المجلة العراقية للعلوم الاحصائية (9) 2006
ص ص [125-139]

أسلوب جديد لإرسال الرسائل السرية عبر البريد الالكتروني

عامرتحسين سهيل الصميدعي* **معن عبدالخالق يحيى البكوع****

المستخلص

تواجه الرسائل النصية السرية المرسلة عبر البريد الالكتروني مشكلات عدة تتسبب في سرقتها أو افشائها والعبث بمحتواها، عليه برزت الحاجة الى ضـــرورة ايجاد وسائل فاعلة للحفاظ عليها من المهاجمين والمتطفلين، فظهرت تقنية الاخفـــاء لتحقيق ذلك.

اعتمدت الطرائق التقليدية المتبعة، اسلوب اخفاء بيانات الرسالة السرية فـــي الفراغات بين كلمات اوجمل الرسالة الحاملة لها بعد تحويلها الى سلسلة من البتات المقابلة لقيم حروفها، فيتم ترك فراغ او فراغين استنادا الى قيمة البت المراد اخفائه (0 او 1) ، مما يتسبب في تغيير شكل الرسالة الحاملة للاخفاء وحجم الملف.

في هذا البحث تم تطبيق اسلوب جديد مكن من استخدام الفراغات ذاتها دون تلاعب او تزحيف لتمثيل القيمتين (0 او 1) مما حقق كفاءة اعلـــى مـــن الطرائـــق السابقة، من حيث دقة الاخفاء وتعذر ادراكه من قبل المهاجم او المتطفـــل، وذلـــك بسبب المطابقة التامة في شكل وحجم الرسالة الحاملة قبل وبعد عملية الاخفاء.

* مدرس مساعد/ المعهد التقني بالموصل
** مدرس مساعد/ المعهد التقني بالموصل

New Way to Send Secret Messages Through Electronic Mail

ABSTRACT

The secret Electronic Mail messages encounter many problems that causes hacking or modifies it, therefore is necessary to find active ways, to keep it out of hackers and intruders, hiding technique was applied to satisfying that.

The Traditional ways depend on hiding secret message data in between words or statements of carrier message, after dividing its characters values in to sequence of bits, was leaving one or two spaces depending on hided bit value (0 or 1).

In this research, a new concept was applied to create only one space in this two cases, this method carried out higher performance than traditional methods, there is no perceptual hiding for hackers and intruders, and satisfied full matching in figure and size of carrier message before and after hiding.

1 _ المقدمة :

تواجه الرسائل السرية المتداولة عبر البريد الالكتروني مشكلة حقيقية نتيجة لتعرضها للسرقة او العبث في حالة افشاء أو سرقة كلمة المرور السرية الخاصة بالمالكين، أو في حالة تعرض تلك المواقع الخاصة للقرصنة من قبل المهاجمين او المتطفلين، عندها تكون تلك الرسائل في متناولهم. هذا فضلا عن ما يتم التوجه اليه في هذه الايام من محاولة الانظمة والحكومات سن تشريعات قانونية تبيح لها بموجبها الاطلاع على كافة الرسائل الالكترونية والوثائق الشخصية، الخاصة بمواطنيها، المتداولة عبر شبكة المعلومات العالمية (الانترنيت)، وذلك عن طريق الشركات المنتجة لمحركات البحث التي تجهز المستخدم بخدمات البريد الالكتروني، حيث من البديهي ان تمتلك هذه الشركات القابلية على فتح جميع تلك المواقع لقدرتها على اكتشاف كلمات مرورها السرية [1].

ان تطبيق تقنية التشفير على الرسائل السرية تفشل في تحقيق هذه الغاية كونها تقوم بتحويل الرسالة السرية الى نص عشوائي مبعثر، وهذا بدوره يكون

مدعاة للشك والريبة لدى المشاهد ويؤكد احتمالية وجود نص مهم في ذلك المحتوى مما يدفع بالمهاجم لمحاولة فك ذلك التشفير، وفي حالة عجزه عن ذلك يقوم بالعبث به لمنع الجهة ذات العلاقة من الاستفادة منه، او تضليلها بابداله بنص اخر مزيف. وهنا تبرز الحاجة الى ضرورة ايجاد وسيلة فاعلة لارسال الرسائل السرية الخاصة بأسلوب يمنع تلك الجهات من الاطلاع عليها او معرفة مضمونها حتى في حالة فتحها لهذه الرسائل.

الأحبار السرية أسلوب طبق منذ القدم حيث تم استخدام مركبات كيميائية لكتابة الرسائل السرية المهمة والحساسة بين اسطر رسائل أو وثائق غير ذات أهمية بطريقة تكون فيها غير مرئية ويتم استرجاعها فيما بعد من قبل الجهة المستلمة بتعريضها للحرارة أو بوسائل أخرى. وبأسلوب مشابه تم إيجاد وسائل لإخفاء الرسائل النصية المهمة أو الحساسة داخل رسائل أخرى غير ذات أهمية، تعد كأغطية حافظة لها.

2ـ الطرائق الشائعة لارسال الرسائل:

اغلب طرق الإخفاء تقوم بتبديل البت الأقل أهمية (Least Significant Bit :LSB)، حيث يتم تبديله ببت واحد من بتات حرف من حروف الرسالة المراد إخفاؤها، وذلك بعد تحويل تلك الحروف إلى سلسلة البتات المقابلة لها حسب الرمز القياسي الأمريكي لتبادل المعلومات (ASCII) [2] . وهنا لا يمكن استخدام هذه الطريقة لان تبديل البت الاقل اهمية قد يؤدي إلى زيادة أو إنقاص قيمة الحرف بمقدار (1) وهذا بدوره يؤدي إلى تزحيف ذلك الحرف إلى الحرف المجاور له بالقيمة صعوداً أو نزولاً، فمثلاً الحرف (تـ) قيمته (5) وتمثيله بالنظام الثنائي (00000101) وبإبدال البت الأقل أهمية سوف تصبح قيمته (00000100) أي الرقم (4) الذي يقابل الحرف (بـ) وبذلك يتحول النص الحامل للرسالة إلى نص عشوائي وتنتفي الغاية من تقنية الإخفاء. لذلك يتم اللجوء إلى وسائل أخرى وهي استغلال الفراغات بين الجمل والكلمات في النص الحامل

للرسالة، حيث يمثل الرقم (0) بفراغ واحد أما الرقم (1) فيمثل بفراغين، وهكذا لجميع بتات الرسالة السرية الثنائية [2 ،3].

الإخفاء في الفراغ يتم بحشر أجزاء الرسالة السرية في الفراغات الموجودة في الرسالة

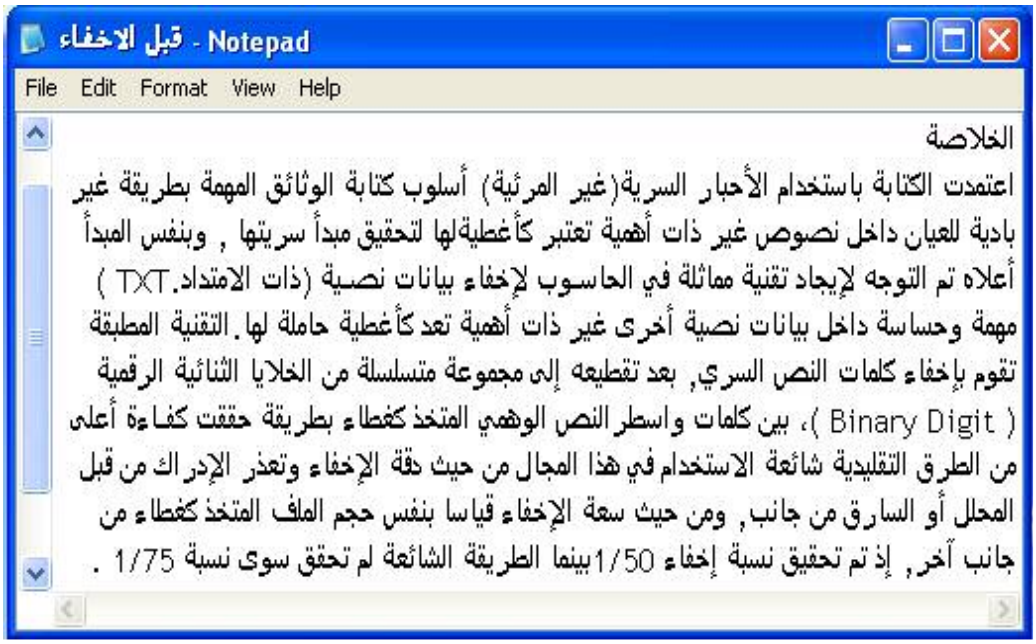
الحاملة، بعد كل جملة من جملها او بعد كل كلمة من كلماتها. أما الإخفاء في كلمات الرسالة فيتم بإرسال رسالة مخفية داخل رسالة أخرى ليست ذات أهمية، وتقوم على فكرة ترشيح أحد حروف كل كلمة من كلمات الرسالة المزيفة لتمثيل حرف من حروف الرسالة السرية المطلوب إرسالها، وهذه الطريقة معقدة جداً وغير عملية من حيث التطبيق في الحاسوب لأنها تتطلب نظام خبير في مجال قواعد اللغة ليتم من خلاله اختيار الكلمة المناسبة وبناء الجملة المطلوبة بطريقة مترابطة، فضلا عن كونها تتطلب قاعدة بيانات ضخمة جداً [4].

الطرائق المطبقة هذه ضعيفة وغير كفوءة لإمكانية ملاحظة التغييرات بالرسالة الحاملة مقارنة بالنص الأصلي، كذلك الزيادة في حجم الملف الاصلي بعد عملية الإخفاء مما يدعو للشك في وجود تغيير بسبب الفراغات الإضافية التي يحشرها، فضلا عن احتمالية تحطم نظام الإخفاء في حالة عرض الرسالة باستخدام أحد التطبيقات الخدمية مثل (word) نتيجة لاحتوائه على بعض المعالجات كالتنسيقات التي تؤدي إلى التلاعب بطول الفراغات بين الكلمات.

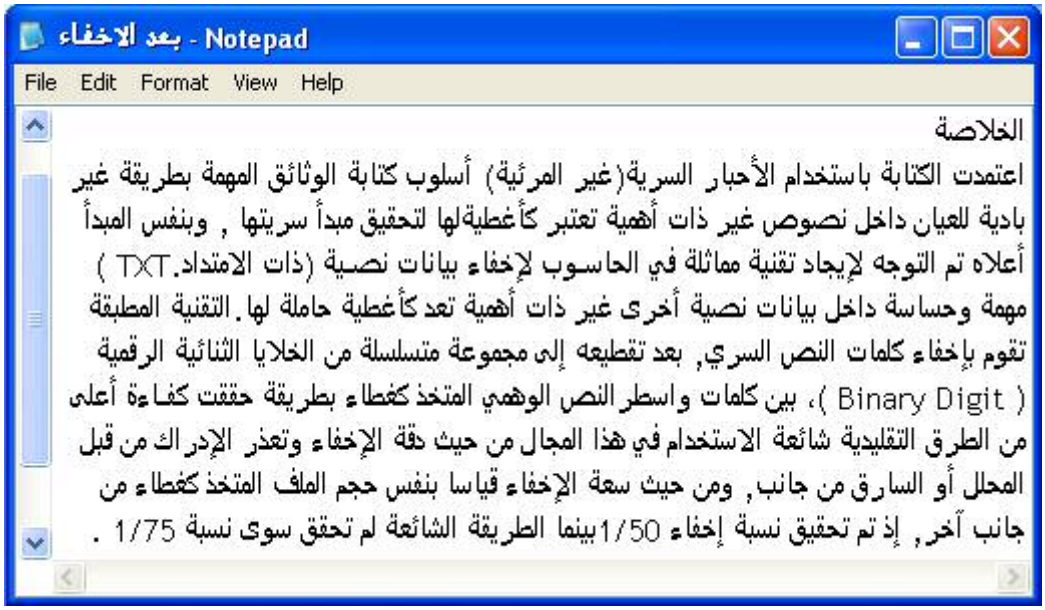
3ـ الاسلوب المطبق :

لتجاوز مشكلة اختلاف عدد الفراغات المتروكة بين الكلمات أو الجمل والمستخدمة في الطرائق التقليدية المتبعة للإخفاء في النص، تم البحث في جدول الرموز القياسية للحاسوب(ASCII) فوجد أن هناك ثغرة مع ملفات النص بالإمكان الاستفادة منها لتحسين الطرائق سالفة الذكر، فبالإضافة الى الرمز القياسي للفراغ وهو(Hexa 20) وجد أن استخدام بعض الرموز في ملفات النص يولد كذلك فراغا، كالرمز(Hexa A0) وهكذا تم اعتماد أحد الرمزين لتمثيل القيمة (0)

والآخر لتمثيل القيمة (1)، وبذلك تم تجاوز مشكلة الاختلاف في الفراغات المتروكة والتي قد يتم تمييزها من قبل المراقب عند مقارنة شكل النص اوحجمه، أما هنا فالرمزان يمثلان فراغاً واحداً فقط، وبالأسلوب الجديد تم التوصل إلى تطابق (% 100) بين النص الأصلي للرسالة الحاملة مع نفس النص الذي يحوي الرسالة المخفية. وكما موضح ذلك في الوثائق النصية بالشكلين(1و2).



الشكل(1) النص المستخدم كغطاء (قبل عملية الإخفاء)



الشكل(2) النص ذاته (بعد عملية الإخفاء)

4_ كيفية الارسال :

لتحقيق عملية الارسال عبر البريد الالكتروني يتم فتح ملف من نوع word بالامتداد (doc.) او من النوع النصي Notepad بالامتداد (txt.)، هذا الملف يحوي الرسالة الحاملة المنتخبة كغطاء للاخفاء وتجرى عليه عملية اخفاء الرسالة السرية المراد ارسالها، وكما مفصل ذلك في خوارزمية الاخفاء في الفقرة (6) من البحث.

عند الانتهاء من عملية الاخفاء يتم استنساخ هذه الرسالة copy ولصقها past داخل المنطقة الخاصة بكتابة الرسالة في صفحة ارسال الرسائل compose، وبعد تحديد عنوان الارسال To وموضوع الرسالة Subject ترسل بتفعيل خيار الارسال send ، والشكل (3) التالي يوضح صفحة الارسال في محرك البحث YAHOO.

الشكل (3) صفحة ارسال الرسائل الالكترونية في محرك البحث YAHOO

5ـ تقييم الاسلوب المطبق :

أولا: إن حجم صفحة النص العربي القياسية هي بالأبعاد (30) سطراً، وكل سطر يحوي (80) حرفاً، وأن معدل طول الكلمة في هذا النص ستة احرف ، أي خمسة احرف والفراغ الفاصل بين كلمة وأخرى، هذا يعني أن عدد الفراغات الموجودة في الصفحة هو (400) فراغاً، ولكون إخفاء الحرف الواحد يتطلب ثمانية فراغات، فان عدد الحروف الممكن إخفاؤها في كل صفحة هو (50) حرفا [5 ،6]. على سبيل المثال بالإمكان إخفاء الرسالة التالية في صفحة قياسية من النص : (**سيبدأ ارسال الوثائق على موقعنا الساعة الواحدة ليلاً**).

ثانيا: غالباً ما يكون حجم ملف الرسالة المنتخبة كغطاء اكبر من الحجم المطلوب لإخفاء الرسالة السرية، هذا يعني بقاء مساحة من ملف الغطاء دون استخدام، وعند فك الإخفاء سوف تكون قيم جميع هذه الفراغات (20H)، وبتجميعها إلى بايتات لتحويلها إلى الرمز المقابل سنجد أنها تقابل الرمز ذو القيمة (00H) أو الرمز المقابل للقيمة (FFH)، هذا اعتماداً على خوارزمية التمثيل عند الإخفاء للقيمتين (1 او 0)، على أن هذه المشكلة من الممكن تجاوزها، لسهولة معرفة أن النص انتهى مع تكرار هذا الرمز، أما المشكلة الأهم فهي عدم توقف عملية فك الإخفاء لحين انتهاء حجم ملف الغطاء، لذلك يمكن وضع بايتين عند بداية الإخفاء لتمثيل حجم ملف الإخفاء، يسبقها وضع رمز خاص بطول بايت يمثل مفتاح الإخفاء، يتم الاتفاق عليه بين المرسل والمستقبل.

ثالثا: لكون حجم المساحات الممكن استخدامها للإخفاء قليلة في ملف الرسالة النصية، فمن غير المنطقي استخدامها لإخفاء ملف صورة أو صوت لكبر حجم هذين النوعين من الملفات. وعلى الرغم من ذلك فانه بالإمكان استخدامها كأغطية لإخفاء الصور أو المخططات ثنائية اللون (Mono)، حيث يتم تمثيل كل خلية صورية ببت واحد فقط، فاللون الأسود يمثل بالقيمة (0) واللون الأبيض يمثل بالقيمة (1). وبما أن بادئة الملف لهذا النوع من الصور قياسية عدا اختلاف البعدين بين صورة وأخرى، والحجم الذي يتم حسابه منهما، لذلك من الممكن تجاوزه والاكتفاء بإخفاء قيم خلايا الصورة فقط، أما أبعاد الملف فيمكن حشرها عند بداية الإخفاء وذلك بتمثيل كل بعد ببايت واحد فقط والتي يمكن أن تمثل أعلى قيمة (255).

ولما كان عدد الفراغات في الصفحة القياسية (400) فراغاً، فانه بالإمكان استخدامها لإخفاء ملف صورة ثنائي اللون بأبعاد (19*20) خلية صورية أو ما يعادلها فضلاً عن قيم بعدي الصورة. أما إن كان حجم الصورة اكبر من ذلك فبالإمكان إخفاؤها في أكثر من صفحة.

6- خوارزمية التطبيق :

إن خوارزمية الإخفاء في النص يجب أن تسبقها مرحلة فحص حجم كل من ملف رسالة الغطاء وملف الرسالة السرية المطلوب إخفاؤها، وبيان مدى تحقيقهما للشرط المطلوب. فان كانت الرسالة المراد اخفاؤها نصية فانه يجب أن تحقق العلاقة التالية:

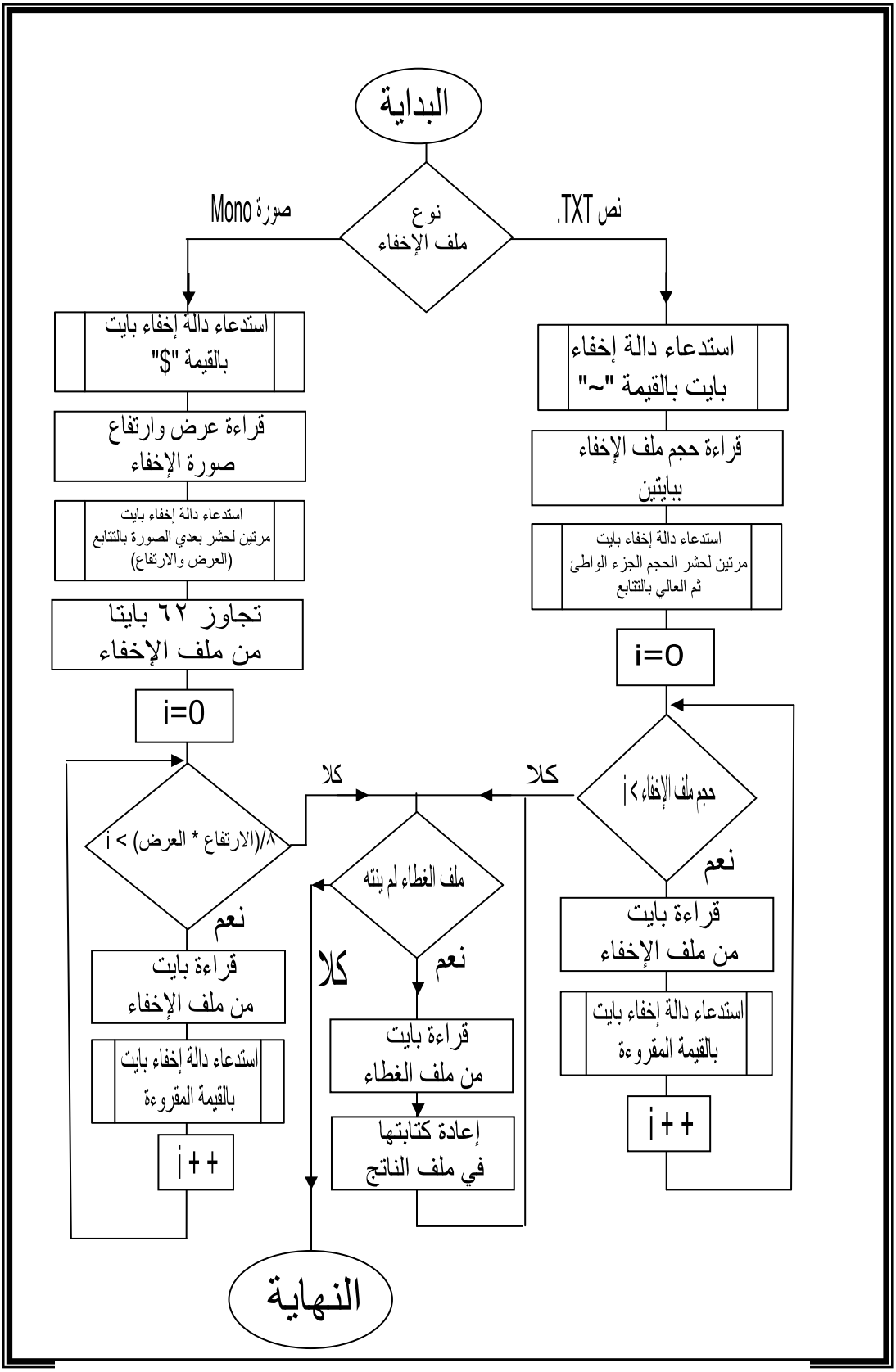
{ حجم ملف الغطاء \ (8*6) }>= { حجم ملف الاخفاء +2+1} .....(1)

أي قسمة حجم ملف الغطاء على معدل طول الكلمة مضروب بعدد البتات المطلوبة لتمثيل كل حرف، والرقم الناتج يمثل عدد الحروف الممكن إخفاؤها في هذا الملف، هذا الحجم يجب أن يكون اكبر أو يساوي حجم ملف النص المراد إخفاؤه مضافاً له القيمة (2) التي تمثل البايتين المستخدمتين لخزن حجم ملف الإخفاء إن كان نصاً، أو بعديه إن كان صورة ثنائية، أما الرقم (1) فيمثل كتلة ثمانية لخزن الرمز المتفق عليه كمفتاح بين المرسل والمستقبل.

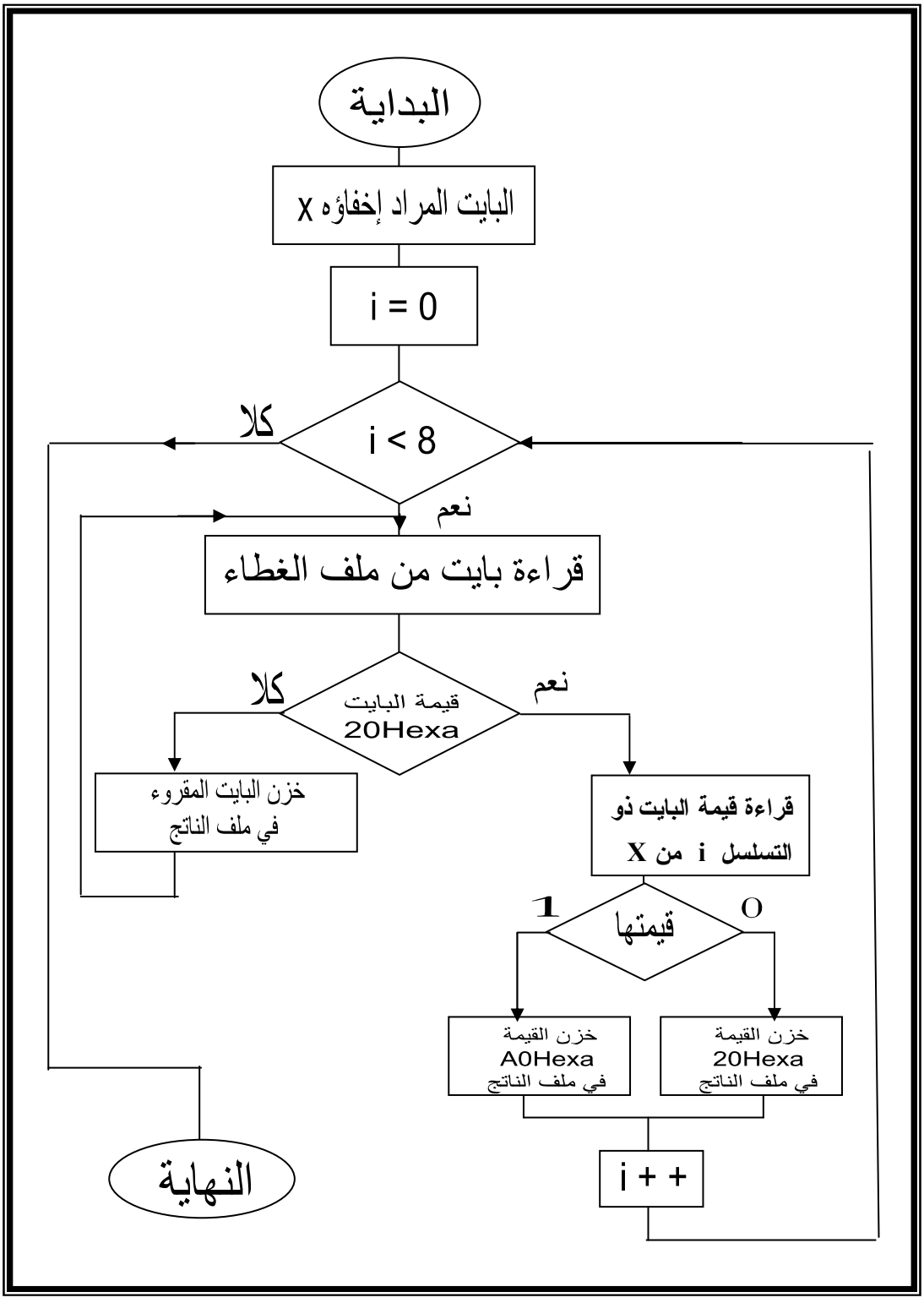
أما إن كان الملف المراد إخفاؤه صورة ثنائية اللون فان الشرط المطلوب تحقيقه، نفس العلاقة في اعلاه سوى أننا نقوم بطرح الرقم (62) من حجم ملف الاخفاء التي تمثل بادئته.

في حالة نجاح شرط الحجم المبين في أعلاه فان عملية الإخفاء يوضحها المخطط الانسيابي المبين في الشكل (4). ودالة الإخفاء التي يتم استدعاؤها عند كل بايت يمكن ايضاحها في المخطط الانسيابي في الشكل (5).

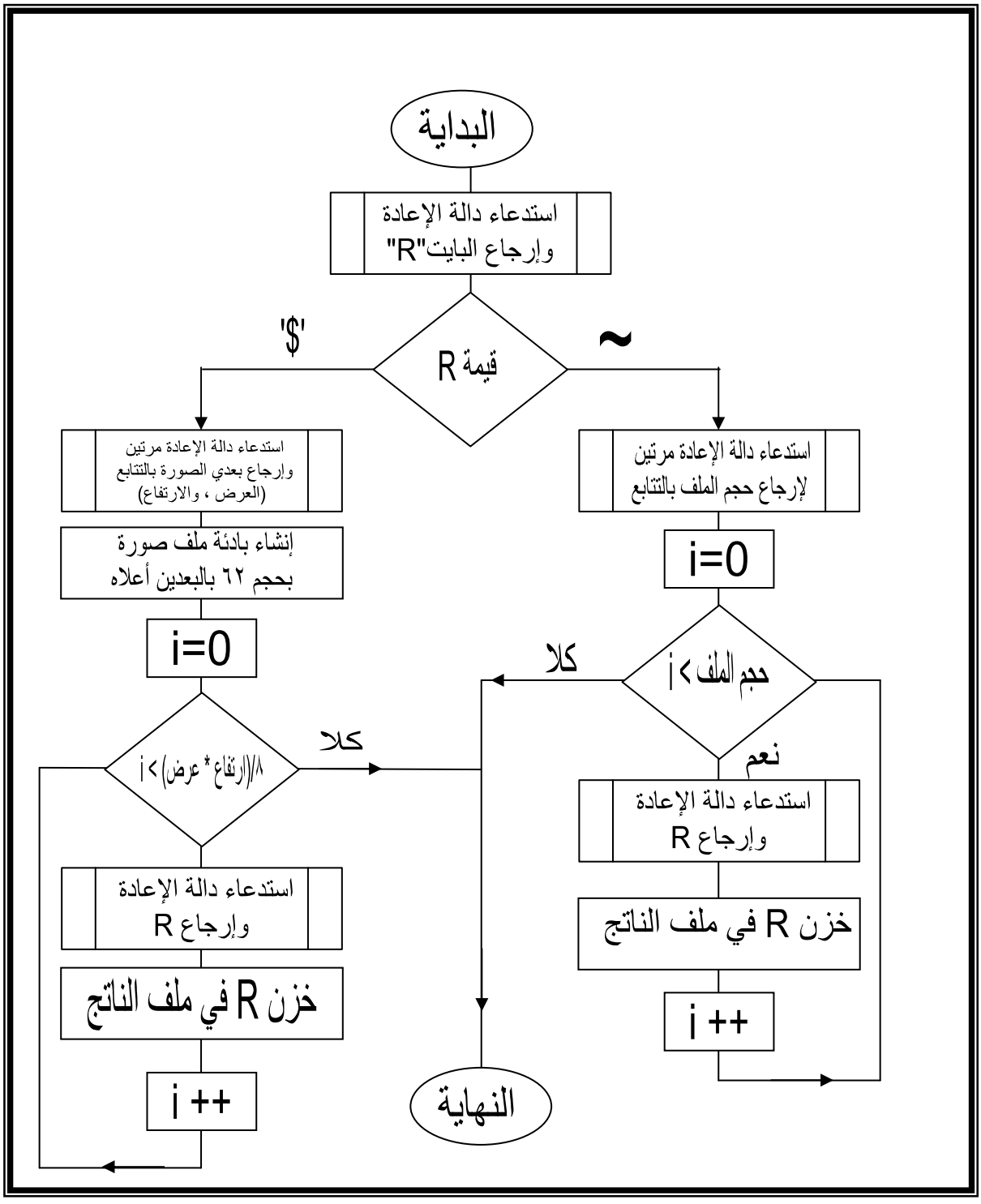
أما عملية فك الإخفاء فإنها تمر بالخطوات التي يوضحها المخطط الانسيابي بالشكل (6). ودالة الإعادة التي يتم استدعاؤها ضمن خوارزمية فك الإخفاء تقوم باستعادة بايت واحد من الملف الحامل عند كل عملية استدعاء، وكما موضح ذلك في المخطط الانسيابي بالشكل (7).



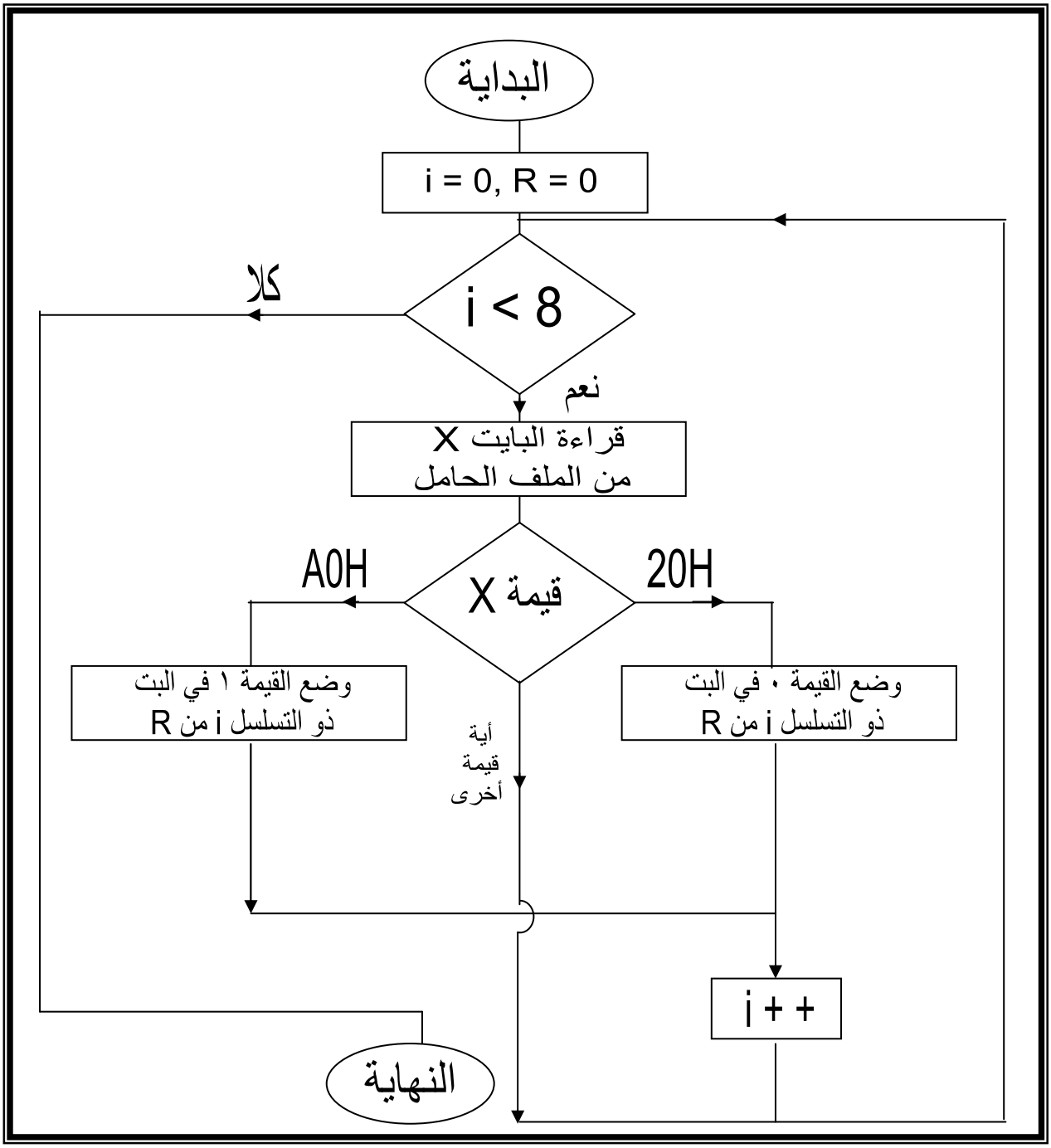
الشكل (4) مخطط انسيابي يمثل عملية الإخفاء في النص



الشكل (5) مخطط انسيابي يمثل دالة إخفاء بايت في ملف



الشكل (6) مخطط انسيابي يبين عملية فك الإخفاء في ملفات الرسائل



الشكل (7) مخطط انسيابي يوضح عمل دالة إعادة بايت من ملف النص

7- النتائج :

في الأسلوب الجديد تم تحقيق الاتي:

1_وجود حالة تطابق تامة في شكل الرسالة الحاملة مقارنة مع شكلها قبل الاخفاء، بينما في الطرائق الشائعة يتم تغيير شكل تلك الرسالة بسبب اعتمادها اسلوب التزحيف، وبالتالي تتغير مواقع الفراغات فتنتفي حالة التطابق.

2_ صعوبة امكانية اكتشاف الرسالة السرية من قبل المهاجمين لعدم حصول حالة التلاعب في هيئة الرسالة الحاملة للاخفاء كما يحصل في الطرائق التقليدية.

3_ حجم الملف الحامل للرسالة لم يتم التلاعب به حيث يبقى ثابتا بعد الإخفاء قياسا بما هو عليه قبل الإخفاء، وهذه الحالة لايمكن تحقيقها في الطرائق الشائعة بسبب الفراغات المضافة لتمثيل قيمة البتات المطلوب اخفاؤها.

4_ على الرغم من صغر حجم الصورة ثنائية اللون الممكن اخفاؤها في هذه الطريقة، الا انها اكبر مما يمكن اخفاؤه في الطرائق الشائعة، لاستغنائها عن الحاجة الى خزن بادئة الملف البالغ حجمها (62) بايتا،

الاستنتاجات:

1_ هذه الطريقة تكون اكفأ من عملية اخفاء الرسالة السرية داخل ملفات الصوراو الاصوات، كون تلك الملفات تتطلب احجام خزن كبيرة، لذا تكون عملية ارسالها كملفات مرفقة (Attach File) بطيئة.

2_ الطريقة مقاومة لعمليات العرض المختلفة للنصوص باستخدام برامج المكتب.

3_ امكانية استخدام هذه الطريقة لارسال المخططات ثنائية اللون صغيرة الحجم.

المصادر

[1] Provos, N.; Honyman, P., " Detecting Steganographic content on the Internet", august 2001, http://www.citi.umich.edu/techreports/citi_tr_01-11.pdf

[2] Silman, J.,"Steganography and Steganalysis: An overview", ***SANA Institute, Information security reading room***, august 2001.

[3] Artz, D., "Digital Steganography: Hiding Data within Data", ***IEEE Internet Computing***, vol.05, May-June 2001, pg.75-80.

[4] Schmidt, M.B.; Bekkering, E.; Warkentin, M., " On the Illicit use of Steganography and its Detection " , ***proceeding of the 2004 world Informational conference***, April 2004 , Las Vegas, NV.

[5] Wanas, M.; El_Sakka, M.R.; Kamel, M.S.," Multiple Classifier Hierarchical Architecture for Hand Written Arabic Character Recognition", ***IEEE Internet Computing***, vol.03, June 1999, Pg. 2834-2838.

[6] Trenkle, J.; Erlandson, E.; Gillies, A.; Schlossber ,"Arabic Character Recognition ", ***Environmental Research Institute of Michigan*** , Ann Arbor,1995 , MI 48113_4001.