جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل _ كلية التربية للعلوم الصرفة
قسم الرياضيات

LOGO.ADAM96.COM

اخفاء البيانات في الصور

مشروع بحث مقدم الى مجلس كلية التربية للعلوم الصرفة _ قسم الرياضيات

كجزء من متطلبات نيل درجه البكالوريوس في الرياضيات

من قبل الطالبة

هدى نعيم محمد عبد الرضا

بأشراف

أ.م.د لميس حمود محيسن

بدسم الله الرحمن الرحيم

قال تعالى :

(فتعالى الله الملك الحق ولا تعجل بالقران من قبل ان يقضى اليك وحيه وقل ربي زدني علما)

صدق الله العلي العظيم

(سورة طه الاية ١١٤)

الاهداء

الى من كان لهم الفضل بعد الله في مسيرتي

الى امي الغالية ، نبع الحنان والعطاء التي كانت دعواتها ترافقني في كل خطوة فكانت سببا في نجاحي

الى ابي العزيز السند والقوة الذي علمني الصبر والاجتهاد وكان دائما الداعم الاول لي

الى زوجي شريك حياتي الذي وقف بجانبي وساندني بكل حب وكان طمأنينة وتشجيع

الى كل من دعمني وساعدني ولو بكلمة طيبة اهدي هذا الجهد المتواضع راجيا من الله ان يكون ثمرة خير وفخر لي ولهم

الشكر والتقدير

الحمد لله حمدا يليق بجلاله و الشكر له على توفيقه و امتنانه ، فالحمد لله الذي هدانا للاسلام و ارشدنا للعلم و وفقنا للخير و الشكر لله سبحانه ان من عليه بتمام هذه الدراسة ، و الصلاة و السلام على نبينا محمد و على الة الطيبين الطاهرين

فالشكر بعد شكر الله تعالى و الى كل من ساعدني و لمن كانت له اليد في انجاز هذا البحث و اختص بالذكر

(الدكتورة : لميس حمود) المشرفة على هذا البحث

كما لا يسعني الا ان اتقدم بجزيل الشكر و وافر التقدير للاساتذة في قسم الرياضيات على ما قدموه لي من توجيه و ارشاد في جميع مراحل الدراسة

الخلاصة

تقنيات التشفير لها تطبيقات واسعة جدا في مجال الحاسوب او لمجالات اخرى ذات الصلة الا انها تستخدم لحماية رسائل بريد الكتروني و معلومات بطاقة الائتمان و امنية بيانات

الاخفاء بحد ذاته فن و علم للتواصل بطريقة تخفي وجود اتصال و بطريقة تضمن ارسال المعلومات عبر وسائل الاتصالات و يضمن بالتالي ارسال محتوى الرسائل عبر وسائل العالم في تغطية تثير شك المتصنت غير المخول ، مثال ذلك من الممكن تضمين نص داخل صورة او ملف صوتي

التشفير هوة دراسة التقنيات الرياضية المتعلقة ب امنيه المعلومات لضمان سالمة البينات التشفير

التشفير يحمي المعلومات عن طريق تحويلها الى رموز و شفرات تكون غير مفهومة للمتصنت حتى ولو استطاع سرقتها اذ انها تظهر له بشكل غير قابل للقراءة

جدول المحتويات

الفصل الاول

١-١ المقدمة

مع التطور السريع في تقنيات الاتصالات وانتشار شبكة الانترنيت، أصبح تبادل الصور الرقمية جزءًا أساسيًا من حياتنا

التجارية أو عبر وسائل التواصل الاجتماعي هذا ، سواء في المجالات الطبية أو العسكرية أو اليومية

الانتشار الواسع للصور الرقمية صاحبه تزايد في المخاطر الامنية، مثل التلاعب بالصور أو سرقتها أو

الطالع غير المصرح به عليها، مما جعل مسألة حماية الصور . والمحافظة على سريتها أمرًا بالغ الاهمية

يعد تشفير الصور أحد أهم أساليب أمن المعلومات، إذ يهدف إلى تحويل الصورة الاصلية إلى صورة غير

مفهومة ال يمكن تفسيرها أو الاستفادة منها إلا من قبل الاشخاص المخولين الذين يمتلكون مفتاح فك التشفير.

وتعتمد تقنيات تشفير الصور على خوارزميات رياضية ومنطقية معقدة تضمن السرية وسالمة البيانات أثناءالتخزين أو الارسال

يسلط هذا البحث الضوء على مفهوم تشفير الصور، وأهميته، وأنواعه، إضافة إلى استعراض بعض

الخوارزميات المستخدمة في هذا المجال، مع بيان مزاياها وتحدياتها. كما يهدف البحث إلى توضيح دور

الخصوصية في العصر الرقمي الحديث. تشفير الصور في تعزيز أمن المعلومات وحماية

التشفير وإخفاء المعلومات هي تقنيات شائعة وواسعة لمعالجة المعلومات رسائل) من أجل

تشفيرها وإخفاء وجودها.

من ناحية أخرى ، التشفير هو دراسة التقنيات الرياضية المتعلقة

استطاع سرقتها اذ انها تظهر له بشكل غير قابل للقراءة.

تصنف نظم التشفير الى انواع حسب عدد مفاتيح التشفير المستخدمة ومدى سريتها، حيث هناك

خوارزميات

ًتشفير تعتمد على مفتاح واحد (Symmetric key). واخرى تعتمد بين المرسل و المستلم ويكون سريا على مفتاحين الاول عام و الثاني

اخفاء لمعلومات أهمية كبيرة وذلك الن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عامل

مساعد على إضفاء حمايةً امنا على معلومات. يستخدم الخفاء في العديد من المجالات، وخاصة في

التجارة

الكترونية التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد آخر. وعلى افت ارض أن المستخدم يتوقع وجود نص ما مخفي

فسيظهر أمامه تحدٍ آخر، وهو معرفة الطريقة المستخدمة في الخفاء و كلمة السر ومفتاح التشفير،

وكل

من هذه الاشياء قد يستغرق اكتشافه وقتاً زمنيا طويلا

عُني النسان منذ القدم بتصنيف المعرفة، وبذل الفلاسفة والمفكرون جهود اًلوضع نظم لهذا التصنيف،

فالتصنيف في اللغة هو تمييز الاشياء بعضها عن بعض وهو أيضا ترتيب الاشياء في أصناف أو أقسام،

وإذا

النقاط ضمن مجموعة معينة أكبر من التشابه بين نقطتين ضمن مجموعتين مختلفتين. فكرة تجمع البيانات

هي فكرةٌ .يمكن تعريف التصنيف بأنه عملية تقسيم مجموعة من البيانات إلى عدة مجموعات. اذ أن التشابه

بين

بسيطة في طبيعتها وهي قريبة جدا من الانسان في طريقه تفكيره حيث اننا كلما تعاملنا مع كمية كبيرة من

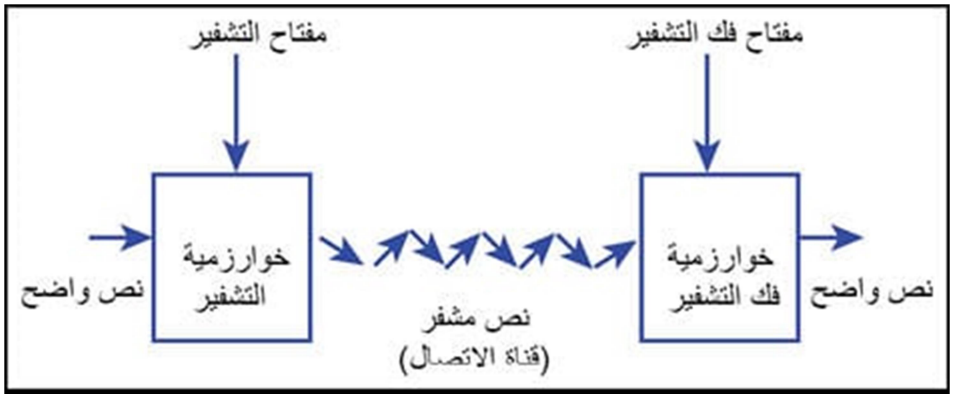
البيانات

نميل إلى تلخيص الكم الهائل من البيانات إلى عدد قليل من المجموعات والفئات، وذلك من اجل تسهيل

عمليه

التحليل. خوارزميات التجميع تستخدم على نطاق واسع ليس فقط لتنظيم وتصنيف البيانات وانما هي مفيدة

[3]



١-٢ الهدف

يهدف هذا البحث إلى دراسة تقنيات تشفير الصور الرقمية وبيان دورها في حماية الصور من الوصول غير

المصرح به، وضمان سرية المعلومات والمحافظة على سالمتها أثناء التخزين أو الارسال عبر شبكات

الاتصال. كما يسعى البحث إلى تحليل ومقارنة بعض خوارزميات تشفير الصور من حيث مستوى الامان

والكفاءة وسرعة التنفيذ، وإبراز أهم التطبيقات العملية لتشفير الصور في المجالات المختلفة مثل الطب

والاتصالات والامن المعلوماتي.

التعرف على مفهوم تشفير الصور الرقمية وأهميته في مجال أمن . المعلومات

دراسة أنواع وأساليب تشفير الصور المستخدمة في الانظمة الحديثة.

تحليل آلية عمل بعض خوارزميات تشفير الصور وبيان خصائصها . الاساسية

مقارنة خوارزميات تشفير الصور من حيث مستوى الامان وسرعة التنفيذ وكفاءة الاداء

توضيح دور تشفير الصور في حماية البيانات الرقمية أثناء الارسال . عبر الشبكات

إبراز التطبيقات العملية لتشفير الصور في المجالات الطبية . والعسكرية والتجارية

المساهمة في زيادة الوعي بأهمية حماية الصور الرقمية من . الاختراق والتلاعب

علم التشفير والاخفاء هما طريقتان لحماية المعلومات من عرضها والعبث بها من قبل الاشخاص الغير

المخولين

لكن كال من الطريقتين لو استخدمت لوحدها، قد ال تعد وسيلة حماية كافية وكاملة. بالنسبة الاخفاء ،المعلومات

مثال ، حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما، فإن الهدف من عملية

الاخفاء يصبح بال قيمة! لذا فإنه ولزيادة حماية المعلومات المخفية يجب علينا استخدام تقنيتي حماية المعلومات التشفير و الاخفاء

يهدف البحث الى تطبيق خوارزمية امنية تحافظ على سرية النصوص المرسلة داخل صورة غطاء عن طريق

تشفير النص وبعثرته داخل الصورة بطريقة التصنيف.

يتكون البحث من مجموعة من الفقرات الاساسية والتي تضم فقرة الدراسات السابقة وفقرات توضيح

[4]

الفصل الثاني

٢-١ خوارزمية التصنيف

التصنيف هو طريقة لتجميع البيانات المتشابهة في مجاميع أو

اصناف مختلفة وكل مجموعة البد أن تكون
متشابهة او لمجاميع المختلفة البد أن تكون غير حاويةٍ على
.بيانات مشتركة
من اهم تقنيات التصنيف وأكثرها K-means تعد طريقة
J. M aqueen فعالية اكتشفها سنة ١٩٦٧ العالم
وهي تعد طريقة بدون اش ارف، إذ تعطى مجموعة من القيم
من الاصناف، وتستعمل K وتحاول تجزئتها إلى
خوارزمية تكرارية لتقلل مجموع المسافات المربعة من الكيان
K– إلى مركز الصنف. واكثر تطبيقات خوارزمية
اذ تقوم بتقسيم processing image في معالجة الصورة
الصورة الى مجموعة الاصناف المكونة لها ومشكلتها انها
تحتوي على حسابات كثيرة. ولغرض تطبيق خوارزمية
على الصور يتم تطبيق خوارزمية التصنيف means-K
على الصور تكون نتيجتها تجزئة القيم اللونية
نفرض أن عدد 2. .الى عدد من المجاميع أو الاصناف
ولذلك فان كل نقطة من الصورة تعطى إلى , K الاصناف هو
واحدة من المناطق بالاعتماد على قربها من القيمة اللونية
الصورة الناتجة تكون على 3. .التي تمثل مركز الصنف
من القيم اللونية وهذا مشابه لتجزئة الصورة إلى K أساس
يتم اختيار أحسن 4. .من عتبة القيم اللونية K,...1,2,
الاصناف لتقسيم الصور هو الذي يمتلك أقل مربع خطأ

والمعرف بالشكل هي الاصناف (Error Square Least)
الجيدةً فإن أقل

[2]

٢-٢- خوارزمية تشفير البيانات القياسية الثلاثية

لقد Data Encryption Standard DES (من قبل فريق
(وضعت طريقة تشفير البيانات القياسي
بت، خوارزمية تشفير البيانات القياسية ٥٦ والذي اعتمد على
مفتاح بطول ١٩٧٤ شركة آي بي إم حوالي عام
الث مرات من خوارزمية تشفير البيانات القياسية العادية ولكنها
اكثر باليين المرات أمانا إذا تكون ابطأ ث الثالثة
أوسع بكثير من ما استخدمت بالشكل الصحيح. استخدمت
خوارزمية تشفير البيانات القياسية الثالثة على نطاق
خوارزمية تشفير البيانات القياسية وذلك لسهولة كسر الخيرة
مع التقدم السريع للتكنلوجيا
بت اي ان ٦٤ هي طريقة لتشفير البيانات تستخدم ثالثة مفاتيح
خوارزمية تشفير البيانات القياسية الثالثة

بت. طريقة التشفير ٦٤ ثالثة مفاتيح كل منها مكون من بت،
يقسم المفتاح المدخل الى ١٩٢ طول المفتاح الكلي
في هذه الخوارزمية هي نفسها الطريقة المستخدمة في
الخوارزمية العادية ولكنها تكرر ثالث مرات حيث يتم تشفير
البيانات بالمفتاح الاول ثم التشفير بالمفتاح الثاني ثم التشفير
، يمثل y ، النص المشفر k و k١ و k٢ بالمفتاح الثالث ٣
x النص الصريح

بناء على ذلك، يعمل تشفير البيانات القياسية الثلاث ثالث مرات
القياسية، ولكن هي أكثر DES أبطأ من

أمنا إذا ما استخدمت بالشكل الصحيح. ان إجراءات فك الشفرة هي نفسها إجراءات التشفير، باستثناء انه يتم
تنفيذها في التجاه المعاكس
هو DESمن المهم الشارة الى انه بالرغم من أن مفتاح الدخال لـ بطول ٦٤ بت، والمفتاح الفعلي المستخدم
هو فقط ٥٦ بت في الطول. حيث البت القل اهمية DES من قبل أقصى اليمين في كل بايت هو بت التماثل
، ويجب ان يكون اوحداً للدلالة ان هناك دائما (Parity bit) عدداً فردياً من ١ في كل بايت، يتم عادة تجاهل هذه
البت في التشفير لهذا فقط ٧ بت من البايت هي التي يتم استخدامها فعال وعليه يكون طول المفتاح هو ٥٦ بت
فقط. هذا يعني أن المفاتيح الفعالة الرئيسية لخوارزمية تشفير البيانات القياسية الثالثة في الواقع ١٦٨ بت
ألن كل واحد من المفاتيح الثالثة يحتو ي على ٨ بت التكافؤ ال يتم استخدامها أثناء عملية التشفير
[1]

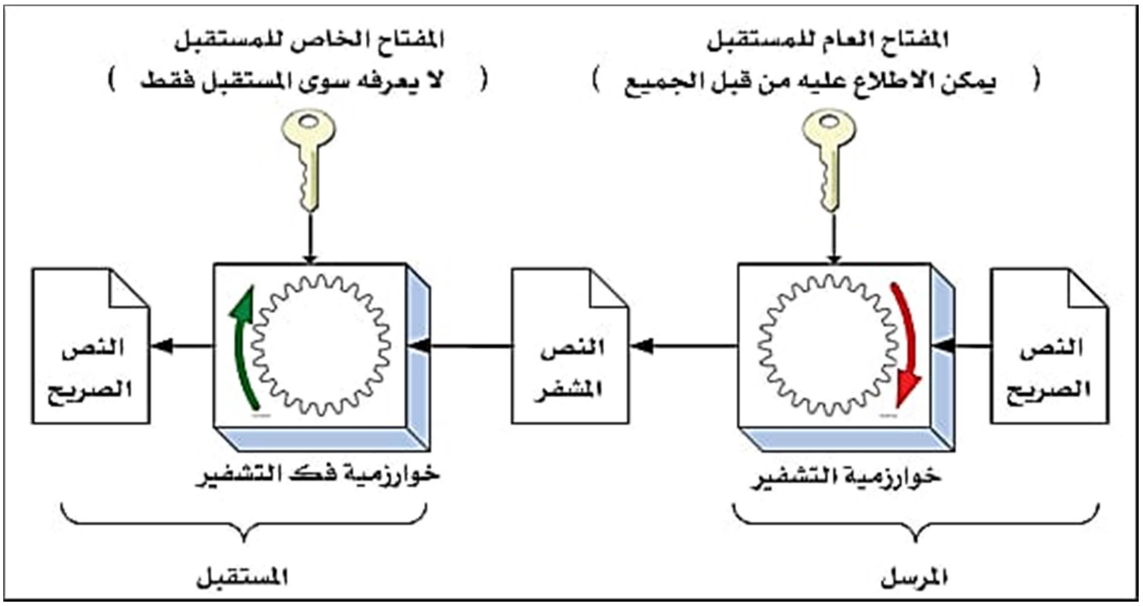
٣-٢- خوارزمية المقترحة

تم في هذا البحث تصميم خوارزمية امنية تتكون من مرحلتين رئيسيتين مرحلة التشفير والخفاء يطبقها
المرسل وهي خوارزمية التشفير والتضمين والثانية يطبقها المستلم وهي خوارزمية الاسترجاع والحصول على النص الصريح

[2]

٤-٢- مرحلة التشفير والتضمين

يتم في هذه المرحلة اجراء المعالجة الاولية لكل من النص والصورة)الغطاء(حيث يتم تطبيق خوارزمية تشفير البيانات على النص لغرض تشفيره وكذلك معالجة DES3 القياسية الثالثة للتصنيف عليها means-kالصورة الاولية بتطبيق خوارزمية واختيار عدد اصناف عشوائي بعد اجراء دراسة على عدد كبير من الاصناف ثم يتم بعد ذلك اختيار الصنف الكبر عددا من الوحدات الصورية والتي يستبدل كل بايت منها ببايت من النص المشفر اي ان عملية الاخفاء سوف تتم لكل القيمة اللونية)٢٤ بت(من الصورة الاصلية قبل التصنيف وب احداثيات الاصناف الاكبر عددا من القيم وبترتيب تنازلي مع اخفاء مفاتيح التشفير وطول النص المشفر، و في حالة كون طول النص اكبر من عدد قيم الصنف الاكبر يتم اختيار الصنف التالي)الاقل (ف الاقل عددا من القيم وهكذا الى ان ينتهي النص، يتم بعد ذلك ارسال الصورة الناتجة، والشكل رقم)٤(يوضح المخطط الانسيابي لمرحلة التشفير والتضمين في الخوارزمية المقترحة.



[3]

٥-٢- خوارزمية القسمة

و هي أحد الخوارزميات المهمة جدا، حيث تقول انه مكننا أن نمثل أي عدد صحيح ، وذلك بواسطة ضرب

بحيث يكون الباقي عدد موجب r مع اضافه باقي b عدد صحيح b . وأقل من العدد

أكبر من صفر، إذا b ، وكانb,y إذا كان لدينا عددين صحيحين : بحيث r,q سيكون لدينا عددين

Y=b*q+ r

q هي حاصل القسمة r . Quotient هي الباقي b .
remainder هي المقسوم Divisor .
Y القاسم هو dividend [2].
مثال لدينا المعادلة:

65 = 3*q + r

هو r هي ٢١) وذلك بقسمة ٦٥ على ٣(، والباقي q قيمة ال
٢.

65 = 3*21 +2

[2]

٢-٦ الخوارزمية الاقليدية الممتدة

يمكن تمثيل القاسم المشترك الاعظم للعددين عن طريق دمج خطي مع عددين اخرين
وذلك كالتالي :

GCD(X,Y)=m*x+ n*y

هناك طريقتين لمعرفة هذه القيم (الطرق هيه مشابهه لبعض، لكن يمكن القول انها مختصره من الاخريات)
الطريقة الاولى : وهيه يمكن ان نطلق عليها التراجع وهنا في هذه الطريقة نقوم بالحل عن طريق خوارزمية اقليدس وبعدها نقوم بالتراجع الخلفي لايجاد القيم

مثال : قم بتمثيل
Linear combination GCD(26,21)
نبدا في الحل كما هو الحال في طريقة اقليدس .
٢٦=١*٢١+٥
٢١=٤*٥+١
٥=٥*١+٠
ونتوقف عند الصفر
الان المعادلة التي قبل المعادلة التي باقي لها صفر (وهي في حالتنا هذه المعادلة الثانية)
نقوم بكتابتها بهذا الشكل .
(١).....١=٢١-٤*٥
وايضا المعادلة الاولى بنفس الشكل
(٢).....٥=٢٦-١*٢١
الان نعوض المعادله ٢ في ١
١=٢١-٤*(٢٦-١*٢١)
ومن غير اجراء عمليه حسابيه فقط نفك القوس لينتج :
١=٢١-٤*٢٦+٤*٢١
نجمع ٢١ +٤*٢١ ليكون لدينا الناتج النهائي :
٢٦*(-٤)+٥*٢١ والناتج يساوي واحد اذا المعادله صحيحه.
الطريقة الثانية :
وهي اسهل واسرع بكثير وسوف نشرحها بنفس المثال السابق
مثال قم بتمثيل

Linear combination GCD (26,21)

نقوم في البدايه بانشاء جدول ونضع هذه القيم فيه

A	Q	X
26		
21		

الان نبدا في اخذ باقي قسمة ٢٦ على ٢١ والناتج نضعه في نفس العمود اسفل ٢١

26 MOD 21 = 5

ونضع ٥ اسفل ٢١

مره اخرى ناخذ باقي قسمة ٢١ و ٢٥ والنتاج نضعه اسفل ٥ وهو ١

والمره الاخيره الباقي هو صفر

وسوف نتوقف عنده

A	Q	X
26		
21		
5		
1		

0		

الان نقسم ٢٦ على ٢١ ونضع الناتج في العمود
Q
(بدا من الصف الثاني والناتج هو عدد كسري لكن نحن سوف ناخذ الجزء الصحيح وهو واحد ايضا نقسم ٢١ على٥
والناتج الصحيح هو ٤ ونستمر هكذا

A Q X

26		
21	1	
5	4	
1	5	
0		

الان في العمود اكس نقوم بوضع اخر قيمتين هن الصفر و الواحد كما في الشكل :

A Q X

26		
21	1	

5	4	1
1	5	0
0		

الان لكي نحسب الصف الثاني في العمود اكس نقوم بالتالي

٤*١+٠=٤

اي سنضرب القيميتين التان يقعان في الصف الاسفل مباشرا ونجمع الناتج مع القيمة في العمود اكس التي تاتي بعد الصفين

٠+١*٤=٤

A Q X

26		
21	1	4
5	4	1
1	5	0
0		

نفس الامر مع السطر الاول :

١+١*٤=٥

A Q X

26		5
21	1	4
5	4	1

1	5	0
0		

الان الخطوة الاخيرة :

A	Q	X
26		5
21	1	4

٢٦*٤-٢١*٥=١

٢٦*(-٤)+٢١*٥=١

وبهذا نكون عرفنا معكوس العدد الاول والثاني

(m,n)

[2]

٧-٢- الاعداد الاولية

تلعب الاعداد الاولية دورا كبيرا جدا في التشفير و خاصة في الطرق الحديثة، و تعريفها كالتالي:

العدد الاولي: هوه العدد الصحيح اكبر من ١ و لا يقبل القسمة الا على نفسة و على ١ باقي الاعداد التي اكبر من ١ و غير اولية تسمى اعداد مركبة

مثال على الاعداد اولية :

٢,٣,٧,٢٣,٢٩,١٦٣ و الكثير غيرها

مثال على اعداد مركبة :
٤(حيث انها تقبل القسمة على ٢)
١٠٠ (تقبل القسمة على ٢ و ٥)

مثال على اعداد غير اولية و غير مركبة
٠ و ١ و جميع الاعداد السالبة

جميع الاعداد الصحيحة التي اكبر من ١ ، و لها قاسم اولي الاعداد الاولية غير منتهية .
إذا كان لدينا عدد صحيح مركب اذا يكون لدى قاسم اولي لا يتعدى الجذر التربيعي ل
و هذا معناه اذا اردنا ان نعرف على العدد هوه اولي ام لا ، سوف نبحث من البداية على ٢ (لان واحد ليس اولي) الى ان نصل الى جذر العدد . و نختبر كل عدد من هذه الاعداد ، هل يقبل القسمة عليها، في حال تحقق ذلك ، نكون قد عرفنا ان العدد ليس اولي ، و اذا لم يتحقق فيكون العدد اولي.

مثال : لدينا العدد ١٠١ ، نبدا بالاختبار من ٢ ، الى جذر ١٠١ و هوه ١٠

هل ١٠١ يقبل القسمة على ٢. لا
هل ١٠١ يقبل القسمة على ٣. لا
هل ١٠١ يقبل القسمة على ٤ و ٥ و ٦و ٧و ٨و ٩. الى ان نصل الى ١٠ ، و ايضا لا يقبل ، اذا النتيجة ان العدد ١٠١ هوه عدد غير اولي

هذه الطريقة في البحث ليست من افضل الطرق في اختيار اولية العدد ، و هناك الكثير من الطرق افضل منها ، وهي Trial Divisionتسمى طريقة

مثال : لدينا عدد ضخم يتكون من ٥٠٠ خانة ، بعد اخذ الجذر Trialالتربيعي اصبح يتكون من ٢٥٠ خانة ، الان طريقه Division
سوف تكون مضيعة للوقت و الجهد لانها سوف تختبر من البداية و حتى ذلك العدد الذي يتكون من ٢٥٠ خانة ، لذلك للتعامل مع الاعداد الضخمة (كما هوه الحال في الشفرات الحديثة) يجب البحث عن حل اكثر كفاءة
و هناك الكثير من الطرق لهذا الامر ، و لكن يمكن لتسريع Trial Divisionالامر اختبار الاعداد الفردية فقط في طريقة

ايضا هناك طريقه و هي تعتمد على عمل الغاء جميع مضاعفات الاعداد ٢ و ٣ و ٥ و ٧ من مدى الاعداد المراد البحث

مثال: نريد معرفة الاعداد الاولية بين ٢ الى ٩٩ ، نقوم بعمل جدول فيه جميع تلك الاعداد (في الغالب تكون في مصفوفة)

بعدها نقوم بشطب مضاعفات العدد ٢ من الجدول ، و مضاعفات العدد ٣ من الجدول ، و هكذا حتى يتبقى لدينا الجدول التالي:

		٧		٥		٣	٢		
١٩		١٧				١٣		١١	
٢٩						٢٣			
		٣٧						٣١	
		٤٧				٤٣		٤١	
٥٩						٥٣			
		٦٧						٦١	
٧٩						٧٣		٧١	
٨٩						٨٣			
		٩٧							

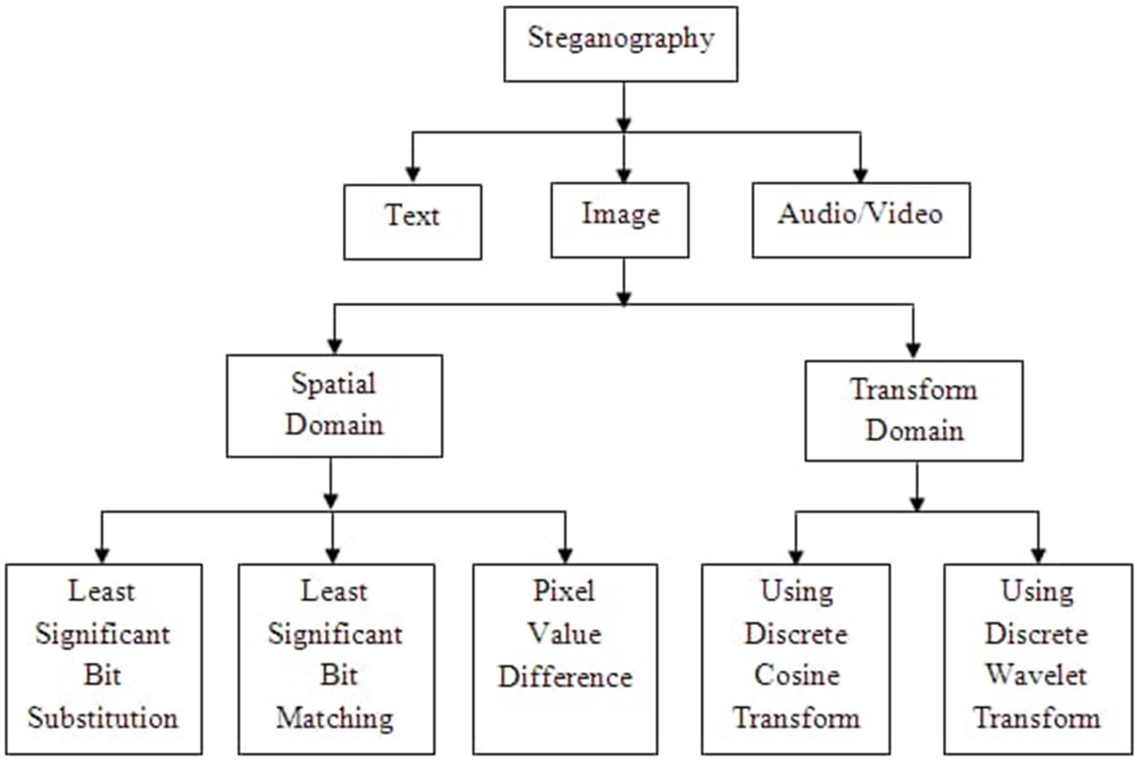
و هو الان يحتوي على جميع الاعداد الاولية من ٢ الى ٩٩ ، على العموم و كما لاحظت انها سوف تستغرق مساحة كبيرة في حاله العدد المراد اختباره كبير ، و لذلك هي غير مستخدمة بكثرة [3]

٢-٨ الاخفاء

الاخفاء هوه علم يهتم ب اخفاء وجود اتصال بين طرفين و دمج الرسائل ضمن اوساط بحيث تكون غير ظاهرة يعمل اخفاء المعلومات من خلال استبدال من البيانات غير المهمة (غير المؤثرة)او غير المستخدمة في ملفات الكمبيوتر العادية (مثل الرسومات ، الصوت ، النص ، الاقراص الملونة) من المعلومات المراد اخفائها ، بشكل غير مرئي و يمكن ان تكون المعلومات المخفية نصا عادية او نصا مشفرا او حتى صورة او فديو

يتم في بعض الاحيان استخدام اخفاء المعلومات عندما لا يسمح التشفير و هوه الاكثر شيوعا و يستخدم الاخفاء لتكملة التشفير فقد يخفى ملف مشفر باستخدام احدى طرق اخفاء المعلومات ، لذلك حتى لو تم فك رموز الملف المشفر لا يتم الوصول الى الرسالة المخفية

يتم اخفاء الرسالة عن طريق ادخالها ضمن الغطاء و الذي غالبا ما يكون ملفا نصيا او صورة او ملفات صوت او فديو ثم ارسالها الى الاطراف المعنية



نتيجة التطور الحاصل في نظم الاخفاء سمح للمستخدم ب اخفاء كميات كبيرة من المعلومات في صورة او ملف صوتي ، هذه الاشكال من اخفاء المعلومات غالبا ما تستخدم بالاشتراك مع التشفير حيث يتم حماية المعلومات على نحو مضاعف ،بحيث المتصنت اذا استطاع العثور على المعلومات اول مرة في ملف الغطاء و هي مهمة صعبة في كثير من الاحيان في حد ذاتها ،يحتاج الى فك تشفيرها قبل التكلم عن كيفية اخفاء المعلومات في ملف صورة ، يجب استعراض كيفية تخزين الصور اولا، ملف الصورة هوة ملف ثنائي يحتوي على تمثيل ثنائي من لون او شدة الاضاءة من كل عنصر من عناصر التي تتالف منها الصورة . الصورة عادة ما

تستخدم اما ٨ بت او ٢٤ بت لتمثيل اللون . عند تمثيل اللون ب ٨ بت ، يصل عدد الالوان الى ٢٥٦ لونا ، كل لون له قيمة ٨ بت .

في نظام الوان ٢٤ بت ، يستخدم ٢٤ بت لكل وحدة صورية ، و توفر مجموعة افضل بكثير من الالوان . في هذه الحالة يتم تمثيل كل وحدة صورية ثلاثة بايتات ، كل بايت يمثل دقة الالوان الثلاثة الاساسية الاحمر و الاخضر و الازرق على التوالي

ابسط انواع الاخفاء هوة اخفاء البيانات داخل ملف صورة باستخدام البت الاقل اهمية لكل وحدة صورية في هذه الطريقة ، يمكن اتخاذ تمثيل ثنائي من البيانات المخفية و الكتابة من كل بايت في الصورة الغطاء . اذا تم استخدام الوان ٢٤ بت ، فان مقدار التغير يكون ضئيلا جدا و غير مدرك للعين البشرية [3]

المصادر

[1] Khashandarag, A.S.; Ebrahimian, N.; (2009), “A New Method for Color Image

Steganography Using SPIHT and DFT, Sending with JPEG Format”, Computer

Technology and Development,. ICCTD '09. International Conference on

[2] Medeni, M.B.O.; Souidi, E.M.; (2010), “Steganographic Algorithm Based On

Error-Correcting Codes For Gray Scale Images”, I/V Communications and

[3] Mahmoud, H.; Alghathbar, K.; (2010), “Novel algorithmic countermeasures for

Differential Power Analysis attacks on smart cards”, Information Assurance and

Security (IAS), 6th International Conference, pp: 52 – 55

[4] Denny Cherry; (2011) “Securing SQL Server: Protecting Your Database from

.Attackers”, Elsevies. Inc. USA