Hybrid Technique for Securing an Object in a Digital Image

Fatin Thair Abd AL-Wahab[1]

[1, 2] Department of Computer Sciences, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq
fatin.22csp40@student.uomosul.edu.iq,

Omar Muayad Abdullah[2]

[1, 2] Department of Computer Sciences, College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq
omaraldewachy@uomosul.edu.iq

ABSTRACT

The research aims to apply techniques of encryption then applying a steganography for securing the information contended in the image through transferring it on internet. We applied these steps first by encrypting the digital image then hiding this image. We used a hill cipher algorithm for encryption and a Least Significant Bit LSB for steganography. The evaluation of the efficiency of this algorithm is conducted in order to gives the highest encryption rate, and based on the hybrid technique of encryption and information hiding on a group of digital images and based on the mean squared error (MSE) measure, the maximum signal to noise ratio (PSNR), and the structural similarity Index measure (SSIM). The results after applying the Hill Cipher algorithm for encryption with the LSB masking technique gave a good encryption and security rate, as the average of the metrics that were used on a set of digital images were as follows: Average Square Error Rate (Av.mse) gives (5.8184) and (Av.psnr) gives (57.567) and (Av.ssim) gives (0.91573175). These results are considered good and give a high security rate, more confidentiality and difficulty of identification and the presence of confidential information in the cover image.

Keywords: Image Steganography, Hill Cipher, Least Significant Bit LSB.

تقنية هجينة لتأمين كائن في صورة رقمية

فاتن ثائر عبد الوهاب ، عمر مؤيد عبد الله
قسم علوم الحاسوب ، كلية الحاسوب والرياضيات ، جامعة الموصل

الخلاصة

يهدف البحث الى تطبيق تقنيتي التشفير ومن ثم الاخفاء من اجل الحفاظ على سرية المعلومات الموجودة في الصورة عند نقلها عبر الانترنت , تتم هذه الخطوات من خلال تشفير الصورة الرقمية بالإعتماد على خوارزمية Hill Cipher ومن ثم إخفاء هذه الصورة الناتجة في صورة اخرى بإستخدام تقنية Least significant bit LSB , حيث يتم اجراء تقييم لكفاءة هذه الخوارزمية من اجل اعطاء اعلى نسبة تشفير, وبالإعتماد على التقنية الهجينة للتشفير واخفاء المعلومات على مجموعة من الصور الرقمية واعتماداً على مقايس متوسط الخطأ التربيعي MSE , نسبة الاشارة الى الضوضاء العظمى PSNR , مقياس التشابه الهيكلي SSIM , حيث اظهرت النتائج ان تطبيق خوارزمية Hill Cipher للتشفير مع تقنية LSB للاخفاء اعطت نسبة تشفير وامان جيدة , حيث كان معدل المقاييس التي تم استخدامها على مجموعة من الصور الرقمية كالتالي معدل متوسط الخطأ التربيعي Av.mse اعطت (5.8184) و Av.psnr اعطت (57.567) و Av.ssim اعطت 0.91573175) وهذه النتائج تعتبر جيدة وتعطي نسبة امان عالي واكثر سرية وصعوبة التعرف وجود معلومات سرية في صورة الغطاء Cover Image.

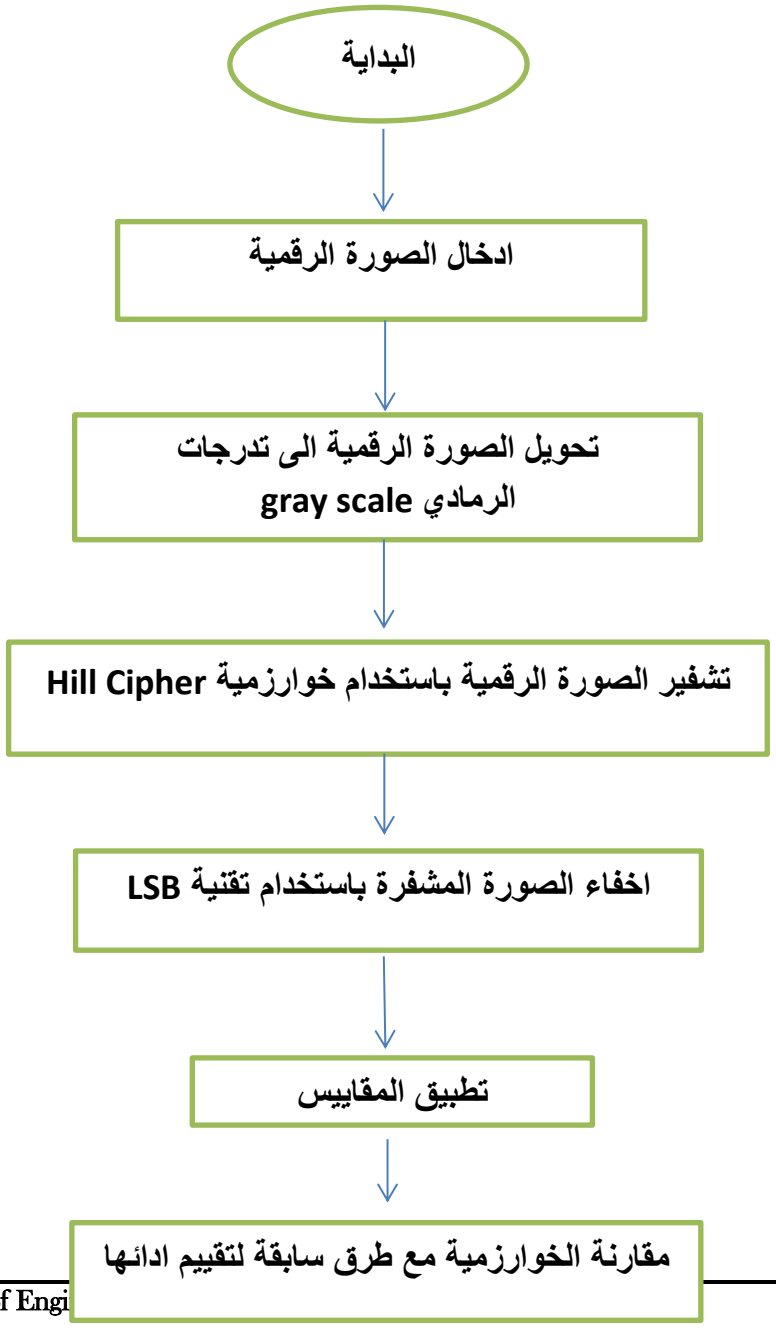
1. Aim of the study

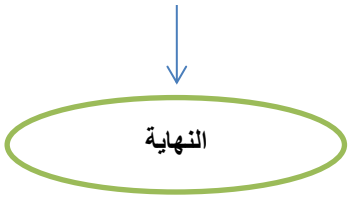
The research aims to apply technique of encryption the applying a steganography on agroup of digital images for securing the information contened in the image through transfering it on the internet form the sender to the recipient .we applied these steps first by encryption the digital image then hiding this image we used a hill cipher algorithm for encrypttion and a Least Siginificat Bit LSB for steganography.then we used the following metrices (MSE , PSNR ,SSIM) for measuring of the work through comparing it with anther works.

يهدف البحث الى تطبيق تقنيتي التشفير ومن ثم الاخفاء على مجموعة من الصور الرقمية بهدف الحفاظ على امنية المعلومات الموجودة في الصورة خلال نقلها عبر الانترنت من المُرسل الى المستلم تتم هذه الخطوات من خلال تشفير الصوره الرقمية ومن ثم اخفاؤها في صوره اخرى تسمى صورة الغطاء (Cover Image) يتم التشفير بأستخدام خوارزمية (Hill Cipher) ومن ثم اخفاء الصوره الناتجة في صورة الغطاء بإستخدام تقنية LSB (Least Significant Bit) وثم استخدام مقاييس معينة لقياس كفاءة عمل هذه الخوارزمية وهذه المقاييس هي (MSA ,SPNS, SSIM)حيث ان MSE اعطت (1.7136e-07) وPSNR اعطت (115.7916) وكذلك SSIM اعطت (1.0000).

1.1 *General Structure of the resarch*

بعد ان تم تحديد الخوارزمية المستخدمة في تشفير الصورة الرقمية ومن ثم اخفاؤها في صورة الغطاء اعتمادا على تقنية LSB تم تحديد الهيكل العام للبحث من خلال المخطط التالي:





الشكل (1) المخطط العام للبحث

تم تحويل صورة ملونه الى تدرجات الرمادي (Gray Scale) لكي يتم معالجتها بإستخدام خوارزميات التشفير المحددة :

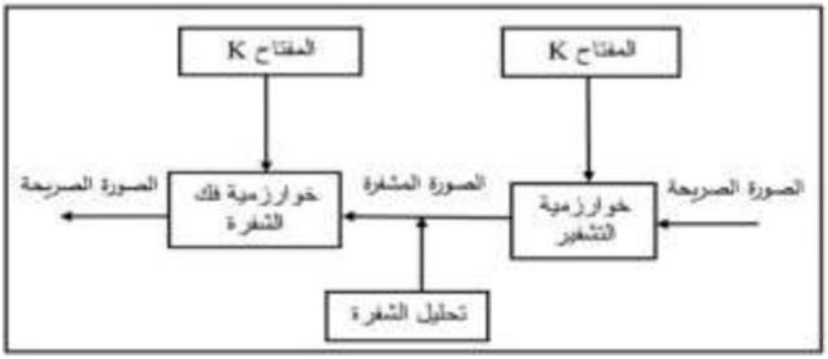
الشكل(2) تحويل صورة ملونة الى صورة رمادية ذات تدرجات رمادي

2. Introdection

Image Processing تعتبر الصور مصدراً جيداً لتوفير المعلومات المرئية و تستخدم الصور في تطبيقات عديدة في مجالات مختلفة. الصور هي تقنية لعرض البيانات وتوثيقها بصرياً وهو مفهوم قديم تم نحته على الصخور ثم تُرسم على الورق ، حتى ظهور اجهزة الكمبيوتر ومعها مفهوم الصور الرقمية . وهي تمثيل حاسوبي لصورة ثنائية الابعاد متمثلة بالاصفار والاحاد (0,1) كل صورة رقمية مكونة من بكسلات و البكسل هو اصغر وحدة في الصورة وكل صورة عبارة عن مصفوفة تتكون من مجموعة نقاط و كل نقطة لها قيمة معينة كلما زادت عدد وحدات البكسل في صفوف واعمدة وحدات البكسل زادت جِدة الصورة .وللصور امتدادات عديده منها (JPG , PMP , GIF , PNG) [1] . يشير مصطلح "الصورة الملونة" إلى الصور الرقمية التي تحتوي على معلومات الألوان. وهي مكونة من ثلاثة أشرطة أحادية اللون، كل منها يخزن لوناً فريداً. يتم استخدام مجموعة متنوعة من التدرجات الرمادية لتمثيل كل قناة لونية في الصور الفوتوغرافية. الرسومات في هذه الحالة هي صور RGB، والتي تمثل اللون الأحمر والأخضر والأزرق. تتطلب كل قناة ألوان RGB 8 بتات من أصل 24 بت/بكسل اللازمة لإنشاء كل صورة ملونة. يُشار إلى الصورة التي يتم عرضها بالألوان الكاملة على شاشة الكمبيوتر أو أي جهاز آخر باسم الصورة الملونة. يشير المصطلحان "الصور بالأبيض والأسود" و"الصور ذات التدرج الرمادي" إلى الصور التي يتم عرضها فقط باللونين الأسود والأبيض أو بتدرج الرمادي، على التوالي. أنواع الملفات التي يمكن استخدامها لحفظ وعرض صورة ملونة عديدة. لتصوير الصور الملونة بدقة يجب أن يحتوي الجهاز المحوسب إما على معدات العرض الخاصة به، مثل الشاشة، التي يمكنها عرض الألوان المطلوبة، أو يجب أن يكون متصلاً بهذا الجهاز . قد يتم إجراء تغييرات على الجهاز المستخدم لعرض الصورة ونوع ملف الصورة من أداة إلى أخرى، قد تتسبب الصورة في ظهور الألوان بشكل مختلف قليلاً.[2]

Cryptography علم التشفير معروف مُنذ العصور القديمة حيث كان يستخدم في المجال العسكري, ان الفرعون هو اول شخص قام بتشفير الاتصالات بين مختلف افرع الجيش . و ذُكر ان العرب لديهم محاولات قديمة في مجال التشفير استخدم الصينيون العديد من طرق التشفير لنقل الرسائل اثناء الحرب وافضل طريقة تم استخدامها في العصور القديمة كانت طريقة يوليوس قيصر احد قياصرة الرومان تستخدم هذه الشبكات لنقل المعلومات الكترونياً سواء بين الناس العاديين او بين المؤسسات العامة او الخاصة سواء كانت عسكرية او مدنية. كان الغرض من استخدامهم للتشفير اخفاء الشكل الحقيقي للرسائل عند وقوعها في ايدي العدو حتى يصعب على العدو فهمها وقد بُذلت جهود هائلة حول العالم يمكن من خلالها تبادل البيانات دون الكشف عن محتواها في المقابل يُدرك الجميع اهمية التشفير والحاجة المتزايدة له خاصة اليوم مع انتشار الانترنت على نطاق واسع والسرقة المتكررة للمعلومات والبيانات الشخصية تكمن أهمية التشفير في الحفاظ على سرية المعلومات المهمه والحساسة ومنعها من الوصول الى الاشخاص غير المرغوب فيهم. يقلل التشفير ايضا من كمية المعلومات التي يتم نقلها عبر ضغط البيانات والتأكد من هوية مرسل الرسالة مما يضمن أن الاشخاص المُصرح لهم فقط هم من يمكنهم عرض هذه البيانات ولكي يكونون قادرون على قراءة محتوياتها يجب عليهم اولاً فتح تشفير تلك البيانات اوالمعلومات لان فتح التشفير هو عملية اعاده البيانات من شكلها المشفر الى شكلها الاصلي وطبيعتها من اجل قراءة محتوياتها وهذا يمكن فقط يتم من خلال معرفة المفتاح المستخدم في عملية التشفير وبتالي يمنع كل شخص ليس لديه المفتاح من قراءة ومعرفة محتويات البيانات او المعلومات المشفرة يوضح الشكل رقم (3) نظام التشفير[3] [4].في انظمة البيانات المفتوحة عندما يتم ارسال واستلام المعلومات والبيانات قد يسئ استخدامها من قبل الخصوم وتتعرض لهجمات مختلفة في مستويات مختلفه لذا تم التوصل الى تشفير البيانات حيث يعتبر التشفير الوسيلة الاقوى والاكثر فعالية لمواجهة الهجمات والحفاظ على امن المعلومات . يعرف التشفير بأنه عملية تحويل البيانات من شكلها الطبيعي الى شكل اخر غير مفهوم من خلال التلاعب الخوارزمي المعقد لحماية البيانات

اوارسالها الى اطراف اخرى بطريقة امنة. هناك نوعان من طرق التشفير وهما التشفير المتماثل (Symmetric Encryption) باستخدام المفاتيح السرية اي ان المرسل والمستلم يستخدمون نفس المفتاح , والتشفير الغير متماثل (A Symmetric Encryption) بإستخدام زوجاً من المفاتيح وهُما المفتاح العام والمفتاح الخاص تعد انظمة التشفير المتماثل اسرع وابسط من الانظمة الغير متماثلة حيث انه كان ولازال يستخدم في نطاق واسع في حل مشاكل الاتصال التقليدية الغير امنة , يتم استخدامه في الانظمة المفتوحة مثل الانترنت وتشفير البيانات بشكل كبير لضمان امن المعلومات ,كل نوع من البيانات له مميزاته لذلك يجب استخدام تقنيات تشفير مختلفة لحماية البيانات السرية من الاستخدام الغير مصرح به [5].يوضح الشكل الاتي نظام التشفير:



الشكل (3) نظام التشفير

Steganography: مع ازدياد تطور ونمو شبكات الانترنت اصبح الحفاظ على امن البيانات وسريتها مصدر قلق كبير وبتالي جذبت تقنيات اخفاء البيانات Hidding techniques الكثير من الناس حول العالم. يتم استخدام تقنيات الاخفاء Steganography techniques في ادارة حقوق النشر الرقمية وحماية المعلومات واخفاء الاسرار والبيانات هذه التقنيات توفر تحديا كبيراً ومثيراً للاهتمام للمحقّين في الطب الشرعي الرقمي . تعتبر البيانات اليوم العمود الفقري للاتصالات , للتأكد ان البيانات مؤمنة ولاتذهب الى جهات غير مرغوبه او مقصودة جاء مفهوم اخفاء البيانات لحماية جزء من المعلومات. البيانات الرقمية يمكن ان يتم استلامها مع القليل من الاخطاء وبدون تدخل الانترنت يوفر وسيلة اتصال لتوزيع البيانات لمختلف المستخدمين لذلك فإن الحفاظ على امن المعلومات والبيانات اصبح ضرورياً للحماية من الوصول الغير مُصرح به [6] .تعتمد تقنية Steganography على اخفاء ملف سرية بيانات الوسائط المتعددة الصغيرة داخل اخرى لكن اكبر بكثير . على الرغم من ان اهداف التشفير واخفاء المعلومات متشابه الا ان هناك اختلاف طفيفاً , يُركز التشفير على الاحتفاظ بمحتويات الرسالة وجعل البيانات غير قابلة للكسر وغير قابلة للقراءة لكن النص المشفر (cipher text) مرئي للعين البشرية ويمكن تميزهُ , بينما الاخفاء يُركز على الحفاظ على سرية وجود الرسالة بحيث تكون غير ظاهرة للاشخاص ويسمح بإستخدام مجموعه متنوعة من المعلومات السرية مثل (الصور ,نصوص , صوت , فديو). تقنيات الاخفاء متاحه منذ زمن طويل لكن اهميتها بدأت تتزايد في الاونة الاخيرة السبب الرئيسي وراء ذلك هو الزيادة في حركة مرور البيانات عبر الانترنت والتواصل الاجتماعي وكثرة استخدامها [7] .التشفير وإخفاء المعلومات هي تقنيات شائعة و واسعة الاستخدام لمعالجة المعلومات (رسائل) من أجل تشفيرها وإخفاء وجودها. هذه التقنيات لها تطبيقات واسعة جداً في مجال الحاسوب والمجالات الاخرى ذات الصلة لأنها تستخدم لحماية رسائل البريد الالكتروني ومعلومات بطاقة الائتمان وأمنية بيانات الشركات والخ....[8]

2.1 *Relative Studies*

أصبح تبادل المعلومات الحساسة بين العديد من الأطراف أمراً بسيطاً نسبيًا بفضل تطور الإنترنت والاتصالات. ومع ذلك، تشمل المشكلات المتعلقة بمثل هذه الاتصالات القنوات غير الآمنة التي تؤدي إلى فقدان السرية والأصالة والنزاهة، من بين مشكلات أخرى. لقد استخدم الباحثون منذ فترة طويلة التشفير وإخفاء المعلومات كحلين مقبولين على نطاق واسع لهذه القضايا. على الرغم من أن البيانات المشفرة تجذب الانتباه وتبرز أهميتها عند اعتراضها، فإن التشفير، وهو عملية تحويل البيانات الحساسة إلى نموذج غير قابل للقراءة، يوفر نقلًا آمنًا للبيانات. من ناحية أخرى، فإن تقنية إخفاء المعلومات، وهي تقنية لإخفاء المعلومات الخاصة، لا تكشف شيئًا عن هذا الاتصال السري. [9] قام الباحثان Dr.R.Sridevi&Vijaya Lakshmi Paruchuri, واخرون(2013) بإجراء دراسة بعنوان 'Image Steganography combined with Cryptography' من أجل إخفاء المعلومات الحساسة في الصورة، تقترح هذه الدراسة نهجاً يجمع بين تقنيات التشفير وإخفاء المعلومات. سيستخدم المرسل أولاً تقنية البت الأقل أهمية (LSB) لتضمين البيانات السرية في الصورة. سيتم استخدام تقنية التشفير لتشفير الصورة المدرجة. في النهاية، سيقدم المتلقي المفتاح السري الصحيح من أجل فك تشفير الصورة المشفرة والحصول على البيانات المخفية. يعد تضمين البيانات وتشفير الصور واستعادة الصورة الأصلية والبيانات السرية من الصورة المشفرة جميعها خطوات في العملية[10] .وايضا قدم الباحث Pranati Rakshit وأخرون(2021) بإجراء دراسة بعنوان ' Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography ' وهدفت الدراسة الى تقديم نهجًا جديدًا لأمن المعلومات من خلال الجمع بين أساليب إخفاء المعلومات الصوتية وأساليب التشفير المرئي. في هذا الأسلوب، نستخدم التشفير المرئي لتقسيم الصورة السرية إلى أجزاء فرعية متعددة، وإنشاء صور فرعية متعددة غير مفهومة. بعد ذلك، وبإستخدام أساليب إخفاء المعلومات الصوتية، يتم إخفاء كل صورة فرعية خلف تسجيل صوتي فريد من نوعه. يتم بعد ذلك نقل صوتيات الغلاف إلى المواقع الضرورية حيث تخضع لخوارزميات إخفاء المعلومات العكسية لاستعادة الصور المكونة غير المفهومة. وأخيرًا، يتم إنشاء الصورة المخفية الحقيقية من خلال تركيب جميع الصور

الفرعية. تستخدم هذه التقنية آلية أمنية من خطوتين لضمان السرية، مما يجعلها آمنة جداً. نظراً لأن كل مكون من مكونات الصورة الفرعية الصحيحة مطلوب لإعادة إنشاء الصورة السرية الحقيقية، فإن احتمالية الاعتراض تقل عند استخدام هذه التقنية. من المستحيل إنشاء صور مخفية مفيدة دون تركيب كل صورة فرعية. يتم تجميع البتات الموجودة في الملفات الصوتية بشكل وثيق معاً. إن الطريقة المقترحة لإخفاء الصوت في المجال الزمني تجعل من الصعب على المستمع تمييز التلاعب بسبب كثافة البيانات العالية في الصوت.[11] وكذلك طور Manikandan T وآخرون. (2021) إطاراً بعنوان Secure E-Health using Images Steganography يجمع بين إخفاء المعلومات والتشفير بحيث لا يتمكن سوى المرسل المعتمد من نقل الصورة السرية إلى المستلم. تتم معالجة صور الأشعة السينية الطبية السرية في المرحلة الأولى من نظام إخفاء الصور. يتم إجراء نفس إجراء فك التشفير من جانب المستلم، ثم يتبعه التحقق على مستويين باستخدام مصادقة البريد الإلكتروني وإنشاء Pega OTP. وهذا يضمن أن الصورة السرية التي قدمها المرسل لا يمكن استلامها وعرضها إلا من قبل المستلم المقصود[12]. تم اقتراح نظام جديد لإخفاء المعلومات داخل الصورة من قبل الباحث Wid Akeel Awadh واخرون (2022) بعنوان ' Hybrid information security system via combination of compression, cryptography, and image steganography ' لتوفير الأمن العالي للمعلومات. حيث هدفت هذه الدراسة الى تقديم سلسلة من الإجراءات لضغط الصورة السرية باستخدام خوارزمية تحويل الموجات المنفصلة (DWT) وتشفير البيانات المضغوطة باستخدام خوارزمية معيار التشفير المتقدم (AES). ولإخفاء البيانات المشفرة، يتم اتباع نهج البت الأقل أهمية (LSB) تم استخدامه. أظهرت النتائج أن النظام المقترح قادر على تحسين مؤشر التشابه الهيكلي (قيمة SSIM 0.92) وجودة الصورة المصاحبة (قيمة PSNR 47.8 ديسيبل). وأظهرت نتائج التجربة أيضًا أن استخدام كلتا الاستراتيجيتين معًا يحافظ على جودة الصورة المخفية بنسبة 68%، ويعزز أداء النظام بنسبة 44%، ويوسع حجم البيانات السرية مقارنة باستخدام كل تقنية على حدة. قد يساعد هذا البحث في معالجة مسألة سعة وأمن المعلومات المقدمة عبر الإنترنت[13]. واقترح Medeni و Souidi(2010)طريقة لبناء طريقة جديدة إلخفاء المعلومات، وهي امتداد لتصحيح الخطأ ورمز بناء إخفاء المعلومات. والطريقة المقترحة تتألف من استخدام منطق فك التشفير لتضمين الرسالة في صورة الغلاف، وتستند على استخالص الترميز[21].

2.2 *Encryption using Hill Cipher algorithm*

Hill Cipher شفرة متناظرة كلاسيكية تعتمد على تحويل المصفوفة لكنها تخضع لهجوم النص الصريح المعروف على الرغم من تعرضه لتحليل التشفير جعله غير قابل للاستخدام من الناحية العلمية الإ انه لايزال يلعب دوراً مهماً في كل من علم التشفير والجبر الخطي يعتمد Hill cipher على الجبر الخطي ويتغلب على مشكلة توزيع التردد لخوارزمية Caesar Cipher [14]. خوارزمية التشفير هي مجموعة من العمليات المصممة لتحويل صورة صريحة الى صورة مشفرة ويعتمد امان انظمة التشفير الحديثة على مفتاح (k) تعتمد على عاملين اساسين :

1.المفتاح الاساسي ويسمى الخوارزمية . 2. طول المفتاح .

اما عملية فك التشفير فتكون عملية معاكسة اي تحويل صورة مشفرة الى شكلها الاصلي [15] .تم تطوير خوارزمية Hill Cipher من قبل عالم الرياضيات Lester hill جوهر تشفيرHill Cipher هو معالجة المصفوفة للتشفير اي تعتمد في استخدامها على المصفوفات, تعتبر خوارزمية Hill من الخوارزميات القويه التي تعطي افضل النتائج في تشفير الصور الرقمية . تأخذ الخوارزمية نصاً عادياً plain text متتاليا الحروف وبدلاً من ذلك تحل محل الحروف المشفرة قيم يتم يتعين قيمة عددية لكل حرف مثل $a = 0, b = 1, \dots, z = 25$ استبدال احرف النص المشفر في مكان احرف النص العادي تؤدي الى معادلة خطية بالنسبة الى m=3 يمكن ان يكون النظام على النحو التالي :

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_1 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$$

يمكن التعبير عن هذه الحالة من حيث متجهات العمود والمصفوفات :

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$$

يتطلب فك التشفيراستخدام معكوس المصفوفة K او يمكننا ببساطة كتابة C=KP حيث ان الاعمدة بطول 3 تمثل النص العادي plaintext والنص المشفر ciphertext , k عبارة عن مصفوفة 3×3 وهو ايضا مفتاح التشفير encryption key ومن ثم تنفيذ جميع العمليات (mod 26) اما فك التشفير يتطلب معكوس المصفوفة k والمصفوفة المعكوسة k^{-1} تعّرف بالمعادلة الاتيه:

$KK^{-1} = K^{-1}K = I = I$

حيث ان I هي معّرف المصفوفة , معكوس المصفوفة غير موجود دائماً وعندما تكون موجودة فإنها تفي بما سبق يتم تطبيق k^{-1} على النص المشفرciphertext ومن ثم اعادة النص العادي plaintext [16][17] وتكون كتالي :

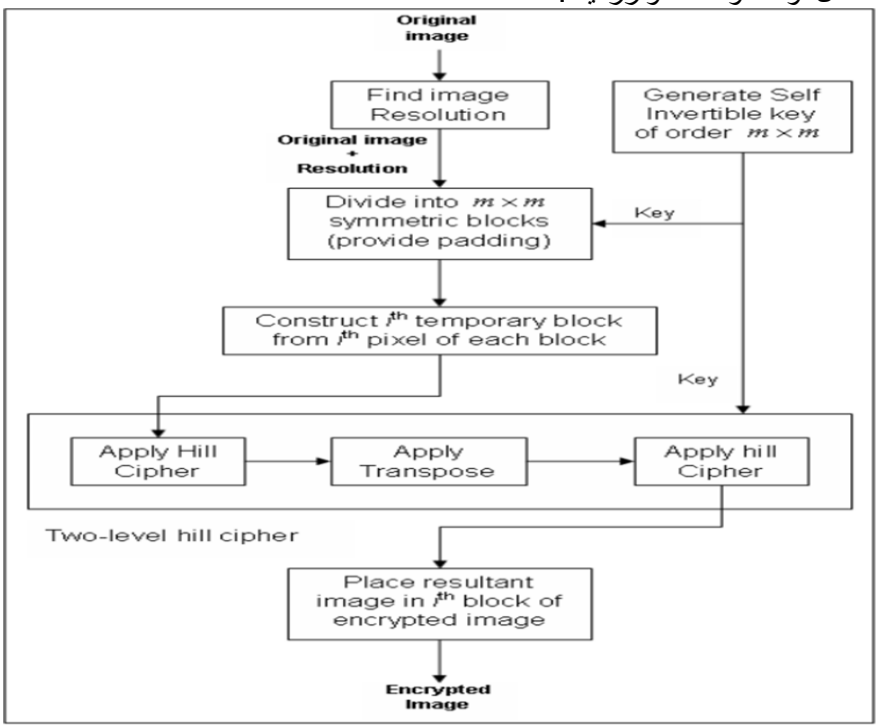
For encryption:

$$C = E_k(P) = K_p$$

For decryption:

$$P = D_k(C) = K^{-1}C = K^{-1}K_p = P$$

تعتبر خوارزمية Hill Cipher احدى خوارزميات تشفير المفاتيح المتماثلة التي تتمتع بعدة مزايا في تشفير البيانات .تعمل خوارزمية هيل بشكل جيد مع الصور الملونة وكذلك الصور ذات التدرج الرمادي ,بالنسبة للصور ذات التدرج الرمادي سيكون المعامل 256 (يعتبر عدد المستويات بمثابة عدد الحروف الهجائية) في حالة الصور الملونة نقوم اولا بتحليل الصور الملونة الى مكونات RGB, ثانيا نقوم بتشفيركل مكونRGB بشكل منفصل بواسطة الخوارزمية واخيرا نقوم بتسلسل المكونات المشفرة معا للحصول على الصور الملونة المشفرة [16] يمثل المخطط التالي طريقة عمل او خطوات الخوارزمية :



الشكل (4) خوارزمية خوارزمية Hill Cipher

2.3 *Image Steganography*

مصطلح Steganography مشتق من الكلمة اليونانية ' Stegos ' والتي تعني الغلاف و' ' grapha مما تعني الكتابة . وتعني ' الكتابة المغطاة' يتم استخدام الاخفاء لاخفاء المعلومات داخل الوسائط الاخرى. وهو احد الطرق للحفاظ على امن البيانات وهو علم او تقنية تُستخدم لحجب البيانات داخل وسيط رقمي مثل (الصور ,نصوص , صوت , فديو) الصور الرقمية هي من اشهر الاستخدامات في اخفاء البيانات وهذا يعود لعدة اسباب منها إنتشار الصور بكثرة وسهولة الوصول اليها وكذلك تنوع احجام الصور وتعدد الالوان داخل الصورة ومساحة الاخفاء كلما كان حجم الصورة اكبر اصبح لدينا مساحة اخفاء ملف بحجم اكبر .وحجم الملف او الصوره التي سنخفيها كلما كانت اصغر من صورة الغلاف كان ذلك افضل[18]. اخفاء الصور هو اسلوب لاخفاء صورة داخل اخرى حيث يتم التلاعب بصورة الغلاف بطريقه تجعل البيانات المخفية غير مرئية مما يجعلها غير مشبوهة كما الحال في التشفير عكسيا .

تكون اليه اخفاء البيانات في الصور كالتالي :

1. نحتاج الى صورة تسمى صوره الغطاء Cover Image التي نخفي بها الصوره المشفره اوالمعلومات السرية المراد اخفاءوها حيث يتم تشفير الصورة بإستخدام احدى خوارزميات التشفير .
2. نقوم بتشفير الصورة الاصلية (Stego Image) التي سنقوم باخفاءها داخل صورة الغطاء لزيادة الامان والحمايه حتى في حال تم اكتشاف البيانات المخفية يحتاج الى ان يفك التشفير اولاً.
3. نحتاج ان نستخدم احد الخوارزميات او التقنيات الاكثر شيوعاً في اخفاء البيانات هي (Last Significant Bit LSB) [19].

يعد إخفاء المعلومات الستند الى البت الأقل أهمية (LSB) أحد الأساليب البسيطة التي تخفي معلومات سرية في LSB لقيم البكسل دون تغيير أي تشوهات. LSB البت الأقل أهمية في معنى اخر ، يتم تغيير البت الثامن من بعض أو كل البايتات الموجودة داخل الصورة من جهة اليمين إلى جزء من المعلومات السرية.عند استخدام صورة ذات 24 بت، يمكن استخدام جزء صغير من كل مكون من مكونات الألوان RGB (الأحمر والأخضر والأزرق)، نظرًا لأنها يتم تمثيل كل منها بواسطة بايت وكل بايت يتكون من 8 بتات] [22 وتستخدم بشكل عام كالتالي يكون الاتصال السري بين الجهات المعروفه او المراد التواصل بينها حيث هذه التقنيه تقوم بإستبدال اجزاء صغيرة من الوسائط الرقمية الغير مستخدمة مع البيانات السرية اي تضمين الكائن المخفي في جسم اكبر بشكل ملحوظ بحيث لايمكن للعين البشرية اكتشاف التغيير. ,يمكن استخدام جميع تنسيقات الملفات الرقمية لاخفاء المعلومات لكن التنسيقات مع درجة عالية من التكرار تكون اكثر ملائمة, البتات الزائدة عن الحاجة للكائن هي تلك البتات التي يمكن تغييرها .صور الغلاف الاكثر شيوعا المستخدمة في اخفاء المعلومات هي الصور الرقمية غالبا ماتحتوي الصور الرقمية على كمية كبيرة من البيانات الزائدة عن الحاجة وهذا ماتستخدمه تقنيات الاخفاء لاخفاء الرسالة .اخفاء المعلومات والتشفير هما من تقنيات الامن المتوازية اي يمكن تنفيذها معا. يتم استخدام Steganalysis للكشف عن وجود اي رسالة سرية مغطاة في الصورة واستخراج البيانات المخفية .يساعد Steganalysis في تصنيف ما اذا كانت الصوره اما صورة Stego او صورة عادية بغض النظر عن تصنيف الصورة يتم إجراء مزيد من التحقيق للكشف عن موقع ومحتوى الصورة السرية داخل صورة الغلاف تعتبر عملية الكشف عن البيانات المخفية اصعب من عملية اخفاؤها وذلك بسبب التنوع الكبير في امتدادات الصور وانواعها ومساحة الاخفاء وحجم الملف المخفي .[7][20]

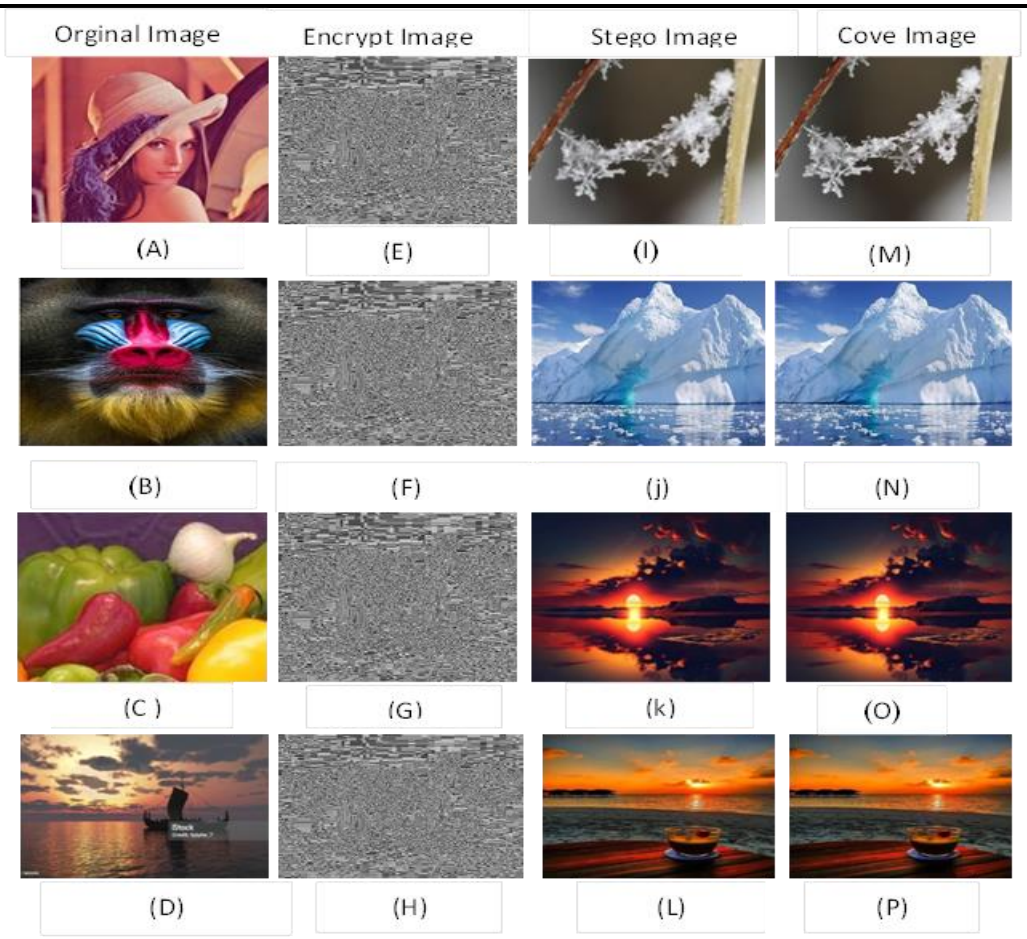
تطبيق المقاييس:

اولا: لدينا مجموعة صور تم تشفيرها بإستخدام خوارزمية التشفير Hill Cipher ثم تطبيق المقاييس لتوضيح نسبة التشفير مقارنة بالصور الاصلية ,حيث كانت نتائج المقاييس على الصور مختلفة كما في الجدول التالي :

الجدول (1) تطبيق المقاييس على الصور بعد التشفير بإستخدام خوارزمية hill Cipher

Image	MSE	PSNR	SSIM
A-E	7201.29	9.556	0.171
B-F	6375.6	10.086	0.212
C-G	5345.52	10.8509	0.0631
D-H	6379	10.0833	0.35088

ثانيا : اخفاء الصورة المشفرة في صورة اخرى تسمى صورة الغطاءCover Image وثم تطبيق المقاييس على الصورة نلاحظ



اختلاف بالقيم كما في الجدول التالي:

جدول (2) تطبيق المقاييس على الصور قبل الاخفاء

Image	MSE	PSNR	SSIM
E-I	105541	7.8966	0.0245651
F-J	6757.89	9.83269	0.0236469
G-K	10034.3	8.11593	0.0118341
H-L	886097	8.65599	0.0419675

جدول (3) تطبيق المقاييس على الصور بعد الاخفاء

Image	MSE	PSNR	SSIM
I-M	0.0537	60.822	0.998022
J-N	0.0545	57.603	0.898861
K-O	2.0544	55.937	0.787164
L-P	21.1110	55.906	0.97888

والجدول التالي يوضح معدل المقاييس للصور المشفرة بإستخدام خوارزمية hill cipher:

جدول (4)معدل المقاييس للصور المشفرة

ت	المقاييس	المعدل
1	MSE	6325.3525
2	PSNR	10.14405
3	SSIM	0.199245

والجدول التالي يوضح معدل المقاييس للصور بعد الاخفاء:

جدول (5) معدل المقاييس للصور بعد الاخفاء

ت	المقاييس	المعدل
1	MSE	5.8184
2	PSNR	57.567
3	SSIM	0.91573175

Conclusions:

Depending on applying the hybrid technigue of encryption and steganography on agroup of digital image, we got a number of conclusions depending on the values obtained from the tables above , as explained below **:**

1. In the level of encryption we noticed that the mean squared error MSE gives highervalue between A and E images where the value was 7201.29
2. Depending on the SSIM metric the results show the image (I-M) gives higher similarity ratio for the cover image befor and after Steganography

References:

[1] F. Nielsen, "Image and Information", arXiv Prepr. arXiv1602.01228, 2016

[2] Ashima Kalra Dr. Aiyah S. Noori Mrs. Veenu & Mr. Jonnadula Narasimharao,'' Digital Image Processing" Book · April 2023,p.p 1-201

[3] K. D. Patel and S. Belani, “Image encryption using different techniques: A review,” Int. J. Emerg. Technol. Adv. Eng., vol. 1, no. 1, pp. 30–34, 2011

[4] S. Liu, C. Guo, and J. T. Sheridan, “A review of optical image encryption techniques,” Opt. Laser Technol., vol. 57, pp. 327–342, 2014

[5] Ramandeep Sharma, Richa Sharma, Harmanjit Singh , "Classical Encryption Techniques, Council for Innovative Research", Volume 3. No.1, pp 84_90.

[6] Shamim Ahmed Laskar, Kattamanchi Hemachandran , "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6 ,p.p 57_86

[7] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography"I.J.Modern Education and Computer Science, 2012, 6, 27-34 Published Online June 2012 in MECS (http://www.mecs-press.org/) DOI : 10.5815/ijmecs.2012.06.04. p.p 28_34

[8] Stallings William; (2006), “Cryptography and Network Security Principles and Practices” , 4 th Edition, Pearson Education, Inc., Prentice Hall.

[9] Proton Sarkar a , Sudipta Kumar Ghosal b,⇑ , Madhulina Sarkar,' Stego-chain: A framework to mine encoded stego-block in a decentralized network' Journal of King Saud University – Computer and Information Sciences 34 (2022) 5349– 5365

[10] Dr.R.Sridevi, Vijaya Lakshmi Paruchuri, K.S.SadaSiva Rao,'' Image Steganography combined with Cryptography'' Vol 9, No 1, Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, J u l y 1 5 , 2 0 1 3 , p.p 976-984

[11] Pranati Rakshit1, Sreeparna Ganguly1, Souvik Pal2, Ayman A. Aly3 and Dac-Nhuong Le," Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography "Computers, Materials & Continua Tech Science Press DOI:10.32604/cmc.2021.014293

[12] Manikandan, T., Muruganandham, A., Babuji, R., Nandalal, V. & Iqbal, M. (2021). Secure E-Health using Images Steganography. Journal of Physics: Conference Series, 21(1), 1-7.

[13] Wid Akeel Awadh1 , Ali Salah Alasady2 , Alaa Khalaf Hamoud ' Hybrid information security system via combination of compression, cryptography, and image steganography ' International Journal of Electrical and Computer Engineering (IJECE) , Vol. 12, No. 6, December 2022, pp. 6574~6584

[14] N.Vijayaraghavan#1, S.Narasimhan#2, M.Baskar#3," A Study on the Analysis of Hill's Cipher in Cryptography "International Journal of Mathematics Trends and Technology (IJMTT) – Volume 54 Number 7- February 2018,p.p 519_522

[15] ف. ح. رضا, "توليد مفاتيح أنظمة التشفير اللامتماثل باستخدام الخوارزمية الجيهية لتشفير وفك الشفرة أسئلة الامتحانات الوزارية والكتب الرسمية," DIRASAT TARBAWIYA, vol. 38, no. 10, pp. 221–237, 2017

[16] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda," Image Encryption Using Advanced Hill Cipher Algorithm",International Journal of Recent Trends in Engineering, Vol. 1, No. 1,p.p 663_667

[17] Younes Qobbi1*, Abdeltif Jarjar2, Mohammed Essaid3 and Abdelhamid Benazzi1," Younes obbi1*, Abdeltif Jarjar2, Mohammed Essaid3 and Abdelhamid Benazzi1" New Image Encryption Scheme Based on Dynamic Substitution and Hill Cipher".Medicon Engineering Themes Volume 1 Issue 2 November 2021, Research Articlep.p 23_30

[18] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez,''A Comparative Study of Recent Steganography Techniques for Multiple Image Formats'' I. J. Computer Network and Information Security, 2019, 1, 11-25, Published Online January 2019 in MECS (http://www.mecs-(/press.org/),DOI: 10.5815/ijcnis.2019.01.02, PP 12-25.

[19] Ashwak ALabaichi1 , Maisa'a Abid Ali K. Al-Dabbas2 , Adnan Salih, " Image steganography using least significant bit and secret map techniques " International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020, pp. 935~946 ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp935-946

[20] NANDHINI SUBRAMANIAN, SOMAYA AL-MAADEED, AHMED BOURIDANE," Image Steganography: A Review of the Recent Advances ", Digital Object Identifier 10.1109/ACCESS.2021.3053998,p.p23409_23423

[21] Medeni, M.B.O.; Souidi, E.M.; (2010), "Steganographic Algorithm Based On Error-Correcting Codes for Gray Scale Images", I/V Communications and Mobile Network (ISVC), 5th International Symposium, pp: 1 – 4.

[22] K. Anandharaj& J. Abdul Samath ," A Review on Various Image Steganography and Cryptography Techniques'' Compliance Engineering Journal ,Volume 11, Issue 2, 2020, ,p.p 107-116.