



اسم المقال: تحسين خوارزمية تشفير الصور الثنائية باستخدام مطابقة النماذج

اسم الكاتب: م.م. حنان زكي حمدي، م.م. سندس خليل إبراهيم

رابط ثابت: <https://political-encyclopedia.org/library/3185>

تاريخ الاسترداد: 2026/04/13 09:04 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت. لمزيد من المعلومات حول الموسوعة السياسية - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسية - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع <https://political-encyclopedia.org/terms-of-use>



تحسين خوارزمية تشفير الصور الثنائية باستخدام مطابقة النماذج

حنان زكي حمدي

سندس خليل إبراهيم

مدرس مساعد

جامعة الموصل/كلية علوم الحاسبات والرياضيات

قسم علوم الحاسبات

sunduskhaleel@yahoo.com

hanan_zeki@yahoo.com

المستخلص

إن أية تقنية مبتكرة تُقدّم لكبس الصور تدمج بين الإرسال السريع والكبس من دون فقدان المعلومات. والاعتبار الأكثر أهمية هو اختيار تقنية ترميز تقلل بيانات الصورة إلى عدد من العناصر التي تحمل صفات تمييزية كافية مع حفظ كافٍ للمعلومات، الفكرة من البحث هي تحسين خوارزمية التشفير بمطابقة النماذج وتحديد أقل ما يمكن من البيانات المطلوبة للحصول على اختزال في حجم البيانات الناتجة من دون فقدان أي من معلومات الصورة، إذ شمل التعديل صيغة تخزين البيانات، فضلاً عن إضافة مرحلة ابتدائية بوصفها معالجة أولية لتهيئة الصورة للتشفير وهي مرحلة إنشاء هيكل الصورة باستخدام عملية التحفيف والتعرية والتقليم. طبقت الخوارزمية المعدلة أو المحسنة على ملفات ذات محتويات مختلفة من دون معالجة أولية، وتم الحصول على نسبة كبس في حجم الملف النهائي بمعدل (٦٧%)، أي نسبة اختزال البيانات في حجم الملف النهائي بمعدل (٣٣%). أما عند إضافة المعالجة الأولية فكانت نسبة الكبس بمعدل (٥٤%)، أي نسبة الاختزال بمعدل (٤٦%).

Improving the Encryption Algorithm of Binary Images by Using Templates Matching

Hanan Zeki Hamdey
Assistant Lecturer
Department of Computer Sciences
University of Mosul

Sundus Khaleel Ebraheem
Assistant Lecturer
Department of Computer Sciences
University of Mosul

ABSTRACT

Any innovated technique introduced for images compression should be mixed between both, rapid transmission and lossless compression. The most important consideration is the selection of an encoding technique that reduces image data into lowest number of elements with a sufficient distinguishing features as well as a sufficient saving of information. The paper aims at developing the encoding algorithm using the method of (Templates Matching) and identifying the less possible required data to obtain a reduced size of resulting data without losing any of the image information.

تأريخ قبول النشر ٢٠٠٧/٨/١٢

تأريخ استلام البحث ٢٠٠٧/٢/١٩

The modification has included data saving formula, as well as the addition primary stage (preprocessing) as an initial processing to prepare the image for encoding, which is considered the stage of constructing image skeleton through thinning, erosion and pruning processes. The modified algorithm has been applied on files with various images contents without preprocessing and a compression percentage has been obtained in the size of the final file by an average of (67%).i.e. data reduction percentage of (33%) in the size of the final file. However, when the preprocessing was added, compression percentage was of (54%).i.e. reduction percentage of (46%).

المقدمة

إن موضوع كبس البيانات يدخل في حقل معالجة الصور، وتحليل الصور يجب أن يكون هناك قدرة لمعالجة النتائج بشكل مباشر، فالفكرة الأساسية للكبس هي إيجاد طريقة لتمثيل البيانات لتأخذ أقل مساحة للخرن، وذلك لاستغلال الموارد والإمكانات المتاحة بأفضل شكل ممكن. إن معظم نماذج أنظمة الكبس تتألف من جزءين رئيسيين (Gonzales and Woodes, 2005,335-337)، الجزء الأول الكبس (Compressor)، ويضم بصورة عامة طور المعالجة الأولية للعملية و طور التحليل والترميز، وأغلب خوارزميات الكبس المطبقة عملياً تدمج عدداً من تقنيات الكبس المنفردة. إن تطور خوارزميات الكبس أدى إلى تطور مماثل في عمليات المعالجة من خلال طور المعالجة الأولية، إذ شمل عمليات كثيرة مثل التحسين وإلغاء الضوضاء... وغيرها، فالهدف من هذه المعالجة هو تحضير الصورة للعملية اللاحقة (النعيمي، ٢٠٠٣، ١٨-١٩)، مما أدى إلى التقليل من كمية الخزن المطلوبة للبيانات، ومن ثم التقليل من عرض الحزمة المطلوبة لنقلها، فضلاً عن زيادة سرعة النقل وتقليل احتمالية حدوث الأخطاء أثناء عملية النقل بوصفه ناتجاً عرضياً لعملية الكبس. أما الجزء الثاني فهو محلل (فك) الكبس (Decompressor)، ويتألف من طور إعادة التحليل (Decoding) متنوعة بطور المعالجة المتقدمة (النعيمي، ٢٠٠٣، ١٥-١٩).

يعد كبس البيانات أحد المكونات الأساسية والمهمة في علم الحاسبات، وتكون الحاجة إلى الكبس بشكل أكثر في خزن وإرسال البيانات (قدو، ٢٠٠٤، ١٩). وقد ازدادت أهمية الكبس بشكل كبير إثر النمو السريع الحاصل في علم الحاسوب والنمو الذي قابله في مجال الأوساط المتعددة، فضلاً عن انتشار الإنترنت بشكل واسع التي تتطلب الجديد والأفضل والأسرع من خوارزميات الكبس (النعيمي، ٢٠٠٣، ١). من هنا يهدف البحث إلى تطوير خوارزمية لها القابلية على التشفير بأسلوب يؤدي إلى اختزال البيانات بحيث يقلل من مساحة الخزن، مما يؤدي إلى تقليل الكلفة ووقت النقل، فضلاً عن تقليل حزمة الإرسال.

طريقة التشفير

تم في هذا البحث تطوير طريقة التشفير بمطابقة النماذج لتشفير الصور الثنائية (ابراهيم، ٢٠٠٦، ٤٣-٦٩)، سنوضح في هذه الفقرة التعديلات المضافة.

١. طور المعالجة الأولية: وهي مرحلة مضافة إلى الطريقة تؤدي إلى تقليل البيانات، إذ بالإمكان اختزال بيانات الصورة بعملية التنحيف والتعرية والتقليم، باستخدام العمليات التشكيلية في الصور الثنائية لإنشاء هيكل الصورة (AI-

Fahady, et al., 2004, 1-9) للتقليل من حجم محتويات الصورة بالنسبة إلى خلفيتها، وذلك بإلغاء بعض الخصائص الصغيرة جداً مثل التشوهات والحافات الزائدة والحصول على عدد أقل من الوحدات الضوئية. والتحفيف عملية أساسية في تحليل الصورة الثنائية وتمثل تقليل عرض الجسم في الصورة من عدة نقاط إلى نقطة واحدة (Fisher,et (Admain and Sameer 1997,101-108) من دون قطع خط موصول أو إيصال خط مقطوع، عليه فقد تم استخدام هذه الطريقة بوصفها معالجة أولية لتهيئة الصور قبيل تطبيق خوارزمية التشفير عليها.

٢. طور الترميز: يتم في هذه المرحلة تطبيق خوارزمية التشفير:
المرحلة الأولى: تحويل الصور إلى الصيغة الثنائية وتصميم النماذج الخاصة بعملية التشفير وتحديد رموز البيانات (ابراهيم، ٢٠٠٦، ٤٧).
المرحلة الثانية: مطابقة النماذج على الصورة، وبذلك يتكون ملف يضم بيانات تتراوح قيمها ما بين (٠-٦) (ابراهيم، ٢٠٠٦، ٤٨).
المرحلة الثالثة: يتم تحويل القيم الناتجة إلى أعداد ثنائية (٠،١)، إذ تمثل كل قيمة بـ (3bits) (ابراهيم، ٢٠٠٦، ٥٠).
المرحلة الرابعة: فقد تم إجراء التعديلات عليها، إذ تم أخذ كل (16bits) ليمثل قيمة واحدة بدلاً من (4bits)، أنظر المقطع البرمجي التالي الذي يحول كل 16 قيمة (تمثل كل قيمة منها bit واحد) من ("٠" أو "١") إلى قيمة واحدة بحجم (word)، إذ تتم مقارنة القيمة، فإذا كانت "١" نستعمل لها shift left مرة واحدة، ثم نعمل OR مع القيمة "٠١" ليدخل bit واحد قيمته "١"، أما إذا كانت القيمة "٠" فإننا سنعمل shift left مرة واحدة فقط ليدخل bit واحد قيمته "٠". وبالنتيجة نحصل على القيمة (x) وتتكون من (16 bit) والتي يتم تخزينها بالملف، وبذلك تتراوح بيانات الملف بين (FFFF-0) بدلاً من (F-0).

```
x=0;    m=1;    /* m is number of bits in x */
while ((m<=16)&&!feof(txt) )
{ fscanf(txt,"%i",&n);
  switch(n)
  { case 1 : x=(int) ((x) << 1);
    x=(int) ((x) | 0x01);
    m++;      break;
    case 0 : x=(int) ((x) << 1);
    m++;      break; } }
```

كما في المثال الآتي :

4000000000000000004A2A1B9249200938B49240000949248
D23249249114514514400000000251501290B6E40246816
B48A800251C5966E4922CB2D24924921400000264924540
0B18036E00948D332454002454005ACB2C600000B49248A
80000129249150000000092491600012000000000024923
8B000000251A0128A80000000048B2C6000002400000000
004C91658000000005C80251500000000252000000945190
A0000000004A469144A00000000480251500000000331500
001292490000000000B92492468A0000049248A800000002
43000033238B486000000000005ACB372491500000B6E49
0C00000000990000090C02400000000000000005B722A000
0000000000000171C000024691464000000000000000025
150000000000000000000000002524920000000000000002
4540000000000000000000000000000165965963000000000000
00005AC000
0092
8001145144A00001992485000000000000000000000000000
000049249249000006E492180000000000000000000000000
00000DC9248B2CB1800000000000000000000000000000000
000
00000000000000000000

٣. أما عند تطبيق المرحلة الرابعة بعد تحديث الخوارزمية فالبيانات الناتجة كانت كما يأتي:

000
000
000
000
000
000
000
DC54065A0000000000160491A280009464924680000006E48A8000
49249238000000001600005AC6000001991A28001192445128000000
0004A492491A92492488940045145144A0094514514400004A2A1B924920
938B4924000949248D23249249114514514400251501290B6E4246816B
48A8251C5966E4922CB2D249249214002649245400B18036E00948D33245400
24545ACB2C6000B49248A8001292491500092491600012000000000249238B025
1A0128A80048B2C600240004C916580005C80251500025200094519A00
04A469144A00480251500331501292490000B92492468A00049248A8000
243033238B486005ACB372491500B6E49C00099090C2400005B722A000
000171C00024691464000002515000000252492000002454000001
6596596300005AC000000000000000000000000000009281145144A0019
9248500000004924924906E49218000000000DC9248B2CB18000000
00000000000000000000

المرحلة الخامسة: تم استخدام طريقة كبس الصور (Run Length Encoding) RLE على بيانات الملف النهائي التي قيمتها مساوية للصفر فقط، إذ يتم حساب عدد الأصفار المتتالية وتكوين رمز يتكون من جزئين، الأول ٠ والثاني يمثل عدد الأصفار (ابراهيم، ٢٠٠٦، ٥١-٥٢).

مناقشة النتائج

على محلل الشفرة (المستلم) معرفة تسلسل معاملات الأنموذج وطريقة تكوين رموز البيانات (كمفتاح) ثم يعمل على فك الكبس بطريقة RLE (أي يتم تكرار الأصفار حسب عددها)، وذلك بعد قراءة عدد الصفوف والأعمدة وحجم الأنموذج، إذ سيحصل على قيم البيانات التي تتراوح بين (FFFF-٠)، ثم يطبق خطوات خوارزمية فك الشفرة للطريقة قبل التحديث كما هي (ابراهيم، ٢٠٠٦، ٥٢-٥٣) عدا الخطوة الخامسة ستبدل إلى ما يأتي:

- تحويل البيانات الناتجة إلى أعداد ممثلة بنظام الأعداد الثنائية، وذلك بتمثيل كل قيمة بـ (16 bits).

إن أغلب عمليات فك الكبس لاتخضع إلى أسلوب عكس الكبس (أي غير عكسية) للحصول على الصورة الأصلية (النعيمي، ٢٠٠٣، ١٩-٢٢)، لذا فإن الصورة المعاد فتحها بعد عملية التشفير تكون من دون فقدان في المعلومات، عليه فلا حاجة لنا إلى مرحلة المعالجة المتقدمة.

اختبار مدى كفاءة الخوارزمية المقترحة

من المعروف أن قياس مدى كفاءة أي خوارزمية للكبس يعرف من خلال حساب نسبة الكبس (Y) (النعيمي، ٢٠٠٣، ٢٢) وحسب القانون:

$$Y = \frac{AS}{BS} * 100 \quad \text{-----}(2)$$

إذ إن :

AS هو حجم الملف النهائي بعد التحديث.

BS هو حجم الملف النهائي قبل التحديث.

أو حساب نسبة اختزال البيانات (Z) حسب القانون:

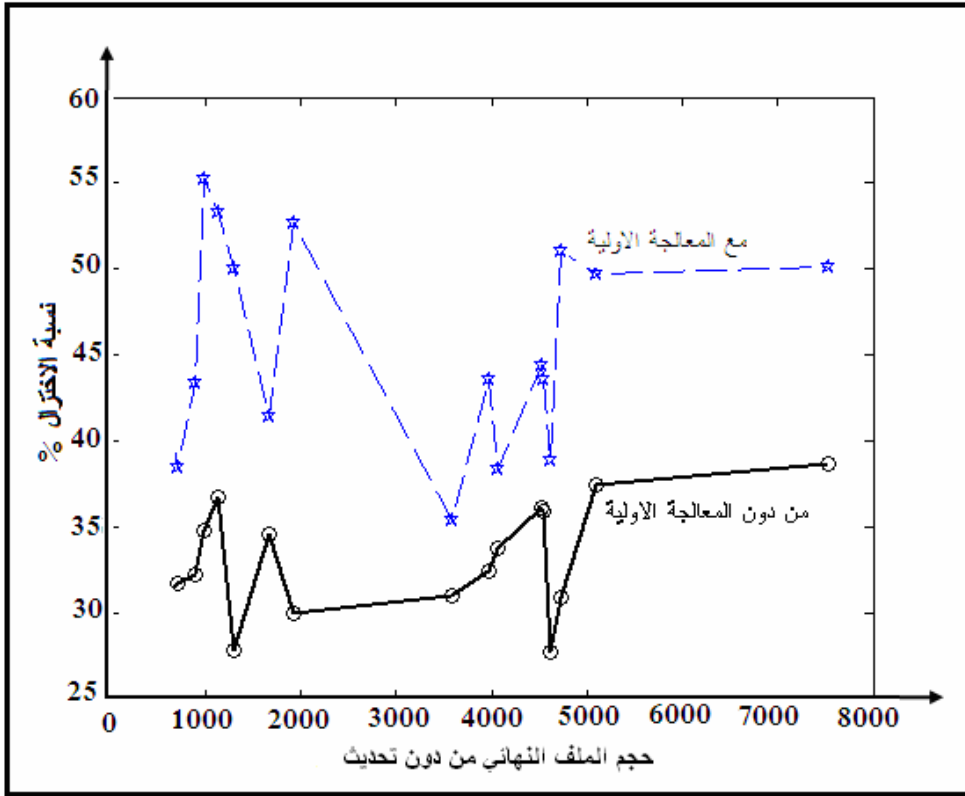
$$Z = \frac{BS - AS}{BS} * 100 \quad \text{-----}(3)$$

وكانت نتائج تطبيق الخوارزمية على نماذج لصور متنوعة ذات الامتداد (BMP) الاحادية اللون (mono) وبأحجام مختلفة كما في الجدول الآتي:

الجدول (١) يبين نسبة الكبس والاختزال من دون معالجة أولية، ومع المعالجة الأولية

ت الأمثلة	حجم الملف النهائي من دون تحديث (بايت)	حجم الملف النهائي بعد التحديث (بايت)		نسبة الكبس (%)		نسبة الاختزال (%)	
		مع المعالجة الأولية	من دون المعالجة الأولية	مع المعالجة الأولية	من دون المعالجة الأولية	مع المعالجة الأولية	من دون المعالجة الأولية
١	٧٠٧	٤٨٣	٤٣٥	٦٨,٣١٧	٦١,٥٢٨	٣١,٦٨٣	٣٨,٤٧٢
٢	٩٠٠	٦١٠	٥١٠	٦٧,٧٧٨	٥٦,٦٦٧	٣٢,٢٢٢	٤٣,٣٣٣
٣	٩٨١	٦٤٠	٤٣٩	٦٥,٢٤٤	٤٤,٧٥٥	٣٤,٧٦٦	٥٥,٢٥٥
٤	١١٤٠	٧٢١	٥٣٢	٦٣,٢٤٦	٤٦,٦٦٧	٣٦,٧٥٤	٥٣,٣٣٣
٥	١٢٩٢	٩٣٣	٦٤٦	٧٢,٢١٤	٥٠	٢٧,٧٨٦	٥٠
٦	١٦٧٣	١٠٩٤	٩٨٠	٦٥,٣٩٢	٥٨,٥٧٧	٣٤,٦٠٨	٤١,٤٢٣
٧	١٩٢٥	١٣٤٨	٩١٠	٧٠,٠٢٦	٤٧,٢٧٣	٢٩,٩٧٤	٥٢,٧٢٧
٨	٣٥٨٠	٢٤٧٠	٢٣١٣	٦٨,٩٩٤	٦٤,٦١	٣١,٠٠٦	٣٥,٣٩
٩	٣٩٧٥	٢٦٨٦	٢٢٤٢	٦٧,٥٧٢	٥٦,٤٠٣	٣٢,٤٢٨	٤٣,٥٩٧
١٠	٤٠٧٠	٢٩٩٨	٢٥٠٧	٦٦,٢٩	٦١,٥٩٧	٣٣,٧١	٣٨,٤٠٣
١١	٤٥٢٥	٢٨٩٣	٢٥١٧	٦٣,٩٣٤	٥٥,٦٢٤	٣٦,٠٦٦	٤٤,٣٧٦
١٢	٤٥٣٩	٢٩١٠	٢٥٥٩	٦٤,١١١	٥٦,٣٧٨	٣٥,٨٨٩	٤٣,٦٢٢
١٣	٤٦١٧	٣٣٣٨	٢٨٢٣	٧٢,٢٩٨	٦١,١٤٤	٢٧,٧٠٢	٣٨,٨٥٦
١٤	٤٧٢٢	٣٢٦٤	٢٣١٢	٦٩,١٢٣	٤٨,٩٦٢	٣٠,٨٧٧	٥١,٠٣٨
١٥	٥١٠١	٣١٩٢	٢٥٦٥	٦٢,٥٧٦	٥٠,٢٨٤	٣٧,٤٢٤	٤٩,٧١٦
١٦	٧٥٣٧	٤٦٢٦	٣٧٦١	٦١,٣٧٧	٤٩,٩	٣٨,٦٢٣	٥٠,١
			المعدل	%٦٧	%٥٤	%٣٣	%٤٦

إن المخطط في الشكل ٢ يوضح العلاقة بين حجم الملف النهائي من دون تحديث الخوارزمية ونسبة الاختزال التي حصلنا عليها بعد تحسين الخوارزمية، فالخط الغامق يبين نسبة الاختزال عندما طبقت الخوارزمية الجديدة من دون المعالجة الأولية، أما الخط المتقطع فيبين نسبة الاختزال عندما طبقت الخوارزمية الجديدة مع المعالجة الأولية.



الشكل (2) : مخطط يبين العلاقة بين حجم الملف النهائي من دون تحديث و نسبة الاختزال

إذ يبين لنا هذا المخطط أن المعالجة الأولية أدت إلى زيادة نسبة الاختزال فأصبحت ٤٦% بدلاً من ٣٣%، مما يزيد من كفاءة الخوارزمية الجديدة.

الاستنتاجات

بما أن الكبس والتشفير من المتطلبات المهمة في مجال الحاسوب والإنترنت، لذا سعينا في هذا البحث إلى تحسين خوارزمية تشفير الصور الثنائية باستخدام مطابقة النماذج بحيث نقل من مساحة الخزن ونظيل من الزمن اللازم لمهاجمة الرسالة، إذ تم تطبيق الخوارزمية المذكورة آنفاً على صور من نوع (BMP) الأحادية اللون مع التحديثات باستخدام لغة C++ وقد أدت الخوارزمية الجديدة إلى رفع كفاءة الطريقة من خلال زيادة كفاءة التشفير والكمس وكما في أدناه:

١. ان استخدام 16bits بدلاً من 4bits في المرحلة الرابعة قد أدى إلى الحصول على نسبة كبس بمعدل (٦٧%)، أي نسبة اختزال بمعدل (٣٣%) كما موضح في فقرة مناقشة الناتجة- أولاً-.

٢. إن استخدام المعالجة الأولية أدى إلى زيادة البيانات التي قيمتها "٠"، وذلك بتقليل حجم محتويات الصورة بالنسبة لخلفيتها ومن دون فقدان في معلومات الصورة

- باستخدام طريقة التنحيف والتعرية والتقليم. وبذلك أصبحت نسبة الكبس بمعدل (٥٤%)، مما أدى إلى زيادة كفاءة الكبس في المرحلة الرابعة. كما في الجدول ١.
٣. من المخطط في الشكل ٢ نلاحظ أنه ليس هنالك علاقة محددة بين حجم الملف النهائي ونسبة الاختزال، لأن نسبة اختزال البيانات لا تتأثر بحجم الملف بل تتأثر بخلفية الصورة (Background) فكلما زادت الخلفية زادت نسبة الاختزال، وكما موضح في فقرة " اختبار مدى كفاءة الخوارزمية المقترحة".
٤. إن التحديث الحاصل في المرحلة الرابعة وإضافة المعالجة الأولية لم يؤثر على معايير شانون لقياس مدى كفاءة سرية الطريقة (Beker and Piper, 1982, 162-166) من حيث بساطة المفتاح وبساطة عملية التشفير وفك الشفرة باستخدام الحاسوب وبقيت نسبة الخطأ تساوي صفراً. أي أن هذه الإضافات البسيطة ستؤثر بشكل ايجابي في زيادة الوقت اللازم لتخمين الخوارزمية في حالة مهاجمتها من قبل المتطفل.
٥. إن إضافة المعالجة الأولية أدت إلى زيادة كفاءة الخوارزمية حسب فرضية أسوأ الاحتمالات (Beker and Piper, 1982, 162-166)، إذ ستزيد من تعقيد الطريقة وعليه ستزداد العشوائية ونحصل على سرية أكبر.

المراجع

أولاً- المراجع باللغة العربية

١. ابراهيم، سندس خليل، ٢٠٠٦، "تشفير الصور الثنائية باستخدام مطابقة النماذج" مجلة الرافدين لعلوم الحاسبات والرياضيات، المجلد ٣، العدد ٢.
٢. قدو، سجي جاسم، ٢٠٠٤، "كبس اشارة الكلام بواسطة استخلاص الخواص"، بحث ماجستير، جامعة الموصل، كلية علوم الحاسبات والرياضيات.
٣. النعيمي، ميسون خضر، ٢٠٠٣، "كبس صور الوثائق النصية العربية"، بحث ماجستير، جامعة الموصل، كلية علوم الحاسبات والرياضيات.

ثانياً - المراجع باللغة الاجنبية

1. Adnan Amin. And Sameer Singh., 1997, "Machine Recognition of Hand-printed Chinese Characters", Inteligent Data Analysis, Vol.1.
2. Henry Beker and Piper Fred. , 1982, Cipher Systems The Protection of Communications.
3. Kubais S. Al-Fahady, Khalil I. Al-Saif and Sundus K. Al-Awbaidi, 2004, "Skeleton Generation of a Binary Image Using Thinning, erosion and Pruning Operation", Rafidain Journal of Science, Vol.15, No.1 Comp., math.& Stati., Special Issue.
4. Rafael Gonzales and Paul Woodes, 2005, Digital Image processing, Publisher: Prentice Hall.
5. Robert Fisher, Simon Perkins, 2000, Ashley Walker and Erik Wolfart, "Thinning" Image Processing Learning Resource, HIPR2, Explore with JAVA.