لفتح هذا التشفير أو تدمير المعلومات المرسلة . لذلك كان لابد من تطوير أمنية البيانات وإنشاء تقنيات ووسائل جديدة، ومن هنا ظهر علم إخفاء المعلومات Information Hiding.[2]

3-1 إخفاء البيانات داخل الصورة Hiding Data in Image

تمثل الصورة داخل الحاسوب كمصفوفة من قيم شدة الإضاءة، وتصف شدة الإضاءة نقطة ضوئية على الشاشة pixel، ومن الممكن تمثيل كل نقطة ضوئية اما باستخدام خلية ثنائية واحدة (1bit)، او تمثيلها باستخدام كتلة ثمانية واحدة 1Byte (8bits)، او تمثيلها باستخدام ثلاث كتل ثمانية 3Bytes (٢٤bits).

وفي التمثيل (24bits) تمثل شدة الاضاءة شدة لون من الالوان الرئيسة الثلاثة الاحمر R والأخضر G والأزرق B، وبدمج شدة الاضاءات الثلاث يتم تشكيل اللون المطلوب(RGB) وبذلك يتم توفير ١٦٧٧٧٢١٦ ($٢^{٢٤}$) لون، وان النسب اللونية الثلاث تمثل اللون الحقيقي لنقطة ضوئية على الشاشة ولذلك يسمى هذا التمثيل تمثيل اللون الحقيقي True color.

وقيم مصفوفة الصورة في التمثيل باستخدام كتلة ثمانية واحدة لا تمثل قيم اللون الحقيقي وإنما تمثل مدخلا لعنوان موقع في لوحة الالوان Palatte الموجودة في ترويسة ملف الصورة، ولذلك يسمى هذا التمثيل تمثيل اللون المزيف Pseudo color، وعدد المداخل في لوحة الالوان هو ٢٥٦

مدخلا وبذلك توفر ٢٥٦ ($٢^٨$) لونا في هذا التمثيل، وان تنظيم لوحة الالوان في الصور الم لونة في هذا التمثيل لا يعتمد على تسلسل التدرجات اللونية بشكل منتظم، اما في الصور الرمادية فتنظيم لوحة الالوان يكون منتظما وذا تدرجات رمادية منتظمة.[٧]

٣-١-١ تقنيات الإبدال Substitution Techniques

أن أجراء تغيير طفيف في أجزاء الوسائط المتعددة يكون غير مدرك من قبل وسائل الإنسان الحسية كالسمع والبصر، لذلك يستفاد من خاصية عدم الإدراك هذه لإخفاء البيانات في الوسائط المتعددة وذلك بتبديل اجزاء من بيانات هذه الوسائط مع البيانات المراد إخفاؤها، وكذلك يستفاد من الاماكن غير المستخدمة من هذه الوسائط لإخفاء الرسالة السرية.[٨]

أ- إبدال الخلية الثنائية الأقل أهمية: Least Significant Bit

تعد تقنيات الإبدال في الخلية الثنائية الأقل أهمية من تقنيات الإخفاء الشائعة الاستخدام وواسعة الانتشار وذلك لسهولة تطبيقها، وتمتاز هذه التقنيات بقدرة عالية على الإخفاء (شفافية) وسعة خزن كبيرة، حيث يمكن إخفاء كمية كبيرة من المعلومات مع تأثير قليل في الغطاء. [٣]
وعند تطبيق تقنية LSB على غطاء من نوع صورة، فأن الخلية الثنائية الأقل أهمية لبعض أو جميع بيانات هذه الصورة تبدل بخلية ثنائية واحدة من الخلايا الثنائية لرسالة السرية، عندما تكون ا لصورة الملونة ذات تمثيل ٢٤ خلية ثنائية فأنه يمكن إخفاء خلية ثنائية في اللون الأحمر وخلية ثنائية في اللون الأخضر وخلية ثنائية في اللون الأزرق، أي ان النقطة الضوئية (pixel) الواحدة تخفي ٣ خلايا ثنائية من الرسالة السرية . مثلا في صورة ذات حجم (٨٠٠×٦٠٠) يمكن إخفاء (Bits ١.٤٤٠.٠٠٠ = ٣×٦٠٠×٨٠٠) أو (١٨٠.٠٠٠ Bytes) من الرسالة السرية.
لنفترض ان لدينا ثلاث نقاط ضوئية من صورة ملونة ذات تمثيل ٢٤ خلية ثنائية تمثيلها الثنائي بدءاً من اليسار هو:

	ازرق	اخضر	احمر
النقطة الضوئية الأولى	11001000	11101001	00100111
النقطة الضوئية الثانية	11101001	11001000	00100111
النقطة الضوئية الثالثة	11101001	00100111	11001000

عندما يضمن العدد 198 ذو التمثيل الثنائي ١١٠٠٠١١٠ في الخلية الثنائية الأ قل أهمية في النقاط الضوئية السابقة تكون النتيجة:

	ازرق	اخضر	احمر
النقطة الضوئية الأولى	1100100**0**	1110100**1**	0010011**1**
النقطة الضوئية الثانية	1110100**1**	1100100**0**	0010011**0**
النقطة الضوئية الثالثة	1110100**1**	0010011**0**	1100100**1**

إن الخلايا الثنائية التي تحتها خط هي الخلايا الوحيدة التي تغيرت في الحقيقة النقاط الضوئية التي استخدمت في عملية الإخفاء. والفائدة الرئيسة لتقنية LSB هي إخفاء كمية كبيرة نسبيا من المعلومات من غير ملاحظة تغيير ملحوظ في الغطاء .[13] [٢]

ب- الفراغ غير المستخدم او المحجوز في أنظمة الحاسوب:

يُستفاد من هذا الفراغ في إخفاء معلومات سرية ، مثال ذلك الطريقة التي يخزن بها نظام التشغيل الملفات على القرص الصلب فأنه ينتج فراغاً غير مستخدم، هذا الفراغ يكون مخصصاً للملفات المخزونة، ويسمى هذا الفراغ الناتج من عملية الخزن بالفراغ المهمل slack space، ومن التقنيات الأخرى استخدام المناطق المحجوزة في بادئة الملفات Files Header كملفات الصورة والصوت، وتعد هذه التقنيات غير كفوءة لصغر حجم هذه الفراغات وسهولة كشفها.[١١]

٤- الخوارزمية المتوازية المقترحة: Proposed Parallel Algorithm

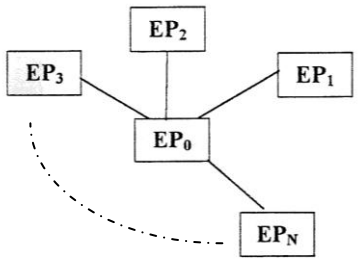
بعد توضيح بعض خوارزميات الاخفاء والاسترجاع تظهر الحاجة الضرورية لإيجاد طريقة برمجية جديدة تقلل من وقت حل هذه الخوارزميات وتوجد الحل بوقت مجدي واقتصادي، لهذا تم استخدام البرمجة المتوازية لهذا الغرض والتي تقوم على اساس عمل معالجات عدة في وقت واحد ومتزامن في حل تفرعات المسالة الرئيسة لغرض الخروج بالحل الامثل وبوقت قصير ومرضي، ويطلق على كل معالج من هذه المعالجات بعنصر معالجة (Processor element) ويرمز له PE.

٤-١ اسلوب ربط المعالجات: The connection of processors

تم استخدام ربط المعالجات بشكل (Star network) لغرض توزيع اجزاء الصور ولكل من صورة الغطاء والصورة السرية على المعالجات المرتبطة بالمعالج الرئيسي المركزي . ويتكون هذا الربط من المعالج المركزي (PE_0) والذي يقوم مقام المعالج الاساسي (master PE) لغرض قراءة كل من الصورتين من الذاكرة الرئيسية، وتقوم باقي المعالجات المرتبطة بالمعالج المركزي مقام

المعالجات المساعدة له، ويمكن تسميتها (PEs Slave) اذ يكون تسلسل هذه المعالجات بالتسلسل i، حيث ان: i= 1,2,….n

يحتوي كل PEi على ذاكرة محلية يخزن فيها برنامج الاخفاء وب رنامج الارجاع لكلا الصورتين المستلمة من المعالج الرئيسي PE0 كما في الشكل (١)



شكل (١): يوضح طريقة ربط المعالجات باستخدام اسلوب Star Networks

٤-٢ عدد المعالجات المستخدمة: Number of Processors

بعد قراءة كلا الصورتين من قبل المعالج المركزي PE_0 من الذ اكرة الرئيسية يبدأ بأول عملية تقسيم للصور (سرية وغطاء) إلى صور جزئية بعدد n من الصور ويقوم بإرسالها إلى المعالجات الأخرى PEi.

اذا كان عدد المعالجات المرتبطة بالمعالج الرئيسي بعدد n.

اذن يكون عدد المعالجات الكلية المستخدمة هو (n+1).

٤-٣ خطوات تنفيذ الخوارزمية المتوازية: Parallel Algorithm Steps

- يبدأ EP_0 بتقسيم كلا الصورتين الى n من الأجزاء وإرسال كل جزء إلى معالج فرعي PE_j. وذلك من خلال استخدام مخازن وسطية (Buffers)
- يستلم كل PE_j جزءهُ المخصص من المعالج الرئيسي ويقوم بما يلي:
  - يبدأ كل معالج PE_j بتطبيق خوارزمية الاخفاء او الاسترجاع على جزء الصورة المستلم.
  - ارجاع الصورة النهائية بعد عملية الاخفاء او ارجاع الصورة المخفية بعد عملية الاسترجاع.
- يقوم المعالج PE_0 بتجميع أجزاء الصور المستلمة من جميع المعالجات PEj.

- عرض الصورة النهائية فيما اذا كانت صورة غطاء بعد عملية الاخفاء او الصورة السرية بعد عملية الاسترجاع.

ان جلّ ما يهمنا من استخدام خوارزمية متوازية في حل تقنية الاخفاء هو الوقت المستغرق لها لحين الحصول على الصورة النهائية جراء عملية الاخفاء او الاسترجاع. ولكي يمكننا الحكم على الخوارزمية بأنها جيدة فانه يجب ان يكون الوقت المستغرق في حل المسالة باستخدام خوارزمية متوازية اقل من الوقت المستغرق في حلها باستخدام خوارزمية اعتيادية.

يستغرق المعالج المركزي PE_0 وقت مقداره C1 جراء عملية قراءة الصورتين الرئيسة من الذاكرة ومن ثم تقسيمها الى n من الاجزاء وتوزيعها على المعالجات الاخرى . بينما يستغرق تطبيق خوارزمية الاخفاء او الاسترجاع لدى كل PE_j وقتا مقداره C2 ومن ثم ارسال الصورة الناتجة ثانية الى المعالج PE_0، والذي يقوم بدوره بدمج جميع الأجزاء المستلمة واستخراج الصورة النهائية بوقت مقداره C3 اذن سيكون وقت تنفيذ الخوارزمية المتوازية هو:

$$t(n) = C1 + C2 + C3 \quad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

وبما ان C3, C1 هو الوقت المستغرق على المعالج PE_0 لذا فانه يمكن كتابة هذا الوقت بالشكل الاتي:

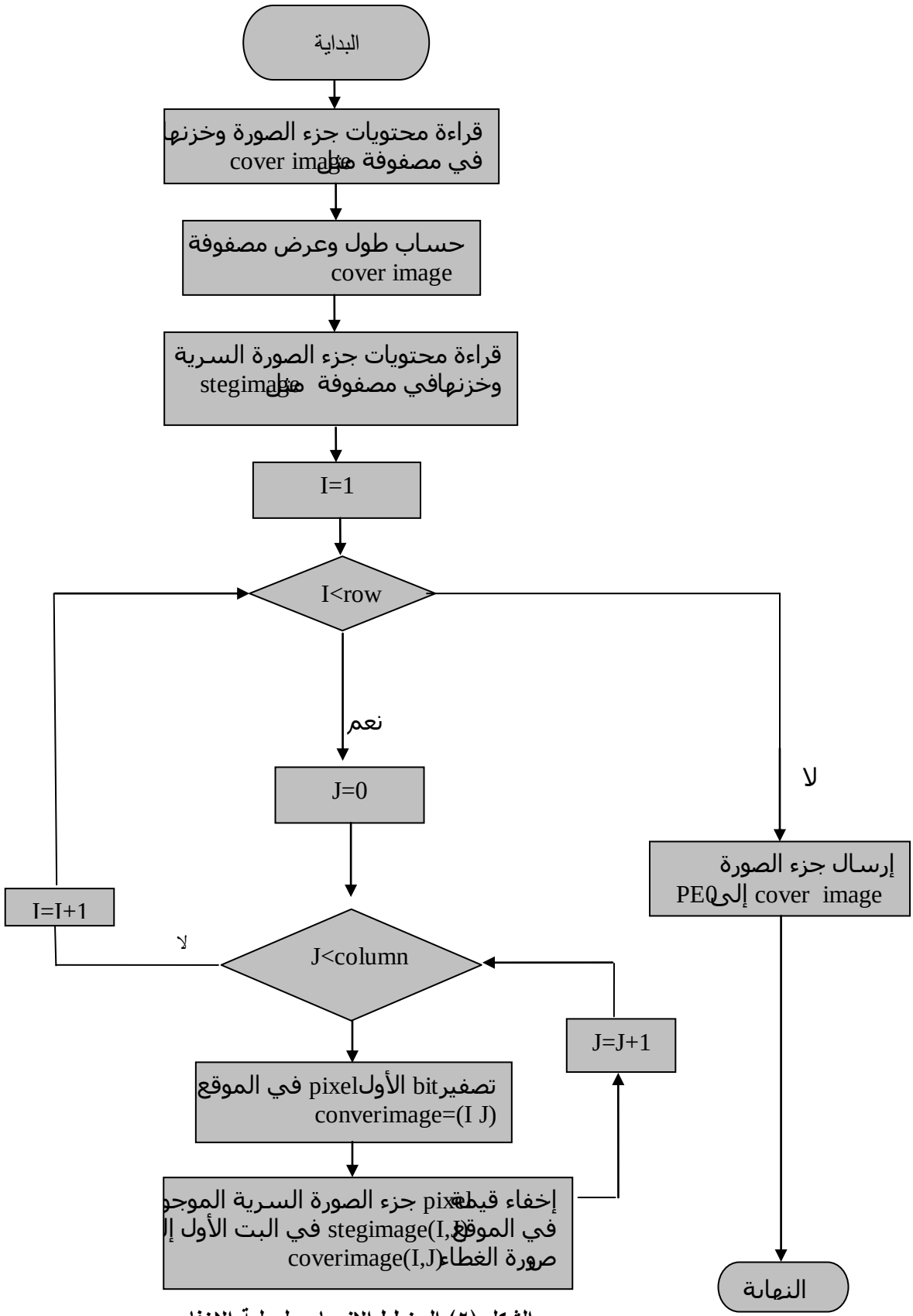
$$C = C1 + C3 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

وان C2 هو الوقت المستغرق على كل PE_j، وانه يمكن قياسه با ستخدام برنامج محاكاة وتمثيله T، اذن سيكون الوقت الكلي للخوارزمية هو:

$$t(n) = T + C \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

ويتم الاتفاق بين المرسل والمستلم على عدد bits التي تم استخدامها في عملية الاخفاء ليتم استرجاعها بصورة صحيحة وهل الرسالة السرية مشفرة او غير مكبوسة.

تتضمن الخوارزمية المتوازية المقترحة اتجاهين رئيسيين هما الاخفاء والاسترجاع والتي يتم نفيذها من قبل كل PE_j حيث يمكن توضيح الخطوات الرئيسية للإخفاء بالمخطط الانسيابي في الشكل (٢) والذي يقدم وصف كاملا لتنفيذ عملية الاخفاء:

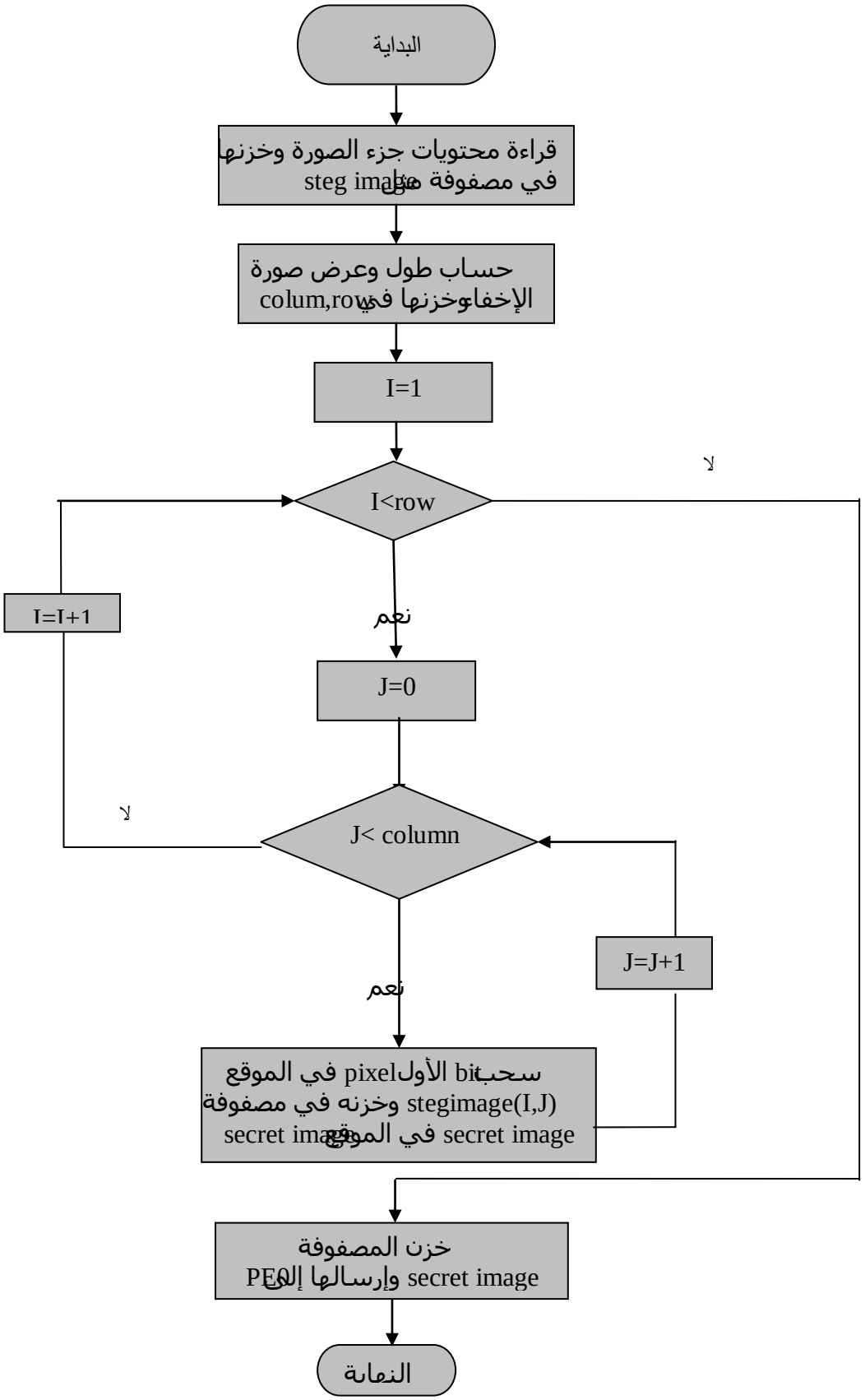


الشكل (٢) المخطط الانسيابي لعملية الإخفاء

وان الخوارزمية المتوازية المقترحة لعملية الاخفاء تتضمن الخطوات التالية:

Step 1: (Processor) PE_0
(1,1) Read the cover image.
(1,2) Start divide the image into n (n=4) sub images.
(1,3) Read the secret image.
(1,4) Start divide the secret image into n sub image.
(1,5) Start broadcast the sub images to the PEs.
(1,6) Send part of cover image and part of secret image to one of PEj.
Step 2: (processors) PE_j
(2,1) **For** i=1 to n **do** in **parallel**
(2,2) Count the length and width of the cover image
(2,3) while (i<row) do
(2,4) while (j<column) do
(2,5) Reset the least significant bit for the pixel at the position (i,j) of cover image.
(2,6) Hide the bit value at position (i,j) of the secret image at the least significant bit at the position (i,j) of the cover image.
end while
end while
(2,7) Send back the cover image after steganography.
end for
Step 3: (Processor PE_0)
(3,1) Receive all the sub images.
(3,2) Merge the sub images to produce the cover image.

أما الجزء الرئيسي الثاني من الخوارزمية تضمن عملية الاسترجاع حيث يمكن توضيح الخطوات الرئيسية للاسترجاع بالمخطط الانسيابي في الش كل (٣) والذي يقدم وصفاً كاملاً لتنفيذ عملية الاسترجاع:



الشكل (٣): المخطط الانسيابي لعملية الاسترجاع

وان الخوارزمية المتوازية المقترحة لعملية الاسترجاع تتضمن الخطوات التالية:

Step 1: (Proceesor PE_0)
(1,1) Read the steo image.
(1,2) Start divide the image into n(n=4) sub images.
(1,3) Start broadcast the sub images to the PEs.

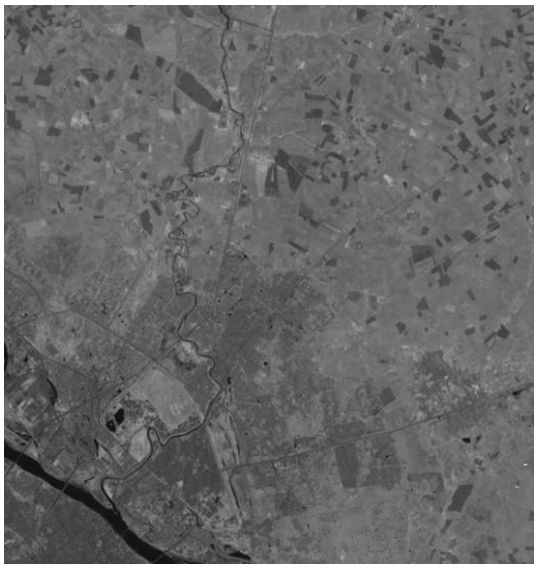
Step 2: (Processor PE_j)
(2,1) For i=1 to n **do** in **parallel**
(2,2) Count the length and the width of the steg image.
(2,3) while (i<row) do
(2,4) while (j<column) do
(2,5) Draw the value of least significant bit at the position (i,j) of steg image and put this value at the position (i,j) of the secret image.
end while
end while
(2,6) Send back the secret image.
end for
Step 3: (Processor PE_0)
(3,1) Receive all the subimages.
(3,2) Merge the subimage, to produce the secret image.

مثال تطبيقي متكامل لخطوات تنفيذ الخوارزمية المقترحة.

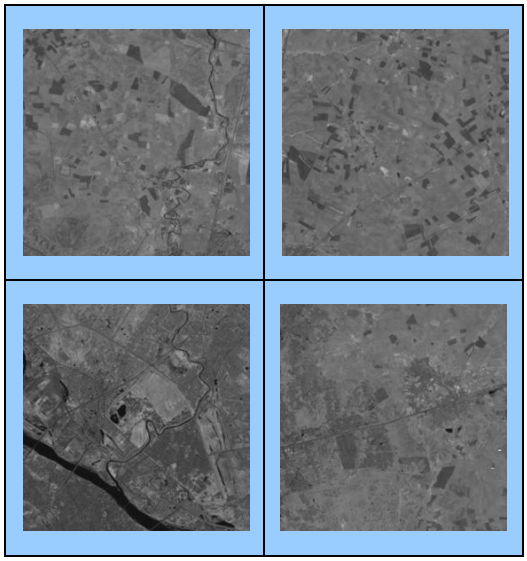
تم استخدام صورة ثنائية مربعة بحجم (1024 x ١٠٢٤) لعملية الاخفاء (الصورة السرية) وتم تقطيع هذه الصورة الى عدد من الاجزاء المتساوية الحجم (في عدد pixel) حيث حجم كل واحد (٢٥٦x 256)، واستخدام صورة رمادية مر بعة كصورة غطاء لعملية الاخفاء بحجم (١٢٠٤x1024)، بحيث تم تقسيم هذه الصورة الى عدد من الاجزاء كل واحد بحجم (٢٥٦x256) مساوي لعدد اجزاء الصورة السرية، ثم تطبيق برنامج محاكاة يشمل عملية الاخفاء (أو الاسترجاع) لجزء من اجزاء الصورة السرية على جزء مقابل من اجزاء الصورة الغطاء.

ثم دمج جميع اجزاء الصورة الغطاء بعد عملية الاخفاء لإظهار الصورة الغطاء كصورة كاملة غير مجزئة.

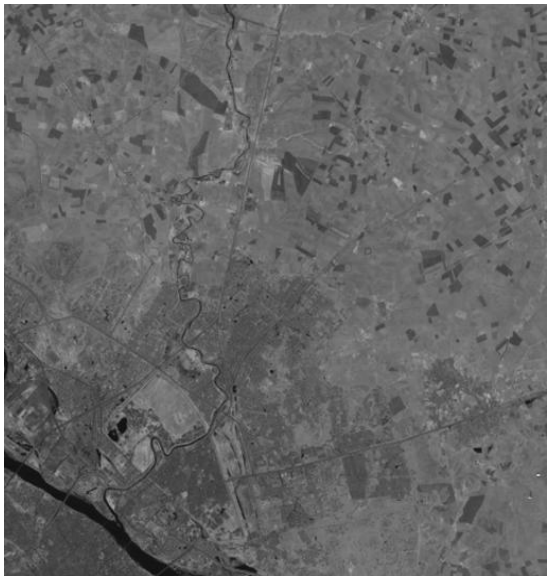
الاشكال (٨.١) تعرض صورة الغطاء قبل وبعد تقسيمها الى اربعة اجزاء متساوية قبل عملية الاخفاء وبعدها وصورة السرية قبل الاخفاء وبعد التقسيم.



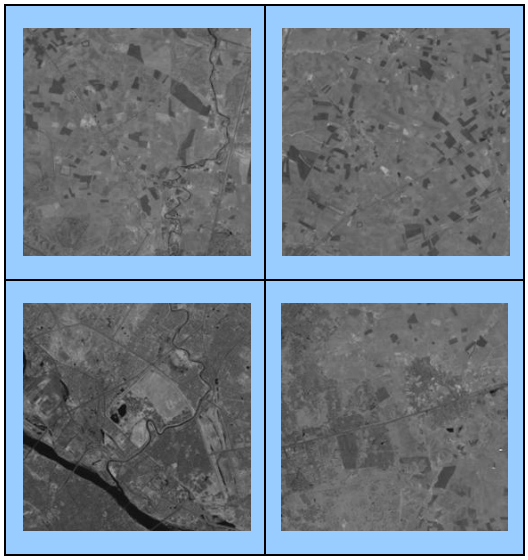
الشكل (): صورة الغطاء قبل الاخ



الشكل (): صورة الغطاء مقسمة قبل

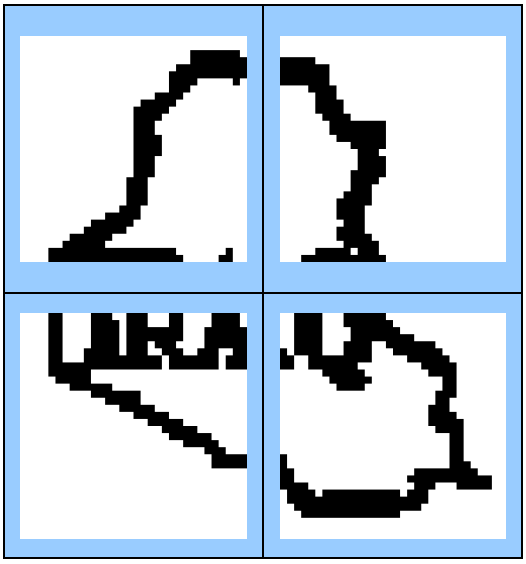


الشكل (): صورة الغطاء بعد الاخفاء
تجميعها في PCI



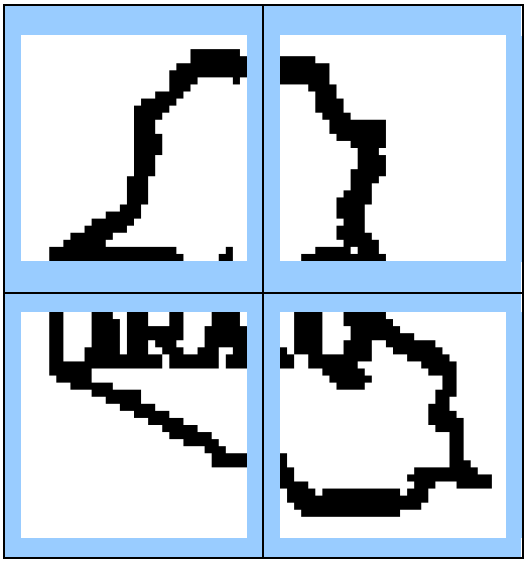
الشكل (): صورة الغطاء مجزءه بعد ا

الشكل(): الصورة السرية قبل الاخ



الشكل(): الصورة السرية بعد ال

الشكل(): أجزاء الصورة السرية بعد ع
الاسترجاع



الشكل(): الصورة السرية بعد الاس
في PE

جدول١ (بيانات جزء من الصورة الموجودة في PEj قبل عملية الأخفاء)

ت	a	b	c
1	1	106	01101010
2	0	102	01100110
3	0	110	01101110
4	1	108	01101100
5	0	104	01101000
6	1	114	01110010
7	0	110	01101110
8	0	106	01101010
9	1	118	01110110
10	0	126	01111110
11	0	128	10000000
12	1	124	01111100
13	0	130	10000010
14	0	132	10000100
15	0	130	10000010
16	0	132	10000100
17	0	130	10000010
18	1	134	10000110
19	0	142	10001110
20	0	138	10001010
21	1	122	01111010
22	1	114	01110010
23	1	102	01100110
24	0	96	01100000
25	1	113	01110001
26	1	123	01111011
27	0	119	01110111
28	0	93	01011101

جدول٢ (بيانات جزء من الصورة الموجودة في PEj بعد عملية الأخفاء)

ت	a	b	c
1	1	107	01101011
2	0	102	01100110
3	0	110	01101110
4	1	109	01101101
5	0	104	01101000
6	1	115	01110011
7	0	110	01101110
8	0	106	01101010
9	1	119	01110111
10	0	126	01111110
11	0	128	10000000
12	1	125	01111101
13	0	130	10000010
14	0	132	10000100
15	0	130	10000010
16	0	132	10000100
17	0	130	10000010
18	1	135	10000111
19	0	142	10001110
20	0	138	10001010
21	1	123	01111011
22	1	115	01110011
23	1	103	01100111
24	0	96	01100000
25	1	113	01110001
26	1	123	01111011
27	0	118	01110110
28	0	92	01011100

تم عمل مقارنة بين بيانات جزء من الصورة الموجودة في احد PEj قبل وبعد عملية الاخفاء وبالشكل التالي :-

أ. الجدول رقم (١) يوضح الحقل (a) قيم الثنائية لجزء من الصورة السرية خريطة اما الحقل (b) يمثل القيم الرمادية (pixel) لجزء من صورة الغطاء والحقل (c) يمثل القيم بالنظام الثنائي للحقل (b).

ب. الجدول رقم (٢) يوضح الحقل (a) قيم الثنائية لجزء من الصورة السرية اما الحقل (b) فيمثل القيمة الرمادية لجزء من صورة الغطاء بعد عملية الاخفاء والحقل (c) يمثل القيمة بالنظام الثنائي للحقل (b).

وكذلك تم قياس زمن تطبيق خوارزمية الإخفاء باستخدام خوارزمية اعتيادية تسلسلية لصورة بحجم (1024×1024) بزمن مقداره (t(n)=٠.٣٤٣٨) ثم قي س زمن تطبيق خوارزمية الإخفاء باستخدام خوارزمية متوازية وتطبيقها على احد أجزاء الصورة وكانت بحجم (64*64) حيث تم تجزئة الصورة الأصلية وصورة الإخفاء إلى 16 جزء وبهذه الحالة سوف يكون زمن تنفيذ الخوارزمية لكل جزء من الأ جزاء الـ 16 هو (٠.٠٤٦٩)، عليه يكون الزمن الكلي للخوارزمية المتوازية (t(n)= ٠.٠٤٦٩+C). حيث C تمثل زمن قراءة وتقسيم الصورة في بداية الخوارزمية وزمن دمج الأجزاء مع بعضها للحصول على الصورة الكلية بعد التنفيذ ، ان الدمج لاجزاء الصورة سيكون من قبل المعالج المركزي حيث ان التوزيع المستخدم هو (star network) كما أشير اليه في الفقرة 3-4).

تبين من خلال قياس مقدار التقارب بين الصورة السرية قبل الإخفاء وبعد الإخفاء من خلال حساب معامل الارتباط(r) كما في المعادلة(٥) correlation coefficient.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{[\sum_m \sum_n (A_{mn} - \bar{A})^2][\sum_m \sum_n (B_{mn} - \bar{B})^2]}} \quad \ldots\ldots\ldots (٦)$$

حيث $\bar{A} = \text{mean2(A)}$ ، $\bar{B} = \text{mean2(B)}$

وكذلك من خلال حساب البعد الاقليدي لكلا الصورتين حسب المعادلة (6) وتبين تطابق كامل لمعلومات الصورة، أي أن الصورة المسترجعة قد حافظت على كافة تفاصي ل الصورة الأصلية (معامل الارتباط n=1). عليه تكون عملية الإخفاء قد نفذت بشكل كفوء جداً.

Normal distance

$$\sqrt{\sum_{i=1}^{n} |X_i - Y_i|^2} \ldots\ldots\ldots\ldots (7)$$

حيث (Xi) تمثل نقطة من الصورة السرية قبل الاخفاء و(Yi) تمثل نقطة من الصورة السرية بعد الاسترجاع التي تقابل النقطة (X) .

الاستنتاجات: Conclusion

تعتبو خوارزمية الاخفاء في الصور الثنائية طريقة فعالة ومرضية في الحفاظ على المعلومات من المهاجم من جهة ومن ضياع المعلومات لصورة الغطاء جراء عملية الاخفاء والاسترجاع من جهة اخرى.

بينما تعتبر هذه الخوارزمية مع جميع الخوارزميات الم تقدمة في عملية الاخفاء غير كفوء ة بالنسبة للصور ذات الاحجام الكبيرة جداً مثل الصور العسكرية وصور التحسس النائي الناتجة عن الاقمار الصناعية،حيث تكون المعالجة لتلك الصورة باعتماد الخوارزميات الكلاسيكية التقليدية فاشلة (مثال ذلك عملية اللافوف الرياضي لا يمكن اجراءها على مصفوفات ذات ابعاد كبيرة جدا وماشابه ذلك) عليه تم اقتراح خوارزمية لتسريع عملية الاخفاء (الاسترجاع) داخل هذه الصور.

الأعمال المستقبلية:

١ – إمكانية تطوير الخوارزمية باتجاه إحلال الخوارزمية الجينية وإمكانياتها في تغيير جيني للصورة قبل الإخفاء لأجل الحفاظ على الصورة من المتطفلين ال ذين قد يتمكنون من استرجاع الصورة المخفية والتي ستظهر مشفرة (باعتماد الخوارزمية الجينية).

٢ – إمكانية اعتماد الهندسة الكسورية لأجل تشفير الصورة (من خلال نسجات الصورة المستخلصة باعتماد البعد الكسري) قبل إخفائها لزيادة في أمنية المعلومات المخفية.

٣ – امكانية استخدام طرق اخفاء اخرى مثل الاخفاء باستخدام DCT وغيرها.

المصادر: References

١) القاضلي، يحيى قاسم (٢٠٠٢): "حل مس ألة التخصيص باستخدام خوارزمية متوازية "، جامعة الموصل، وزارة التعليم العالي والبحث العلمي.

٢) سلو، اميرة بيبو (٢٠٠٩): "تقنيات اخفاء المعلومات باستخدام الش بكات العصبية وبروتوكالات الشبكة، جامعة الموصل، وزارة التعليم العالي والبحث العلمي.

٣) الحمامي، علاء حسين و الحمامي، محمد علاء (٢٠٠٨)، "إخفاء المعلومات : الكتابة المخفية والعلامة المائية"، إثراء للنشر والتوزيع، الشارقة.

4) Bashir M.S. khalaf (1990): "Parallel Numerical Algorithms for solving ordinary Differential Equation", amazon.co.uk:basher Ms kalaf: books University of Leeds, U.K. www.amazon.co.uk/parallel-numeriecl-a.

5) Ian Foster (1995): "A Parallel Machine Model" puplished by Addison-wesley.

6) Johnson, Neil F., Duricy, Zoran and Jajodia, Sushil (2001), "Information Hiding: Steganography and Watermarking Attacks and Countermeasures", University of George Mason en.wikipedia.org/wiki/steganography.

7) Kenneth A. Berman and Jerome L. paul, "sequential and parallel algorithms". university of Cincinnati, LData palished, 1996 ISBN-13 www.alibris.com/search/books/qwork/15.

8) Ronald L Krutz, PH.D. (2003), "Hiding in Plain Sight: Steganography and the Art of Covert Communication", by Eric cole. wiley pulishing.Inc.canada www.aaliris.com/search/books/isbn/978

9) Mohanty, Saraju P., (1999), "Digital watermarking: Atutorial Review", Rep. INDIN in statue of science. www69.homepage.vi//anova.edu/Nathan.s.

10) Morkel, T., Eloff, J.H.P. and Olivier, M.S., (2005), "An Overview of Image Steganography", University of Pretoria. Pretoria, South Africa. tmorkel@cs.up.ac.za eloff@cs.up.ac.za molivier@cs.ac.za

11) Nori Ahmed, Ahmed Sami, (2006), "An Investigation for Steganography in Moving Pictures", Unpublished D. Ph. Thesis, University of Mosul, Iraq.

12) Potdar1, Vidyasagar, A.Khan1, Muhammad, (2004), "E-Forensics Steganography System for Secret Information Retrieval", School of Information Systems, Curtin University of Technology, Perth, Western Australia.

13) Queirolo, Francesco, (2001), "Steganography in Images". www.scribd.com/doc/28133213/steganograph-in-Images.

14) Selim G. AKI (1989): "The Desigen and Analysis of Parallel Algorithms". www.research.ibm.com/masplas/masplas/masplasol/nagaraja.pdf