# Using Template Machine Technique and Encryption For Securing An Object In Digital Image

# استخدام تقنية مطابقة النموذج والتشفير لتأمين كائن في الصورة الرقمية

**Ahmed Mohamed Hussein** College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq. ahmed9019moh@gmail.com

**Omar Muayad Abdullah** College of Computer Sciences and Mathematics, University of Mosul, Mosul, Iraq

ABSTRACT/الملخص

The research aims to apply template matching technology to a group of digital images in order to detect an eye object in the images, and then this object is encrypted in the resulting image depending on a set of algorithms (RSA, Hill Cipher, Elliptic Curve), where a comparison and evaluation were made. For the efficiency of these three algorithms after applying them to the template that was identified in the resulting image in order to determine the algorithm that gives the highest encryption rate and depending on the mean square error measure, the maximum signal-to-noise ratio, the structural similarity measure, and the time it takes to perform the encryption process, and the results were shown after determining The template to be processed is that the (RSA) algorithm gave the highest coding ratio at a rate of 0.0113, which is the best ratio based on the Structural Similarity Scale (SSIM) being closer to zero. The metrics MSE gives (18869.7) for the RSA and The metrics SSIM gives (0.010) for the RSA and the execution time for RSA was (0.115) and that is considered the best compared to other two algorithm. Consider the current status of research and forecast the future.

يهدف البحث الى تطبيق تقنية مطابقة القالب على مجموعة من الصور الرقمية من أجل الكشف عن كائن معين في الصوره ، ومن ثم يتم تشفير هذا الكائن في الصورة الناتج، اعتماداً على مجموعة من الخوارزميات وهي ( RSA , Hill Cipher , Elliptic Curve) ، حيث تم اجراء مقارنه وتقييم لكفاءه هذه الخوارزميات الثلاث بعد تطبيقها على القالب الذي تم تحديده في الصوره الناتجه من اجل تحديد الخوارزميه التي تعطي اعلى نسبه تشفير واعتمادا على مقياس متوسط الخطا التربيعي، نسبه الاشاره الى الضوضاء العظمى، مقياس التشابه الهيكلي، والمده الزمنيه المستغرقه لتنفيذ عمليه التشفير واظهرت النتائج بعد تحديد القالب المطلوب معالجته ان خوارزميه ( RSA) اعطت اعلى نسبه تشفير بمعدل ( 0.0113 )والتي هي افضل نسبه اعتمادا على مقياس التشابه الهيكلي ( SSIM ) كونها اقرب الى الصفر وكذلك اعطت هذه الخوارزميه ايضا اقل مده تنفيذ مقارنه بعمل الخوارزميات الاخرى حيث أعطت المقاييس MSE( 18869.7) لـ RSA وم SSIM (0.010 ) ووقت التنفيذ لـ RSA كان (0.115) وهذا يعتبر الأفضل مقارنة بالخوارزميتين الأخريين.

**Keywords:** template matching, RSA, algorithm, encryption process

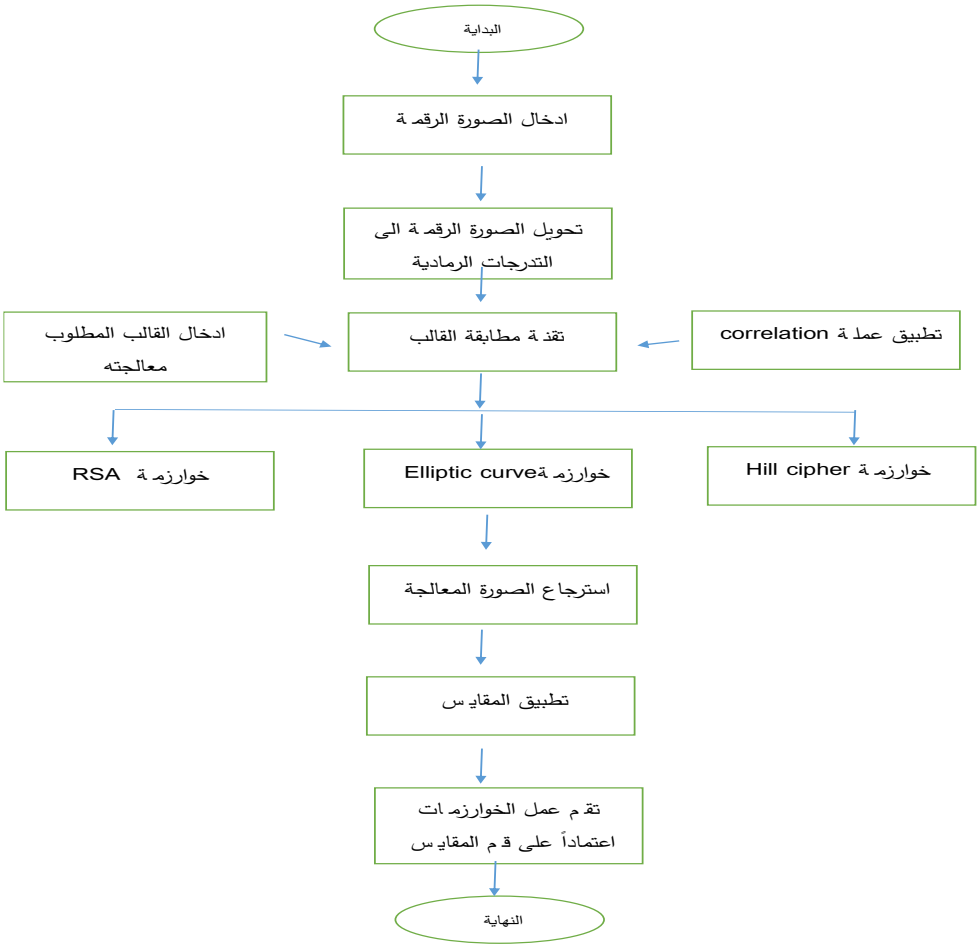
## 1. Aim of the study

يهدف البحث الى تطبيق تقنيه مطابقه القالب على مجموعه من الصور الرقميه من اجل الكشف عن كائن معين في هذه الصوره الرقميه ومن ثم يتم تشفير هذا الكائن في الصوره الناتجه اعتمادا على الخوارزميات ومن ثم ملاحظه الفرق بين نتائج هذه الخوارزميات الثلاث وهي ( RSA , Hill Cipher , Elliptic

Curve) من خلال ملاحظه الخوارزميه التي تعطي اعلى نسبه تشـــفير اعتمادا على المقاييس المســـتخدمه وهي ( SSIM ,PSNR,MSE ,TIME ) وبالتالي يعطي ســـريه عاليه في حال ارســـالها عبر الانترنت لكي يتم اســـترجاعها من قبل المســـتلم باستخدام عمليه فك التشفير اعتمادا على الخوارزميه المستخدمه .

### 1.1 المخطط العام للبحث :

بعد ان تم تحديد الخوارزميات المســـتخدمه في البحث واعتمادا على تقنيه مطابقه القالب في التحديد والكشف عن كائن معين في الصـوره الرقميه وليس معلومات الصـوره بشـكل كامل، وتم تحديد الهيكل العام للبحث من خلال المخطط التالي :




الشكل 1: المخطط العام للبحث

## 2. المقدمة :

الصور هي طريقة لعرض البيانات وتوثيقها بصريًا ، وهو مفهوم قديم تم نحته على الصخور ، ثم ترسم على الورق ، حتى ظهور أجهزة الكمبيوتر ومعها مفهوم الصور الرقمية. الصورة الرقمية هي تمثيل حاسوبي لصورة ثنائية الأبعاد ممثلة بالأصفار والآحاد (0-1). كل صورة رقمية على الكمبيوتر مكونة من بيكسلات ، البكسل هو أصغر وحدة في الصورة ، وكل صورة عبارة عن مصفوفة تحتوي على كلما زاد عدد وحدات البكسل في صفوف وأعمدة وحدات البكسل ، زادت حدة الصورة. صور رقمية من أوائل

تم تحويل كل صوره رقميه ملونه الى صوره ذات تدرجات رماديه ( grayscale ) لكي يتم معالجتها باستخدام خوارزميه التشفير المحدده وكما في الشكل التالي:

الصورة الرمادية الصورة الملونة

الشكل 2: تحويل صورة ملونة الى صورة رمادية ذات تدرجات رمادية .

عشرينيات القرن الماضي ، عندما تم إنشاء نظام لإرسال الصور من لندن إلى نيويورك عبر المحيط الأطلسي [1].

يعني التلاعب بالصور الرقمية أكثر من مجرد عملية تزيين وإدراج الصور تظهر بعض الزخارف والرسومات الموجودة عليها لاحقًا في شكل مختلف عن الشكل الأصلي ، ولكن تم التلاعب بها رقميًا في الصور ، لكن من الناحية العملية لا يهتمون بهذا الجانب من معالجة الصور على الإطلاق ، كما هو الحال هنا ركز على ترميز الصور رقميًا بشكل صحيح وإيجاد طرق لمعالجة هذه البيانات الرقمية بحيث تكون هذه الصور أو يمكن استخدام المعلومات التي تحملها الصورة بواسطة جهاز ، سواء كان جهاز كمبيوتر أو روبوتًا أو آلات أخرى.تُستخدم عمليات معالجة الصور الرقمية في العديد من المجالات مثل التعرف على الأنماط أوالغرض والمجالات الصناعية مثل كشف الورم وتأكيده بالصور الشعاعية في المجال الطبي من امتلاء الحاوية إلى حد معين ونظام المراقبة ومناطق الأمان الأخرى [2].

في معظم مشكلات اكتشاف الكائنات في رؤية الكمبيوتر ومعالجة الصور ، من الضروري عادةً التعرف على التشابه بين المشاهد المختلفة المعروضة على النظام وقياسه. يعد اكتشاف الكائنات في الصور والتعرف عليها موضوع بحث رئيسي في مجتمع رؤية الكمبيوتر ، ومن بينها ، تعد تقنية مطابقة القالب طريقة شائعة جدًا لاكتشاف الكائنات وإيجاد مقياس التشابه بينها للعثور على الأجزاء المراد اكتشافها. تحاول مطابقة القالب الإجابة على أحد أبسط الأسئلة حول الصورة ، نظرًا لوجود كائنات محددة في الصورة ومكان وجودها. القالب هو وصف للكائن (وبالتالي الصورة نفسها) ويستخدم كقالب للبحث عن الصور عن طريق حساب مقياس الاختلاف بين القالب وجميع الأجزاء الممكنة من الصورة التي قد تتطابق مع القالب. إذا أحدثت أي من هذه الخطوات اختلافًا طفيفًا ، فقد تم اعتبارها تكرارا محتملا لهذا الكائن. مطابقة الأنماط هي تقنية متقدمة لرؤية الآلة تحدد تلك الأجزاء من الصورة التي تتطابق مع نمط صورة معين. تتضمن بعض تطبيقاته الواسعة مطابقة موقع الكائن واكتشاف حافة الصورة لرسم خرائط المسار وتقنيات تسجيل الصور للروبوتات المتنقلة ، والتي لها أيضًا تطبيقات في التصوير الطبي ,[3] [4].

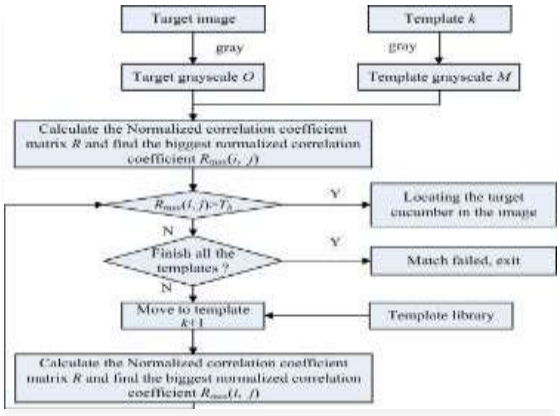
## 2.1 Template Matching Concept

المفهوم الأساسي لمطابقة القالب هو عملية البحث عن ملفات موقع الصور الفرعية تسمى القوالب في صورة ما. هناك العديد من الطرق التي يمكن استخدامها للانعكاس. يناقش هذا المفهوم تطبيق مطابقة القالب لمطابقة الصور الصغيرة ، والتي هي أجزاء من صورة أكبر ، وبمجرد العثور على العديد من القوالب المقابلة ، يمكن استخدام مراكزها كنقاط تحكم مقابلة لتحديد معلمات المطابقة. تتضمن مطابقة القالب مقارنة قالب معين بنوافذ من نفس الحجم في صورة ما وتحديد النافذة الأكثر تشابهًا مع القالب [5]. تتكون خوارزميات مطابقة القالب الأساسية من التحقق من كل موقع في الصورة لحساب دالة تشويه تقيس التشابه بين القالب والصورة. ثم التقط الحد الأدنى من التشويه أو الحد الأقصى لموضع الارتباط ، حدد موقع القالب في الصورة الممسوحة ضوئيًا .مقاييس التشويه النموذجية هي مجموع التباين المطلق ومجموع التباين التربيعي من ناحية أخرى ، من حيث مطابقة القالب ، عادةً ما يتم استخدام الارتباط المتبادل العادي ( NCC) لقياس التشابه. من أجل تحديد مناطق مطابقة ، تحتاج الطريقة إلى مقارنة عينة الصورة بالصورة المصدر عن طريق تمرير قالب. بتحريك القالب ، تقيس العملية التشابه بين المناطق في صورة القالب والصورة المصدر. في كل موقع ، يتم حساب مقياس للإشارة إلى مدى تشابه التصحيح مع منطقة معينة من صورة المشهد. ثم تعثر العملية على الحد الأقصى أو الحد الأدنى للموقع في الصورة الناتجة عن طريق القياس [6].

## 2.2 Template Matching techniques

تقنية في معالجة الصور الرقمية للعثور على أجزاء صغيرة من الصورة تتطابق مع صورة القالب. يمكن استخدامه في التصنيع ، كجزء من مراقبة الجودة ، كطريقة للتنقل عبر الروبوت المتحرك ، أو كطريقة لاكتشاف الحواف في الصور. تعد طريقة مطابقة القالب واحدة من أهم تقنيات التعرف على الأشياء ، في مجال معالجة الإشارات الرقمية ومعالجة الصور ، فهي أساس تتبع

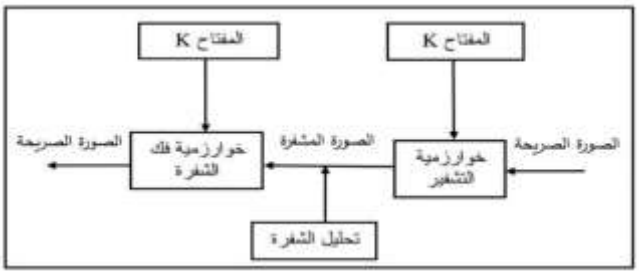
الكائن في مجال رؤية الكمبيوتر. يتم إجراء مطابقة القالب التقليدية من خلال الارتباط بين صورة قالب التدرج الرمادي w والصورة ذات التدرج الرمادي المصفاة f ، حيث يتم تحديد موضع القالب في الصورة المرشحة. يمكن إنجاز هذه المهمة عن طريق قياس التشابه بين صور القالب والصور المرشحة لتحديد وتوطين وجود مثيلات الكائن في الصور. عند تطبيق هذه الطريقة على صورة ملونة ، يجب تحويل الصورة إلى تدرج رمادي أو تحللها إلى مكونات RGB الخاصة بها للمعالجة المنفصلة. يتم تطبيق تقنيات مطابقة القوالب على الصور الملونة عن طريق إنشاء تحويلات فورييه الرباعية للقالب والصور الملونة المرشحة ، ثم ربط هذه التحويلات عبر الارتباط. علاوة على ذلك ، تم تحسين هذا النهج من خلال تمثيل كل من الصور والقوالب على أنها تنسيقات ذات طبقات متعددة الدقة لتقليل وقت المعالجة. تم تنفيذ الخوارزمية المقترحة باستخدام وظائف Matlab وتطبيقها على صور وقوالب مختلفة. هذه التقنية هي أحد المجالات التي حظيت باهتمام كبير مؤخرًا. لقد تحولت إلى ثورة في مجال الرؤية الحاسوبية. توفر مطابقة القوالب بُعدًا جديدًا لقدرة معالجة الصور ، وعلى الرغم من وجود العديد من المحاولات لحل المشكلات المختلفة في هذا المجال ، إلا أن المفاهيم الأحدث تظهر دائمًا في هذا المجال الصعب. في هذه الدراسة ، تمت مناقشة تقنيات مختلفة وتم اقتراح هندسة طيفية جديدة قائمة على FPGA لقياس التشابه السريع. الشكل (3) يوضح خوارزمية عمل تقنية مطابقة القالب [8] ,[7].




الشكل 3:خوارزمية عمل تقنية مطابقة القالب

### 2.3 المفهوم العام للتشفير

علم التشفير أو التشفير معروف منذ العصور القديمة حيث كان يستخدم في المجال العسكري. أن الفرعون هو أول شخص قام بتشفير الاتصالات بين مختلف أفرع الجيش. وذكر أن العرب لديهم محاولات قديمة في مجال التشفير. استخدم الصينيون العديد من طرق التشفير والتشفير لنقل الرسائل أثناء الحرب. كان الغرض من استخدامهم للتشفير إخفاء الشكل الحقيقي للرسائل عند وقوعها في أيدي العدو لأنه سيكون من الصعب على العدو فهمها ، وأفضل طريقة تم استخدامها في العصور القديمة كانت طريقة يوليوس قيصر. ، أحد القياصرة الرومان. العالم متصل بشبكات مفتوحة. تستخدم هذه الشبكات لنقل المعلومات إلكترونيا ، سواء بين الناس العاديين أو بين المؤسسات الخاصة والعامة ، سواء كانت عسكرية أو مدنية. يجب أن تكون هناك طريقة ما لحماية سرية المعلومات ، وقد بُذلت جهود هائلة حول العالم ، يمكن من خلالها تبادل البيانات دون الكشف عن محتواها . في المقابل ، يدرك الجميع أهمية التشفير والحاجة المتزايدة له ، خاصة اليوم مع انتشار الإنترنت على نطاق واسع والسرقة المتكررة للمعلومات والبيانات الشخصية. تكمن أهميته في الحفاظ على سرية المعلومات المهمة والحساسة ومنعها من الوصول إلى الأشخاص غير المرغوب فيهم. يقلل التشفير أيضًا من كمية المعلومات التي يتم نقلها عبر الضغط. البيانات ، والتأكد من هوية مرسل الرسالة . يُعرَّف التشفير بأنه عملية تحويل البيانات من شكلها الطبيعي إلى شكل آخر غير مفهوم من خلال التلاعب الخوارزمي المعقد لحماية البيانات أو إرسالها إلى أطراف أخرى بطريقة آمنة ، مما يضمن أن الأشخاص المصرح لهم فقط هم من يمكنهم عرض هذه البيانات ولكي تكون كذلك. قادرون على قراءة محتوياته ، يجب عليهم أولاً فتح تشفير تلك البيانات أو المعلومات ، لأن فتح التشفير هو عملية إعادة البيانات أو المعلومات من شكلها المشفر إلى شكلها الأصلي وطبيعتها من أجل قراءة محتوياتها ، وهذا يمكن فقط يتم ذلك من خلال معرفة المفتاح المستخدم في عملية التشفير ، وبالتالي يمنع كل شخص ليس لديه المفتاح من قراءة ومعرفة محتويات البيانات أو المعلومات المشفرة. توضح الأشكال ( (4) نظام تشفير ) ,[9] .[10]




الشكل 4: نظام التشفير

حيث تنقسم إلى قسمين:

اولاً : خوارزمية التشفير :-

هي مجموعة من العمليات المصممة لتحويل صورة صريحة إلى صورة مشفرة ، ويعتمد أمان أنظمة التشفير الحديثة على مفتاح التشفير (k). تعتمد قوة وفعالية التشفير على عاملين أساسيين: 1. المفتاح يأخذها ويسمى الخوارزمية 2. طول المفتاح.

ثانياً :خوارزمية فك التشفير :

العملية العكسية ، أي تحويل صورة مشفرة إلى شكلها الأصلي [11].

مراحل خوارزمية العمل المقترحة :

المرحلة الاولى : ادخال الصورة الرقمية :

يتم في هذه المرحله تحويل الصوره الرقميه والتي تم تحديدها مسبقا بالنوع ( jpg.) باحجام مختلفه تتراوح من 475.7KB و 750.6KB من ثم تحويلها الى مصفوفه رقميه.

المرحلة الثانية :- المعالجة الاولية لتفاصيل الصورة الرقمية :

هذه الخطوه اضـــافه تقنيه الحشـــو ( padding ) الى اطار الصـوره الرقميه، حيث يتم تكرار معلومات الصـوره الاصـليه عن طريق تقنيه ( pixel replication padding ) لتجنب فقدان معلومات الاطار الاصـلي للصـوره اثناء عمليه المعالجه ،ومن ثم تحويل كل صـــوره رقميه ملونه ناتجه الى صـــوره ذات تدرجات رماديه.

المرحلة الثالثة :-

اولاً المعالجة باستخدام خوارزمية RSA : -

يتم في هذه المرحله اعاده تحديد مقياس ( output) من بيانات عدديه صحيحه الى المجال [1-0] من اجل اعطاء دقه مضاعفه الصوره الرقميه ومن ثم تحديد قيمة الانحراف المعياري ( standard deviation) بعد ذلك يتم تحديد قيمه المفتاح العام (public key) والمفتاح الخاص ( private key) حيث يتم تحديد قيم هذه المفاتيح اعتمادا على الخطوات التاليه ,[12] [13].

اولاً : ال key generation او ال key creation يتم تكوين المفتاح العام بالاعتماد على الخطوات التالية :

خطوة 1) توليد عددين اوليين كبيرين عشوائياً p , q ويكون العدد المحدد لكليهما عدد اولي لا يقبل القســمه الا على نفســه او على واحد [14].

خطوة 2 ) حســاب قيمة n والناتجة من عملية ضــرب ال ( p) في ال ( q).

$$n= p*q$$

خطوة 3) حســاب قيمة الاوليرΦ (n) من خلال المعادلة التالية .

$$\Phi (n) =(p-1)(q-1)$$

خطوة 4)اختيار عدد صــحيح عشــوائياً e على ان يكون العدد اكبر من ال واحد واصــغر من الاوليرΦ (n) حيث ان قيمة ال e وقيمة الΦ (n) لا يوجد بينهما قواسم مشتركة .

$$1< e < \Phi(n)$$

الصيغة العامة لتوليد المفتاح هيا

$$Key= ( n , e)$$

ثانيا : Image Encryption -:

هذه الخطوة يتم فيها تشفير الصورة بالاعتماد على المفتاح العام بتطبيق المعادلة الاتية:

$$C=m^e \bmod n$$

C تمثل الصورة المشفرة M . الصورة قبل التشفير . eالرقم الأول في ال key

n يمثل الرقم الثاني في ال key ويمكن توضيح عمل خوارزمية ال RSA من خلال المخطط التالي:


الشكل 5:خوارزمية ال RSA

نقوم بتطبيق هذه الخوارزمية على القالب الذي تم تحديده بواسطة تقنية مطابقة النموذج المطبق على الصورة الاصلية لتأمين وتشفير المقطع المحدد من الصورة الاصلية لتشفيره باستخدام خوارزمية RSA كما موضح بالشكل التالي .

(a) المقطع المحدد للتشفير من الصورة الاصلية

(b) المقطع المشفر باستخدام خوارزمية ال RSA

(c) المقطع المشفر ياستخدام خوارزميةHill

(d) المقطع المشفر باستخدام خوارزمية Elliptic

الشكل 6: التشفير باستخدام خوارزمية( RSA ,Hill, Elliptic)

ثانياً : المعالجة باستخدام ( Hill cipher) :-

تم في هذه المرحله تحديد مقياس ( OUTPUT) من بيانات عدديه صحيحة الى المجال [1-0] من اجل اعطاء دقة مضاعفه للصوره الرقميه ومن ثم تحديد الانحراف المعياري (STADARD DIVIION)، بعد ذلك يتم تحديد مصفوفه قالب

الكائن الذي تم تحديده من الصـــوره الاصـــليه من اجل المعالجه وتحديد متجه المفتاح الخاص ومن ثم تطبيق المعادله التاليه [15], [16]:

C=K*P MODE 255

حيث ان : تمثل مصفوفة القالب :P

قيمة المفتاح الخاص :K

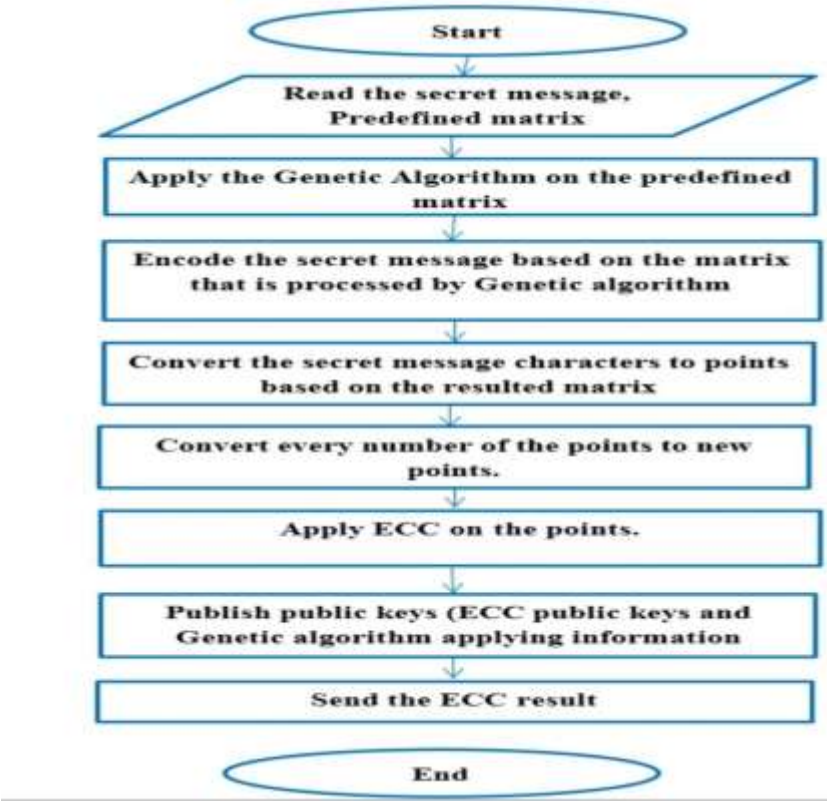
القالب بعد تطبيق التشفير :C

ويمكن توضيح عمل خوارزمية ال Hill Cipher من خلال المخطط التالي


الشكل 7:يوضح عمل خوارزمية ال Hill Cipher

ثالثا : المعالجة باستخدام خوارزمية ال Elliptic Curve:-

إنَّ التشـــفير باســـتخدام المنحنيات الإهليلجية ECC، تماماً مثلُ التشـــفير RSA، هو نوع من مفاتيح التشـــفير العامة، فالفكرة الرئيسية منها هي القفل. إذا أردتُ أنْ أرسلَ رسالةً سريةً لك فإنني أطلب منك أن ترسـل لي قفلاً مفتوحاً تمتلك أنت فقط مفتاحه. ثم أقومُ بوضـع الرسـالة في صـندوق، أقفلها بذلك القفل وأرسـلها لك. الشـيُء الجيد في ذلك الأسلوب هو أنَّه يمكنُ إرسال الرسالة عبر قنوات غير آمنة فحتَّى لو كان هناك طرف ثالثٌ يراقب الإرســال فإنه لا يملك مفتاح القفل وأنه لا يحتاج كل منا لمفتاح خاص به. بإمكانك أن ترسـل رسـائلاً سـريةً للكثير من الأشـخاص بهذه الطريقة بدون الاضـطرار لأن تعطيَ أيَّ مفتاح [17] في مفتاح التشـفير العام يتم تشـفير الرسـائل باسـتخدام معلومات رياضـية معينة، والتي تشـكل المفتاح العام، بحيث أنَّ فتحَ القفل والتشـفير يشـبه تماماً كسـرَ ذلك القفل. فك التشـفير لا يتمُّ إلا عن طريق مفتاحٍ رياضـيٍ خاصٍ، لدرجةِ أنّه أقرب للمسـتحيل أنْ تحددَ فيما إذا كنتَ تعرف المفتاح العام الذي يقوم بالتشـــفير. في تشـــفير RSAالمفتاح العام يتضـمن أعداداً طبيعيةً، والتي تسـتخدم في الحاسبات لتشفير الرسائل. لفكّ تشفيرِ الرسائل، تحتاج أن تعرفَ قواســـم (عوامل) تلك الأعداد الطبيعية، فإذا كانت تلك الأعداد كبيرةً جداً فإنَّ العوامل تأخذ الكثير من الحســـابات لكي تقوم بفك الشيفرة أو بالأحرى فإنَّه مستحيل أنْ تفكَّها . فقط الحواسيب التي تمتلك المفتاح الخاص (قواسم العدد المشفر) هي التي تستطيع أن تقوم بفكّ تشـــفير الرســـالة بســـهولة )لمزيد من المعلومات حول التشـــفير [18]. ويمكن توضـــيح عمل خوارزمية ال Elliptic curv في الشكل رقم (8))




الشكل 8:يوضح عمل خوارزمية ال Elliptic curve

تطبيق المقاييس :-

جدول ( 1) جدول لمعدل المقاييس للصورة الاولى

| ت | نوع المقياس | نوع المعالجة المستخدمة | القيمة |
|---|---|---|---|
| 1 | PSNR | RSA | 5.373 |
| | | Hill Cipher | 9.556 |
| | | Elliptic curve | 8.727 |
| 2 | SSIM | RSA | 0.010 |
| | | Hill Cipher | 0.171 |
| | | Elliptic curve | 0.027 |
| 3 | MSE | RSA | 18869.7 |
| | | Hill Cipher | 7201.29 |
| | | Elliptic curve | 8727.37 |

بعد اجراء المعالجات السابقة على الصور الرقمية ، تم تطبيق مجموعة المقاييس لتوضيح نسبة التشفير مقارنة بالصور الاصلية ، حيث كانت نتائج المقاييس على صور مختلفة كما في الجدول التالي

وزمن تنفيذ للمعالجات المستخدمة في الصورة الاولى موضح بالجدول التالي

جدول( 2 ) يوضح فيه زمن تنفيذ المعالجات

| ت | نوع المعالجة المستخدمة | زمن التنفيذ |
|---|---|---|
| 1 | RSA | 0.115 |
| | Hill Cipher | 0.391 |
| | Elliptic curve | 0.258 |

نتائج المقاييس المطبقة على الصورة الثانية

جدول ( 3 ) معدل المقاييس بالنسبة للصور الثانية

| ت | نوع المقياس | نوع المعالجة المستخدمة | القيمة |
|---|---|---|---|
| 1 | PSNR | RSA | 3.673 |
| | | Hill Cipher | 10.086 |
| | | Elliptic curve | 7.242 |
| 2 | SSIM | RSA | 0.136 |
| | | Hill Cipher | 0.212 |
| | | Elliptic curve | 0.371 |
| 3 | MSE | RSA | 27906.4 |
| | | Hill Cipher | 6375.6 |

| | | | |
|---|---|---|---|
| | | Elliptic curve | 12270.6 |

.

وزمن تنفيذ للخوارزميات المستخدمة في الصورة الثانية موضح بالجدول التالي

الجدول( 4) جدول لزمن تنفيذ الخوارزميات على الصورة الثانية

| ت | نوع المعالجة المستخدمة | زمن التنفيذ |
|---|---|---|
| 1 | RSA | 0.251 |
| | Hill Cipher | 0.371 |
| | Elliptic curve | 0.286 |

نتائج المقاييس المطبقة على الصورة الثالثة :-

الجدول( 5) جدول لمعدل المقاييس بالنسبة للصور الثالثة .

| ت | نوع المقياس | نوع المعالجة المستخدمة | القيمة |
|---|---|---|---|
| 1 | PSNR | RSA | 4.670 |
| | | Hill Cipher | 10.8509 |
| | | Elliptic curve | 10.122 |
| 2 | SSIM | RSA | 0.0202 |
| | | Hill Cipher | 0.0631 |
| | | Elliptic curve | 0.04240 |
| 3 | MSE | RSA | 22184.8 |
| | | Hill Cipher | 5345.52 |
| | | Elliptic curve | 6322.33 |

وزمن تنفيذ للخوارزميات المستخدمة في الصورة الثالثة موضح بالجدول التالي

جدول (6) جدول لزمن تنفيذ الخوارزميات على الصورة الثالثة

| ت | نوع المعالجة المستخدمة | زمن التنفيذ |
|---|---|---|
| 1 | RSA | 0.260 |
| | Hill Cipher | 0.536 |
| | Elliptic curve | 0.290 |

نتائج المقاييس المطبقة على الصورة الرابعه :-

جدول(7) جدول لمعدل المقاييس بالنسبة للصور الرابعة .

| ت | نوع المقياس | نوع المعالجة المستخدمة | القيمة |
|---|---|---|---|
| 1 | PSNR | RSA | 5.15411 |
| | | Hill Cipher | 10.0833 |
| | | Elliptic curve | 7.18411 |
| 2 | SSIM | RSA | 0.21061 |
| | | Hill Cipher | 0.35088 |
| | | Elliptic curve | 0.2802 |
| 3 | MSE | RSA | 12521.9 |
| | | Hill Cipher | 6379 |
| | | Elliptic curve | 11547.9 |

وزمن تنفيذ للخوارزميات المستخدمة في الصورة الرابعة موضح بالجدول التالي

جدول (8) جدول لزمن تنفيذ الخوارزميات على الصورة الرابعة

| ت | نوع المعالجة المستخدمة | زمن التنفيذ |
|---|---|---|
| 1 | RSA | 0.251 |
| | Hill Cipher | 0.911 |
| | Elliptic curve | 0.280 |

والجدول التالي يوضح معدل النتائج التي تم الحصول عليها في الجداول السابقة :

جدول (9) معدل المقاييس باستخدام ال (RSA )

| ت | المقياس | المعدل |
|---|---|---|
| -1 | MSE | 20370.7 |
| -2 | PSNR | 4.717 |
| -3 | SSIM | 0.0942 |

جدول (10) معدل المقاييس باستخدام ال (Elliptic )

| ت | المقياس | المعدل |
|---|---|---|
| -1 | MSE | 9,717.05 |
| -2 | PSNR | 8.318 |
| -3 | SSIM | 0.2755 |

جدول (11) معدل المقاييس باستخدام ال (Hill )

| ت | المقياس | المعدل |
|---|---|---|
| -1 | MSE | 6325.35 |
| -2 | PSNR | 10.143 |
| -3 | SSIM | 0.34497 |

## 3. Conclusions

The template matching technique with encryption using algorithms (RSA, Hill cipher, Elliptic curve) was applied to a group of digital

images. In this research, a number of conclusions were reached after applying and implementing the algorithms specified in the research, as shown in the tables, where the conclusions were reached. next:

1. The Mean Squared Error (MSE) of RSA algorithm was better than Elliptic curve and Hill Cipher algorithms.
2. The RSA algorithm, based on the PSNR scale, gave better results compared to the other two algorithms.
3. Depending on the scale (SSIM), the results showed that the (RSA) algorithm gave better results compared to the other two algorithms.
4. Execution time using RSA algorithm was faster than the other two algorithms.

## 4. الاستنتاجات

تم تطبيق تقنية مطابقة القالب مع التشفير بإستخدام الخوارزميات (RSA, Hill cipher , Elliptic curve) على مجموعة من الصور الرقمية وقد تم التوصل في هذا البحث الى مجموعة من الاستنتاجات بعد تطبيق وتنفيذ الخوارزميات المحددة في البحث وكما موضح في الجداول حيث تم التوصل ال الاستنتاجات التالية:

١. مقياس متوسط الخطأ التربيعي (MSE) لخوارزمية (RSA) كان افضل من الخوارزميات Elliptic curve و Hill Cipher.

٢. خوارزمية RSA اعتمادا على مقياس (PSNR) اعطت نتائج افضل مقارنة بالخوارزميتين الاخرتين.

٣. اعتمادا على المقياس (SSIM)اظهرت النتائج انه خوارزمية (RSA) اعطت نتائج افضل مقارنة بالخوارزميتين الاخرتين.

٤. زمن التنفيذ المستغرق بإستخدام خوارزمية (RSA) كان أسرع من الخوارزميتين الاخرتين.

## References


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

[2] ن. ع. حسين, "الصورة الرقمية إحدى ملامح الإعلام الجديد دراسة الصورة الخبرية في موقع:(المدى برس)," *مجلة بحوث الشرق الأوسط*, vol. 51, pp. 413–444, 2019.

[3] N. S. Hashemi, R. B. Aghdam, A. S. B. Ghiasi, and P. Fatemi, "Template matching advances and applications in image analysis," *arXiv Prepr. arXiv1610.07231*, 2016.

[4] Y. Sun, X. Mao, S. Hong, W. Xu, and G. Gui, "Template matching-based method for intelligent invoice information identification," *IEEE access*, vol. 7, pp. 28392–28401, 2019.

[5] J. N. Sarvaiya, S. Patnaik, and S. Bombaywala, "Image registration by template matching using normalized cross-correlation," in *2009 international conference on advances in computing, control, and telecommunication technologies*, 2009, pp. 819–822.

[6] L. Ding, A. Goshtasby, and M. Satter, "Volume image registration by template matching," *Image Vis. Comput.*, vol. 19, no. 12, pp. 821–832, 2001.

[7] Q. N. N. Le, A. Bhattacharyya, M. T. Chembakasseril, and R. Hartanto, "Real-time sign detection and recognition for self-driving mini rovers based on template matching and hierarchical decision structure.," in *ICAART (1)*, 2020, pp. 208–215.

[8] R. Brunelli, *Template matching techniques in computer vision: theory and practice*. John Wiley & Sons, 2009.

[9] 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.

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

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

[12] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang,

"An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem," *Int. J. Bifurc. Chaos*, vol. 30, no. 15, p. 2050233, 2020.

[13] G. Ye, K. Jiao, and X. Huang, "Quantum logistic image encryption algorithm based on SHA-3 and RSA," *Nonlinear Dyn.*, vol. 104, pp. 2807–2827, 2021.

[14] D. M. Alsaffar *et al.*, "Image encryption based on AES and RSA algorithms," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1–5.

[15] H. Touil, N. EL AKKAD, and K. SATORI, "Text encryption: hybrid cryptographic method using Vigenere and Hill Ciphers," in *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, 2020, pp. 1–6.

[16] M. Essaid, I. Akharraz, and A. Saaidi, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, 2019.

[17] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," *Mathematics*, vol. 10, no. 20, p. 3878, 2022.

[18] G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Eng. J.*, vol. 61, no. 9, pp. 6785–6795, 2022.