Journal of Education and Science
Vol. 28, No.4, 2019, pp.189-205
ISSN 1812-125X
http://edusj.mosuljournals.com

Encryption and Compression Digital Video Files using Artificial Neural Networks and Genetic Algorithm

Hasan M.A. Anwer
Department of Software Engineering
College of Computer Science and Mathematics
University of Mosul
hasanmaher@uomosul.edu.iq
DOI: 10.33899/edusj.1970.163335

Received 20/ 06/ 2018 **Accepted** 02 / 10 / 2018

Abstract

The research and studies of encryption and compression of digital files to the confidentiality and ease of dealing with networks and the Internet, by reducing the size of files transmitted through multimedia, and also used to increase the confidentiality of information transmitted.

The purpose of the research is to encrypt and compress colored digital video files using artificial neural networks and genetic algorithm, The digital video file is entered into Audio Video Interleave (AVI) and cut into a set of frames, Each frame is then analyzed into the three color segments (red, green and blue) And an audio input from the Waveform Audio File Format (WAV) type (which represents the encryption key), the encoded frame was then inserted into the compression algorithm, A hybrid compression method was adopted which is considered as one of the solutions that reduces the size of the required data on the one hand and gives it a secret on the other, Where it was segmentation and clustering the encoded frames into a cluster of clusters (The optical pixels), which have been introduced into the artificial neural network (back propagation network), The genetic algorithm has been used to calculate the weight values of each cell of the network. The decryption and decompression is then performed, and by using a set of testing and comparison tools that showed that the results were consistent with the research requirements, and Matlab R2017b was used to implement research algorithms.

Keywords: Encryption, compression, clustering, digital video, BPN, GA.

تشفير وكبس ملفات الفيديو الرقمي باستخدام الشبكات العصبية الاصطناعية والخوارزمية الجينية

حسن ماهر أحمد أنور
قسم هندسة البرمجيات
كلية علوم الحاسوب والرياضيات
جامعة الموصل
hasanmaher@uomosul.edu.iq

DOI: 10.33899/edusj.1970.163335

الاستلام 2018 / 06 / 20 القبول 2018 /10 / 02

الخلاصة

تهدف البحوث والدراسات الخاصة بتشفير وكبس الملفات الرقمية إلى سرية وسهولة التعامل مع شبكات الاتصالات والانترنيت، وذلك من خلال تقليل حجم الملفات المنقولة عبر الوسائط المتعددة، وكذلك تستعمل لزيادة سرية المعلومات المنقولة.

يهدف البحث إلى تشفير وكبس ملفات الفيديو الرقمي الملون باستعمال الشبكات العصبية الاصطناعية والخوارزمية الجينية، إذ تم إدخال ملف الفيديو الرقمي من نوع AVI وتقطيعه إلى مجموعة من الأطر ثم تحليل كل إطار إلى الشرائح اللونية الثلاث (الأحمر والأخضر والأزرق) ثم تطبيق بوابة XOR بين كل شريحة ومقطع صوتي مدخل من نوع WAV (والذي يمثل مفتاح التشفير)، تم بعد ذلك إدخال الإطار المشفر إلى خوارزمية الكبس إذ تم العمل على اعتماد طريقة مهجنة للكبس والتي تعتبر كأحد الحلول التي تعمل على تقليل حجم البيانات المطلوبة من جهة وإعطائها سرية من جهة أخرى، إذ تم تقسيم وعنقدة الأطر المشفرة إلى مجموعة من العناقيد (النقاط الضوئية) والتي تم إدخالها إلى الشبكة العصبية الاصطناعية (شبكة انتشار الخطأ خلفيا)، وقد تم الاعتماد على الخوارزمية الجينية في حساب قيم الأوزان لكل خلية من خلايا الشبكة، وأخيرا عملية فك التشفير والكبس، وعن طريق استعمال مجموعة من أدوات الفحص والمقارنة تبين أن النتائج كانت متوافقة مع متطلبات البحث، وتم العمل على استعمال لغة Matlab R2017b لتنفيذ خوارزميات البحث.

الكلمات المفتاحية: تشفير، كبس، العنقدة، الفيديو الرقمي، شبكة الانتشار العكسي، الخوارزمية الجينية.

1-المقدمة Introduction:

في السنوات الأخيرة ازدادت ضخامة المعلومات الصورية المخزونة التي تعالج رقمياً في مختلف الاختصاصات والتطبيقات، لهذا أصبحت عملية كبس البيانات وتشفيرها حقلاً مهماً في العديد من التطبيقات، إذ أن معظم أنظمة التشغيل الحديثة تعتمد على الرسومات أو الصور، ولكون بيانات الفيديو الرقمي تحتل مساحة كبيرة في الذاكرة أدى ذلك إلى الاهتمام الكبير في إيجاد تقنيات لكبس البيانات الفيديوية أو الصورية[1].

لا يزال كبس البيانات يمثل حقلا مهما جدا في مجالات كثيرة منها نقل المعلومات خلال شبكة الاتصالات الرقمية فضلا عن أهميته في تقليل مساحات الخزن في الذاكرة المستعملة لخزن هذه البيانات وأهميته في الاستعمال الأمثل للإمكانيات والموارد المتوفرة مما يؤدي ذلك إلى تقليل الكلفة بشكل عام، من جهة أخرى يؤدي إلى تقليل وقت نقل الملف المستعمل وتقليل حزمة الإرسال (Bandwidth).[2]

إن الحاجة لتطوير كثير من الطرائق لتحليل الإشارة والمقاطع الفيديوية لا تكفي فلا بد من وضع وتطوير طرائق لكبسها، إذ إن هناك عدة تقنيات لكبس البيانات ويعتمد اختيار التقنية على نوع البيانات المراد كبسها فبعض هذه التقنيات تلائم الصور النصية وأخرى تلائم الصور الثابتة وغيرها تلائم الصور المتحركة[3].

2-الدراسات السابقة Previous studies:

مع تطور أجهزة الحاسوب الرقمية التي دخلت تطبيقاتها كافة مجالات الحياة وأصبح التطور في مجال الحاسوب وتطبيقاته المختلفة التي تتراوح من التطبيقات الصناعية إلى الأبحاث الفضائية احد أهم مقاييس تطور الدول في العصر الحديث فقد قدم العديد من الباحثين دراسات متنوعة في هذا المجال، ففي عام 2017 اقترح الباحثان Choudhary وAbrol بحثا تم من خلاله تشفير صورة رقمية بطريقة مبنية على الخوارزمية الجينية التي تستعمل لتوليد المفتاح بمساعدة مولد الأرقام العشوائية، إذ يمر الجيل الرئيسي بعدد من الخطوات لزيادة تعقيد المفتاح فقد تم تنفيذ خوارزميات جينية مع بتات التقليب (bits flipping) لتشفير وفك تشفير تدفق البيانات ويتم تطبيق عملية التشفير على ملف ثنائي بحيث يمكن تطبيق الخوارزمية على أي نوع من أنواع الصور[4].

وفي عام 2017 قدم الباحثان Kin و Coker بحثا تم فيه كبس الفيديو الرقمي باستعمال الشبكات العصبية الاصطناعية إذ عمد الباحثان على تقديم نظامًا للتشفير التلقائي يتكون من شبكات عصبية تلافيفية متكررة ثنائية الاتجاه (Recurrent Convolutional Neural Networks) لكبس الفيديو واستنتج الباحثان من خلال النتائج الى أن شبكات RCNN يمكن أن تتعلم من المعلومات الزمنية الموجودة في إطارات ثابتة متتالية ولكنها تفشل في تحقيق معدلات كبس وسرعات متطورة جدًا بسبب التعقيدات الحسابية[3].

وفي عام 2018 قدم الباحثان Zhang و Wu بحثا اقترحا فيه طريقة لتقليل نسبة فقد البيانات في الصور الرقمية المكبوسة عبر دمج معيار الدقة في تصميم الشبكة العصبية بحيث لا يمكن إسقاط أو تشويه أي هياكل صغيرة ومميزة من الصورة الأصلية علاوة على ذلك تم تصميم الشبكة العصبية المضادة للقطع الأثرية للعمل على مجموعة من معدلات بتات الكبس بدلاً من مجموعة ثابتة كما في الماضي واظهرت النتائج التجريبية أن الطريقة المقترحة يمكنها استعادة تفاصيل الصورة الدقيقة التي يتم تدميرها أو تفتيتها بخوارزميات أخرى[5].

3- المخطط العام للبحث General Research Plan:

إن الحاجة لتطوير كثير من الطرائق لتحليل الإشارات والصور المتتالية لا تكفي ولكن يجب أن يتم وضع الطرائق لتشفيرها وكبسها وتطويرها، وقد تم العمل على اعتماد طريقة مهجنة لتشفير وكبس ملفات الفيديو الرقمي والتي تعتبر كأحد الحلول التي تعمل على تقليل حجم البيانات المطلوبة من جهة وإعطائها سرية من جهة أخرى.

تم في هذا البحث إدخال ملف الفيديو وتقطيعه إلى مجموعة من الأطر (وهي بمثابة صور رقمية متتالية بفترات زمنية محددة) ثم تحليل كل إطار إلى الشرائح اللونية الثلاث (الأحمر والأخضر والأزرق) ثم تشفير كل شريحة ليتم إدخالها إلى الشبكة العصبية (شبكة انتشار الخطأ خلفيا)، وقد تم الاعتماد على الخوارزمية الجينية في حساب قيمة الأوزان لكل خلية من خلايا الشبكة، وكما في المخطط الانسيابي (1).

المخطط الانسيابي (1): المخطط العام للبحث

تم العمل على إدخال ملفات الفيديو الرقمي ذات الامتداد (AVI)، وذلك لأنها تحتوي على صيغة الترميز الحقيقي المستعمل بالكبس للفيديو والصوت، إذ أن ملفات الفيديو من نوع (AVI) تعد من أكثر ملفات الفيديو الرقمي شهرةً، وهي من أكثر الملفات المستعملة في الأبحاث العلمية، وأن AVI هي اختصار لتداخل الفيديو والصوت (Audio/Video Interleaved) إذ أخذت الحروف الأولى من الكلمات الثلاث[1].

دُعِمَ هذا النوع من الملفات من شركة مايكروسوفت (Microsoft) فملفاته ذات امتداد (AVI.) تحت بيئة نظام التشغيل ويندوز (Windows)، وإن ملفات AVI تتكون من سلسلة من الصور من نوع BMP وبيانات صوتية رقمية من نوع WAV [3][6].

4- التشفير والعنقدة Encryption and clustering:

علم التشفير (Cryptography) هو العلم الذي يعنى بالطرق التي تعمل على حماية المعلومات ونقلها في مجال واسع، إذ أن عملية تشفير البيانات تتم من خلال تحويل البيانات من صيغتها الطبيعية إلى صيغة أخرى غامضة غير قابلة للفهم عبر مجموعة من العمليات والخطوات بهدف حماية البيانات أو إرسالها لأطراف أخرى بطريقة أمنة[7]، وإن فك التشفير هي عملية التحويل من الشكل المشفر الى الصريح إذ تتم عن طريق مفتاح التشفير، وتقسم خوارزميات التشفير حسب طريقة العمل على اجزاء ورموز البيانات إلى نوعين[8]:

أ- **التشفير المقطعي:** يعتمد على مبدأ تقسيم المحتوى الاصلي (نصوص أو صور أو اي شيء آخر) إلى مجموعات متساوية الطول من البتات تسمى بلوكات (Blocks) أو مقاطع ثم تشفير كل مقطع على حدى مثل خوارزمية(Data Encryption Standard (DES.[4]

ب- **التشفير المتصل:** ويعتمد على مبدأ تشفير البيانات المتصل أو جدول البيانات بشكل مستمر إذ يتم توليد مفتاح مستمر يتم دمجه مع البيانات الأصلية بخوارزمية تشفير ذات مفتاح متماثل وغالبا يتم ذلك بعملية XOR المنطقية وهو ما اعتمد عليه البحث.

أما انواع خوارزميات التشفير حسب نوع مفتاح التشفير وفك التشفير:[8]

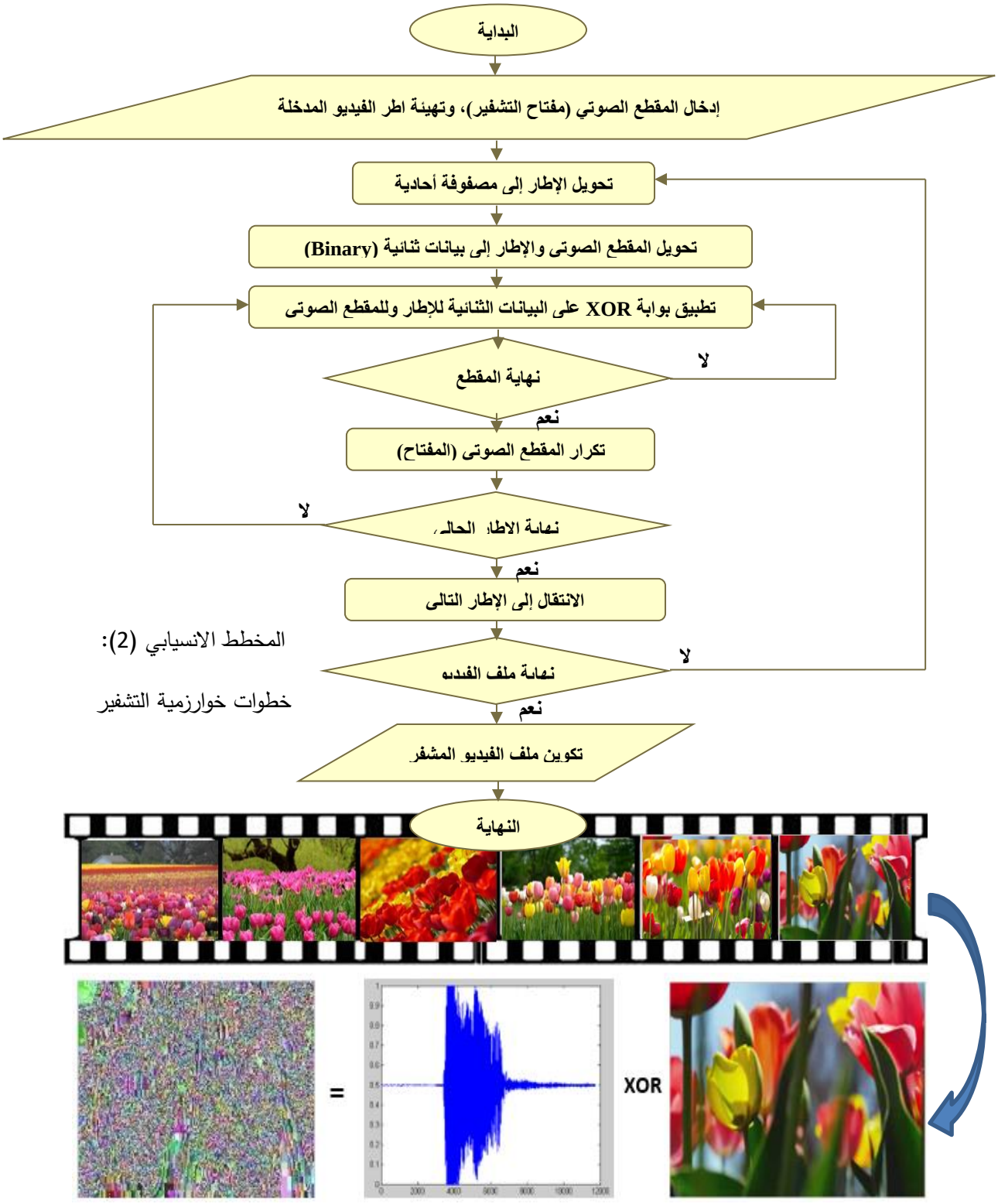
أ- **التشفير المتناظر (symmetric systems):** إذا يستعمل نفس المفتاح في التشفير وفك التشفير حيث يقوم نظام التشفير المتماثل باستعمال نفس المفتاح في التشفير وفك التشفير ومن مزايا التشفير المتماثل انه سهل الاستعمال وسريع.[9]

ب- **التشفير غير المتناظر (asymmetric systems):** يتم استعمال مفتاح للتشفير واخر لفك التشفير وباستعمال هذين الزوجين من المفاتيح إحداهما عام (public) والآخر خاص (private) يستطيع مفتاح واحد منهما فقط أن يقوم بفك الشفرة التي ينشئها الآخر.[9]

أما خوارزمية التشفير فهي مجموعة من العمليات التي تهدف إلى تحويل بيانات أطر الفيديو المدخلة إلى اطر فيديو مشفرة، فبعد الحصول على الشرائح الثلاث الملونة يتم تحويل كل شريحة إلى مصفوفة أحادية البعد ثم يتم العمل على إدخال مقطع صوتي من نوع wav ثم إجراء عملية XOR بين المصفوفة الأحادية والمقطع الصوتي، وكما موضح في الشكل (1)، والمخطط الانسيابي (2)، لتنتج مصفوفة أحادية مشفرة والتي ستطبق عليها خطوات الكبس.

المخطط الانسيابي (2):

خطوات خوارزمية التشفير



الشكل (1): تشفير الإطار الأول من ملف الفيديو

بعد تشفير اطر الفيديو المدخل تم تقطيع كل شريحة لونية إلى مجموعة من النقاط الضوئية (pixels) فمثلا (2*2) إذ يتم في كل مرة إدخال أربعة نقاط ضوئية إلى الشبكة العصبية الاصطناعية.

إن الفكرة العامة من مسألة العنقدة تتلخص بتجزئة مجموعة من البيانات المعطاة إلى مجاميع (عناقيد) إذ أن نقاط البيانات في العنقود الواحد تكون متشابهة مع بعضها البعض أكثر من تلك النقاط في العناقيد الأخرى[10]، إذ أن العنقدة هي عملية تقسيم البيانات إلى مجاميع اعتمادا على بعض المقاييس المتشابهة لهذه المجاميع وتعتبر عملية عنقدة البيانات عملية أساسية ومركزية في الذكاء الاصطناعي إذ يتم تعريف العنقود بواسطة مركز العنقود والطريقة الأكثر شيوعا لإيجاد التشابه بين البيانات ومراكز العناقيد هي الاعتماد على المسافة الاقليدية (Euclidean distance).[11]

إن عملية العنقدة هي مفهوم جديد في مجال الكبس يعمل على تجميع الأشياء مثل النقاط في الصورة التي تحتوي على عامل مشترك أو تمتلك خاصية متشابهة في مجموعة واحدة تختلف فيها عن مجموعات أخرى، قد يكون هذا التشابه بين العناصر في المجموعة الواحدة (العنقود) هو البعد بين كل من هذه العناصر عن نقطة معينة عندها تسمى هذه العملية بالعنقدة (Clustering)، أو قد تكون العنقدة من نوع العنقدة المفاهيمية (Conceptual Clustering) أي أن العناصر في المجموعة (العنقود) لها مفهوم (concept) واحد فيما بينها أي أن العناصر تقسم إلى مجموعات على أساس مبدأ معين وليس على أساس التشابه في مقياس معين، إن الهدف من العنقدة هو تحديد المجاميع الحقيقية (الفعلية) في مجاميع غير معنونة إلا أن تحديد العامل المشترك بين العناصر والذي على أساسه ستحدد جودة عملية العنقدة لن يكون ثابت ولجميع البيانات ولكن سيحدد من قبل المستعمل الذي سيطبق العديد من العوامل لحين إيجاد النتائج من عملية العنقدة التي تناسب احتياجاته، لتبدأ بعدها عملية الكبس.

يعرف الكبس بأنه تقنية تستعمل لتقليل حجم ملف البيانات الرقمية لغرض التقليل من المساحة الخزينة وزيادة سرعة النقل مع الاحتفاظ بالمعلومات الضرورية للبيانات، وان كبس البيانات يعتمد على أنواع البيانات المراد كبسها وحسب تركيبها والخواص التي تحتويها تلك البيانات.[12]

أ- **الكبس بدون فقدان (Lossles Compression):** في هذا النوع من الكبس من الممكن إعادة البيانات التي تم كبسها وبشكل مطابق للبيانات الأصلية، إذ تستعمل خوارزميات هذا النوع بشكل واسع مع ملفات النصوص التي لا تسمح بفقدان أي من معلوماتها أثناء عملية الكبس كما يُستعمل مع تطبيقات الصور الطبية وفي صور الوثائق الأرشيفية.[10][1]

ب- **الكبس بفقدان (Lossy Compression):** هذا النوع من الكبس يتطلب بعض الخسارة من البيانات التي لا يمكن أن تسترد أو يعاد تركيبها بصورة مطابقة للبيانات الاصلية بحيث أن هذا الفقدان لا يكون مؤثرا عند أعادة تركيب البيانات (وهو ما اعتمد عليه هذا البحث) أي ان نسبة التشوه في البيانات قليل جدا وكلما كان التشوه اقل ونسبة الكبس أعلى تكون النتيجة أفضل.[13][2]

5- بناء الشبكة العصبية الاصطناعية والخوارزمية الجينية:

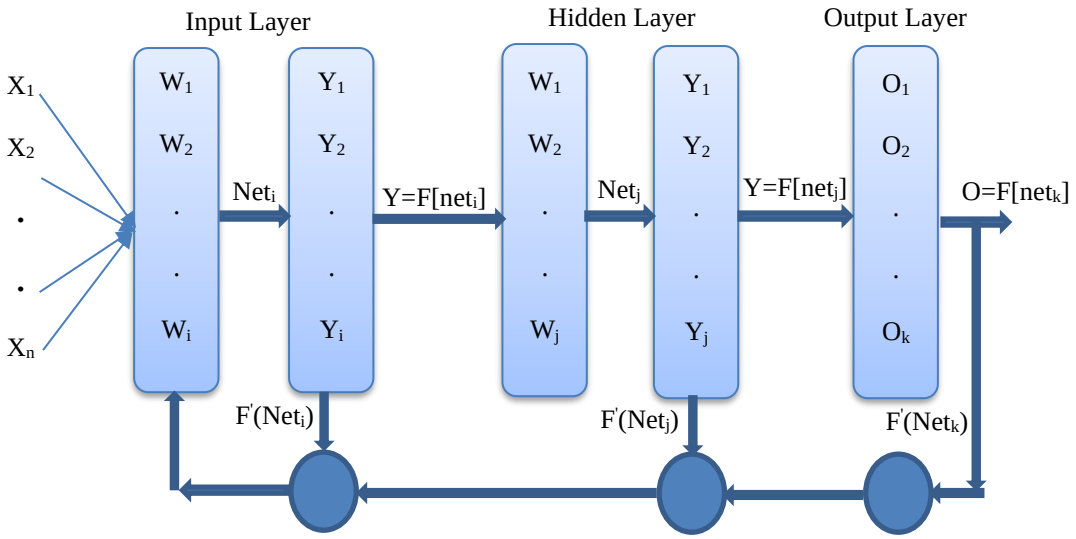
Building Artificial Neural Network and Genetic Algorithm:

الشبكة العصبية الاصطناعية نظام معالجة للمعلومات له مميزات أداء معينة بأسلوب يحاكي الشبكات العصبية الحيوية، إذ أن معمارية الشبكة العصبية النموذجية تتكون من طبقة الإدخال وطبقة الإخراج والطبقة الخفية الوسطية، وتعد شبكة الانتشار العكسي (Back Propagations Network) إحدى أهم الشبكات

العصبية الاصطناعية متعددة الطبقات[10]، إذ أدت دوراً رئيساً في إعادة بروز الشبكات العصبية الاصطناعية كأداة لحل الكثير من المشاكل على نطاق واسع، وتمكنت هذه الشبكات من حل العديد من المشاكل منها استخلاص الخواص والتصنيف والكبس وغيرها، أما طريقة تدريب هذه الشبكة فتعرف بطريقة التدريب بالانتشار العكسي لاحتساب الخطأ، وهي طريقة لحساب الانحدار التدريجي للخطأ وتهدف لإيجاد القيمة الصغرى لمربع الخطأ الكلي لقيمة الإخراج المحسوب للشبكة[14][15]، تمت عملية التدريب على مرحلتين:

1- مرحلة الانتشار الأمامي: تستقبل فيها كل وحدة إدخال إشارة إدخال ومن ثم تنشر هذه الإشارة إلى كل وحدة من وحدات الطبقة الخفية ثم تحسب كل وحدة من وحدات الطبقة الخفية بدورها قيمة التنشيط لهذه الإشارة وبعدئذ ترسل هذه الوحدات إشارتها إلى كل وحدة من وحدات طبقة الإخراج، ثم تقوم كل طبقة من طبقات الإخراج بحساب معامل التنشيط لها لتشكل استجابة الشبكة من اجل عينة الإدخال المعطاة، وخلال مرحلة التدريب تقوم كل وحدة من وحدات الإخراج بمقارنة تنشيطها المحسوب مع قيمة الإخراج الفعلي لتحديد قيمة الخطأ الحاصل لهذه العينة في تلك الوحدة.

2- مرحلة التغذية العكسية: واعتمادا على مقدار الخطأ المحسوب يتم استعمال معامل الخطأ لتوزيع الخطأ على وحدات طبقة الإخراج ويتم نشره بصورة عكسية إلى الوحدات في الطبقات السابقة لاحتساب الخطأ فيها إذ يستعمل في مرحلة تحديث قيم الأوزان، والشكل (2) يوضح عمليتي التغذية الأمامية والتغذية العكسية للشبكة.



الشكل (2): شبكة الانتشار العكسي (Back Propagations Network)

إذ أن X, Y: يمثلان على التوالي الإدخال والإخراج، و W: تمثل قيمة الوزن، و d: تمثل قيمة الاخراج المطلوب (الهدف)، و δ, η: يمثلان قيمتي نسبة التعلم ومقدار الخطأ، و F،f': تمثلان قيمتي دالة التفعيل ومشتقاتها.[3][16]

وقد تضمنت خوارزمية التدريب للشبكة الخطوات الآتية:[14][17]

1- تهيئة الأوزان **W** بقيم صغيرة يتم اختيارها بصورة عشوائية ضمن فترة محددة، ثم معالجتها بالخوارزمية الجينية.

2- تحديد بيانات التدريب ممثل بالإدخال (الإطار المدخل) والناتج المطلوب وبهذه الصيغة $[X_p, T_p]$ (الإدخال والإخراج المطلوب)، ثم عملية التنفيذ بالاتجاه الأمامي feed forward إلى قيمة الإخراج لكل وحدة j في كل الطبقة L.

$$net^{L+1}_{pj} = \sum_{i=1}^{n} W^{L}_{ij}\, out^{L}_{i} + bias_j^{L+1} \quad \ldots\ldots\ldots\ldots (1)$$

$$out_{pj}^{L+1} = F(net_{pj}^{L+1}) = 1/1+e^{-\beta net^{L+1}_{pj}} \quad \ldots\ldots\ldots\ldots (2)$$

إذ أن net^{L+1}_{pj} تمثل مجموع ضرب كل من الإدخالات الخاصة بالخلية j مع الأوزان المقابلة لها، وان Out^{L+1}_{pj} هو إخراج الوحدة بعد تطبيق الدالة عليها، أما إدخال الطبقة الأولى (طبقة الإدخال) يفهرس برمز 0 وهذا يؤدي إلى أن $out^{0}_{pj} = Xj$ و Xj يمثل إدخال المقطع Pattern.

3- حساب الخطأ بين الإخراج الحقيقي للشبكة (out^{o}_{pj}) والإخراج المطلوب target من زوج التدريب، ثم استعمال قيمة الإخراج Out_{pj} المحسوبة في الطبقة الأخيرة، وقيم الإخراج المطلوب Target لحساب قيمة الـ δ من خلال المعادلة الآتية:

$$\boldsymbol{\delta^{o}_{pj} = (t_{pj} - out^{o}_{pj})}\, f'(net^{0}_{pj}) \quad \ldots\ldots\ldots\ldots (3)$$

لكل j المستعملة في المقطع Pattern، إذ ان t_{pj} هي قيمة الإخراج المطلوب للوحدة j، $f'(net)$ هي المشتقة لدالة التنشيط ((f(net)).

4- حساب قيمة (δ) للطبقة الخفية hidden Layer بإسلوب الانتشار العكسي وحسب المعادلة الآتية (إذ أن m هي عدد الوحدات في الطبقة L):

$$\delta^{L+1}_{pi} = f'(net^{L+1}_{pi}) \left[\sum_{j=1}^{mL+1} \delta^{L+2}_{pj}\, w^{L+1}_{ij}\right] \quad \ldots\ldots\ldots\ldots (4)$$

5- تحديث الأوزان Wij باستعمال المعادلة التالية :

$$W^{new}_{ij} = w^{old}_{ij} + \Delta w^{L}_{ij} \quad \ldots\ldots\ldots\ldots (5)$$

إذ أن $\Delta\, w^{L}_{ij}$ تحسب بالطريقة التالية:

$$\Delta W^{L}_{ij} = \delta \eta_{\mathbf{pj}}^{\mathbf{L+1}} out^{L}_{pi} \quad \ldots\ldots\ldots\ldots (6)$$

6- الرجوع إلى الخطوة الثانية وتكرارها لكل النماذج p والى أن يصل الخطأ إلى قيمة مقبولة.

أما خوارزمية الاختبار فتضمنت الخطوات الآتية:[5][17]

1- تهيئة بيانات الاختبار لكي تكون ملائمة لعملية الاختبار.

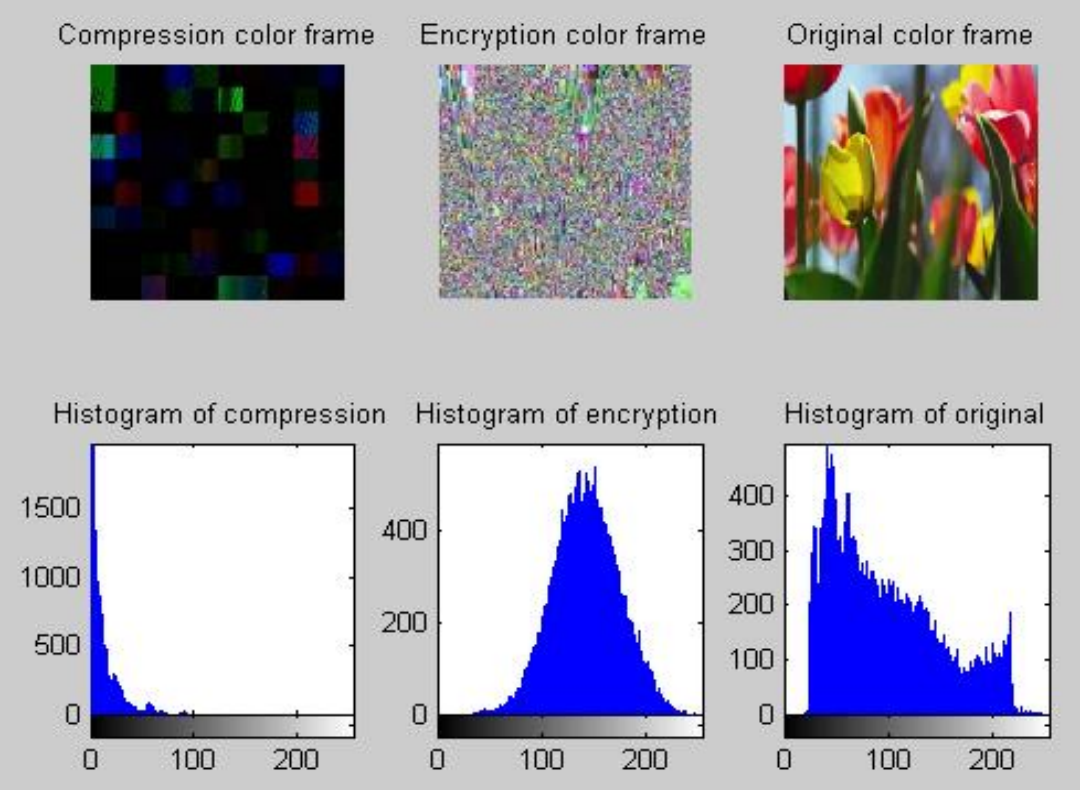
2- استرجاع ملف الأوزان من وحدة الخزن Wi، ثم اختيار سجل اتصال أو مقطع بيانات (pattern) الاختبار X_p.

3- تنفيذ عملية التغذية الأمامية Forward Activation Function:

$$R_i = X_p * W_i \quad \ldots\ldots\ldots (7)$$

4- إذا لم يتم تجاوز عدد بيانات الاختبار، اذهب إلى الخطوة الثانية، وإلا اذهب إلى الخطوة الخامسة.

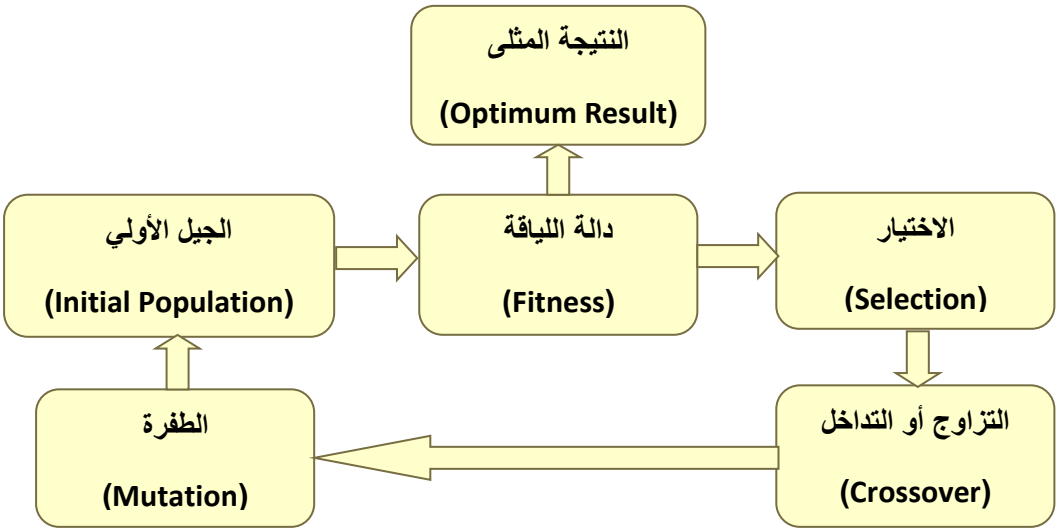
5- نهاية الاختبار، والشكل (3) يوضح مراحل تنفيذ الخوارزمية.



الشكل (3): نتائج التشفير والكبس على الإطار الأول من ملف الفيديو الرقمي

إن عملية حساب الأوزان تمت باستعمال الخوارزمية الجينية، وذلك لأنها تعتبر تقنية بحث تستعمل في مجال الذكاء الاصطناعي تحديدا في فرع البحث وحل المشاكل إذ تقوم بإيجاد أفضل الحلول لمشاكل التحسين بالاعتماد على العشوائية في البحث.

إذ تتضمن الخوارزمية الجينية عددا من الخطوات الأساسية، هذه الخطوات ثابتة لمختلف المسائل ولكل التطبيقات ويكون الاختلاف في صيانة كل خطوة من الخطوات وتطبيقها، إذ أن خطوات المسألة مترابطة بعضها مع البعض الآخر ولا يمكن تطبيق هذه الخوارزمية على أية مسألة ما لم تطبق جميع الخطوات، وإلا تفقد الخوارزمية الجينية قيمتها وفائدتها في إيجاد الحل أو تحسينه، والمخطط (3) يوضح آلية عمل الخوارزمية الجينية.



المخطط (3): خطوات عمل الخوارزمية الجينية

أما خطوات عمل الخوارزمية الجينية المقترحة:

1- تكوين جيل عشوائي من N من الكروموسوم و M من الجينات.

2- حساب دالة اللياقة (fitness function) لكل كروموسوم في الجيل الحالي.

3- توليد جيل جديد (new population) بتكرار الخطوات الآتية حتى يكتمل الجيل، إذ يجب أن يحتوي الكروموسوم على معلومات عن الحل الذي سوف يقدمه وقد تم استعمال طريقة الشريط الثنائي إذ يمثل كل كروموسوم بواسطة سلسلة ثنائية تحوي عدد من البتات يمكن لكل بت في السلسلة أن يمثل بعض الميزات الخاصة بالحل وهو أن تكون السلسلة كلها تمثل رقم إذ يكون شكل الكروموسوم كالتالي:

Chromosome1: 1101100100110110

Chromosome2: 1100111000011110

يتم اختيار (selection) كروموسومان ليمثلا الوالدين من الجيل الحالي بالاعتماد على دالة اللياقة لهم، إذ كلما كانت دالة اللياقة للكروموسوم أعلى كلما زادت نسبة اختياره[4]، وبالاعتماد على نظرية داروين في التطور فإن الأفضل في الجماعة هو الذي يشكل الجيل الجديد، ويمكن وصف هذه العملية من خلال الخطوات الآتية:[11]

أ- الجمع: حساب مجموع لياقة كل الكروموسومات في الجماعة ويرمز له بالرمز (S).

ب- الاختيار: إختيار رقم عشوائي من المجال (0,S) ويرمز له بالرمز (r).

ت- الحلقة: جمع كل اللياقات في الجماعة من الصفر وحتى S الى أن يصبح S أكبر من r يتم التوقف وتعاد قيمة الكروموسوم الذي تم الوقوف عنده، علما أن الخطوة الأولى تنفذ مرة واحدة فقط من أجل كل جماعة.

4- يتم إجراء عبور أو تزاوج (crossover) بين الكروموسومين عند نقطة التزاوج إذا كان لديهما احتمالية تزاوج، ويتم التزاوج بانقسام كل كروموسوم عند نقطة التزاوج، ثم يوصل كل جزء من احد الكروموسومين مع الجزء المقابل من الكروموسوم الآخر، فينتج كروموسومان جديدان (children)، إن الطريقة المستعملة لتنفيذ العبور تتم عن طريق اختيار نقطة للعبور عشوائياً ثم نسخ كل ما قبلها من الأب الأول وكل ما بعدها من الأب الثاني، ويوضح المثال الاتي عملية العبور (إذ يمثل الرمز (|) نقطة العبور):

Chromosome 1: 11011 | 00100110110
Chromosome 2: 11001 | 11000011110
Offspring 1: 11011 | 11000011110
Offspring 2: 11001 | 00100110110

إذا لم يكن هناك عبور فإن الجيل الجديد الناتج سوف يكون نسخة مطابقة للأبوين أما إذا تم العبور فإن الجيل الناتج سيتكون من أجزاء من كروموسومات كلا الأبوين، وإن كان احتمال العبور 100% فإن كل أفراد الجيل الجديد تكون ناتجة عن العبور وإذا كان احتماله 0% فيكون الجيل عبارة عن نسخة مطابقة لكروموسومات الجماعة القديمة ولكن هذا لا يعني بأن الجيل الجديد هو نفسه القديم إذ يتم تنفيذ العبور على أمل أن الكروموسومات الجديدة ستحتوي على أقسام جديدة من الكروموسومات القديمة وبهذا فإن الجديدة تكون أفضل وفي جميع الأحوال فإنه من المجدي ترك بعض الأجزاء من الجماعة القديمة في الجيل الجديد.[18]

5- يتم عمل طفرة (Mutation) للكروموسوم الجديد إذا كان لديه احتمالية إجراء طفرة عليه (Mutation probability)، بعد تنفيذ العبور تظهر بعض الطفرات إذ تحدث الطفرات نتيجة قلب أو عكس بت (Bit) وان الغاية من الطفرة هي منع الوقوع في مشكلة كون كل الحلول في الجماعة هي حل مثالي للمسألة المراد حلها[17]، وإن تشفير الطفرات بالإضافة إلى العبور تعتمد بشكل أساسي على تشفير الكروموسومات إذ تغير الطفرة الجيل الجديد الناتج عن العبور عشوائياً ويمكن التبديل عشوائياً بعض البتات من (1) إلى (0) أو بالعكس وكما في المثال الاتي:

Original offspring 1: 1101111000011110
Original offspring 2: 1100100100110110
Mutated offspring 1: 1100111000011110
Mutated offspring 2: 1100101100110100

إذا لم تحدث طفرات فإن الجيل الجديد يتشكل مباشرة بعد العبور (ينسخ مباشرة) بدون أي تغييرات أما إذا كان هناك طفرات فإن واحد أو أكثر من الكروموسومات تتغير وإذا كان احتمال الطفرات 100% يتغير الكروموسوم بكامله أما إذا كان 0% فلا يتغير شيء.[16]

بشكل عام تمنع الطفرات الخوارزميات الجينية من الوقوع في نهاية محلية وينبغي أن لا تتم الطفرات بكثرة لأن الخوارزمية الجينية عندها ستتحول إلى بحث عشوائي(Random search).

6- عملية الاستبدال (accepting) وهي عملية إضافة الكروموسوم الناتج إلى الجيل الجديد.[13]

7- اختيار شرط التوقف عن البحث[13]، إذ:

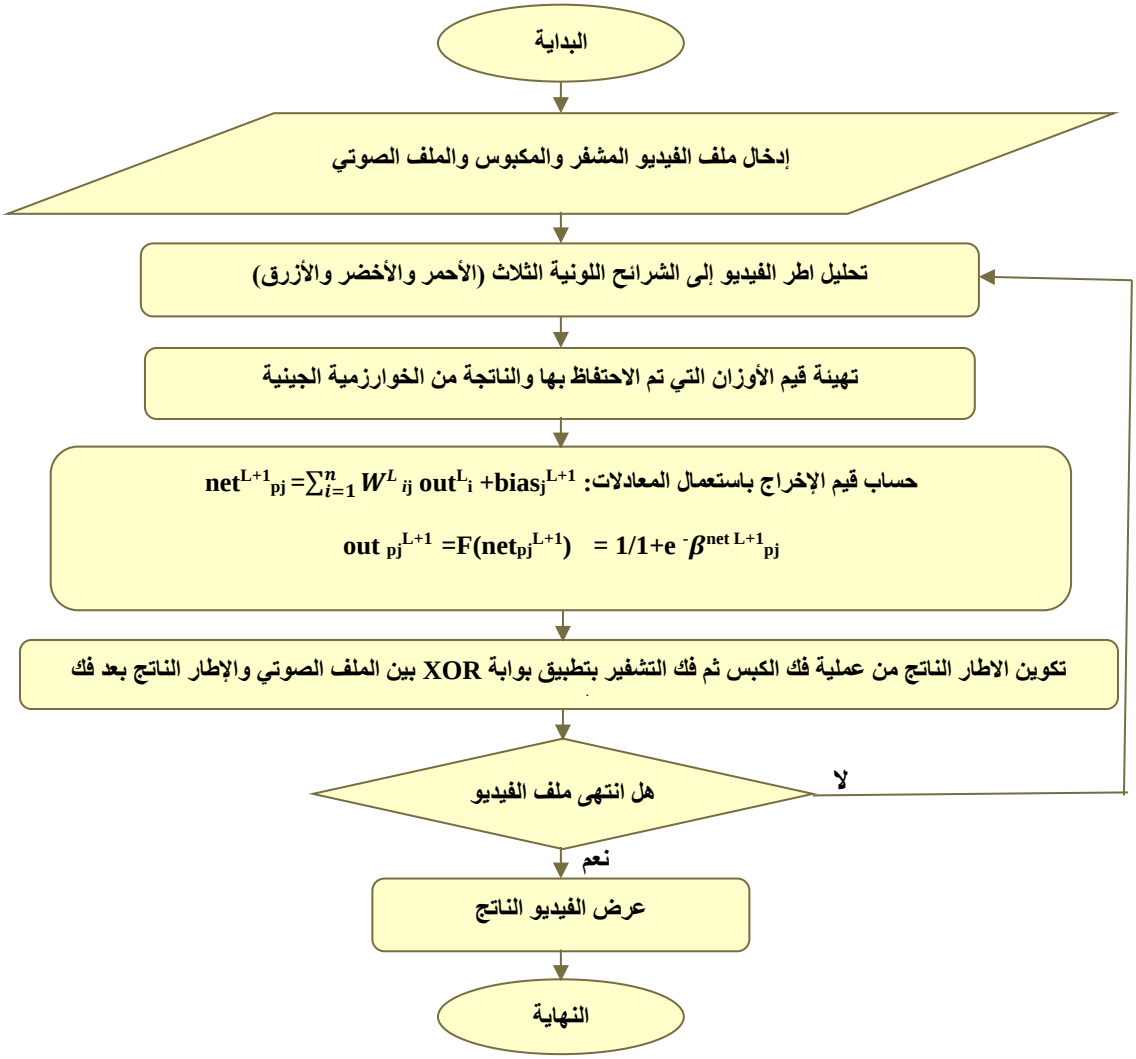
أ- تحقق شرط التوقف: يتم التوقف للخوارزمية الجينية، وإعادة الحل الجيد من آخر جيل متكون.

ب- عدم تحقق شرط التوقف: الرجوع إلى الخطوة (2)، إذ أن كل تكرار لهذه العملية يسمى بالجيل الجديد (Generation)، وبعد نهاية التنفيذ يتم تقديم تقرير عن الحقائق التي تم التوصل إليها.

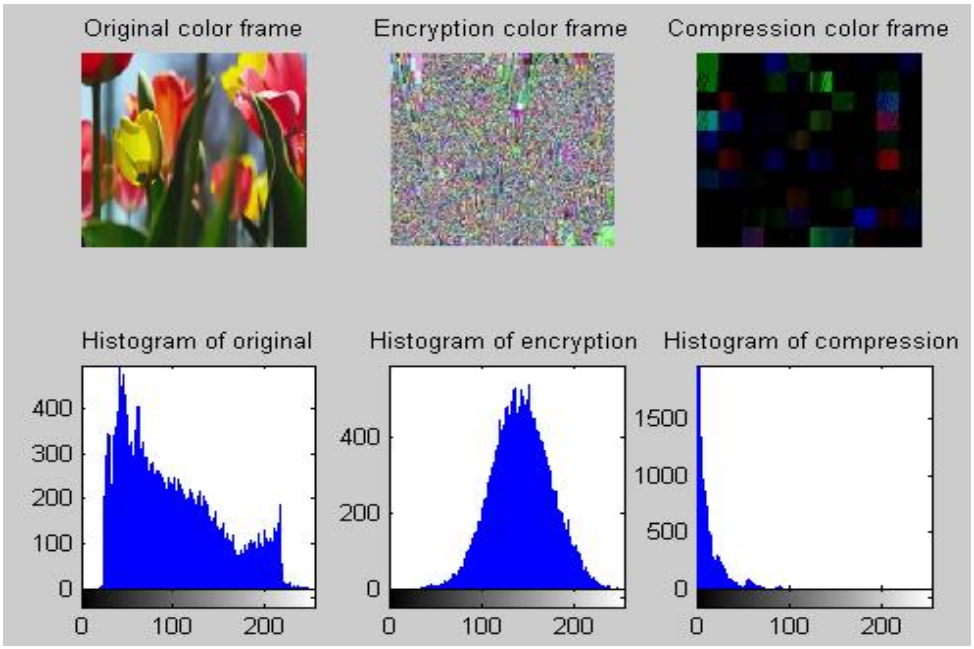
6-فك الكبس والتشفير Decompression and Decryption:

بعد أن تمت عملية التشفير والكبس، يتم فك تشفير وكبس ملفات الفيديو وذلك من خلال تنفيذ عمليات معاكسة لعملية التشفير والكبس، وكما في المخطط الانسيابي (4).

إذ يتم العمل على إدخال ملف الفيديو المشفر والمكبوس ثم تحليل اطر الفيديو إلى الشرائح اللونية الثلاث (الأحمر والأخضر والأزرق)، ثم استرجاع قيم الأوزان التي تم الاحتفاظ بها والناتجة من الخوارزمية الجينية وسينتج عنها اطر مشفرة لتبدأ مرحلة فك التشفير وذلك من خلال إدخال ملف الصوت (مفتاح فك الشفرة) ثم عمل XOR مع الأطر المشفرة لينتج بعد ذلك ملف الفيديو غير المشفر وغير المكبوس، والشكل (4) يوضح الخطوات العملية لمرحلة فك الكبس والتشفير.



المخطط الانسيابي (4): خطوات فك الكبس والتشفير



الشكل (4): نتائج فك الكبس وفك التشفير على الإطار الأول من ملف الفيديو

7-مقاييس الدقة Measures Of Accuracy:

بعد أن تم تطبيق جميع الخوارزميات والحصول على نتائجها، تم حساب نسبة الكبس وتقييم النتائج بوساطة اختبارات الدقة وذلك عبر استعمال طرائق رياضية، وتوجد عدة أنواع من الاختبارات الإحصائية أهمها:

1- إيجاد اقل قيمة لمربع الخطأ (Minimum Squared Error) بين إشارة الإدخال والإخراج، إذ تمثل M و N عدد الأعمدة والأسطر للإشارة، وتمثل $I_i(m,n)$ و $I_{21}(m,n)$ إشارة الإدخال والإخراج، إذ:

$$MSE = (\sum_{MN}[I_i(m,n)-I_{21}(m,n)]^2) / (M*N) \quad \ldots\ldots\ldots\ldots (8)$$

2- قياس نسبة الضوضاء (Peak Signal-to-noise ratio): إذ تمثل R^2 قيم البيانات إذا كانت Floating Point أو Unsigned integer:

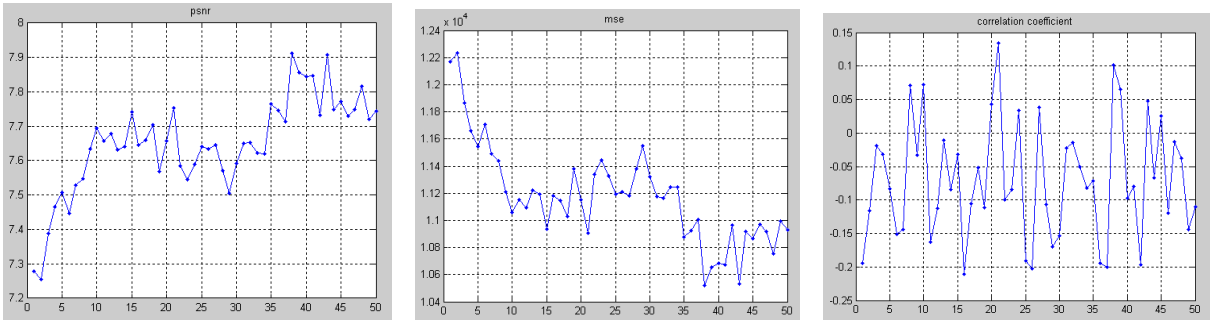
$$PSNR = 10\log_{10}[R^2/MSE] \quad \ldots\ldots\ldots (9)$$

3- معامل الارتباط (Correlation): هو مقياس لقوّةِ العلاقةِ بين المتغيرات العشوائية، إذ:

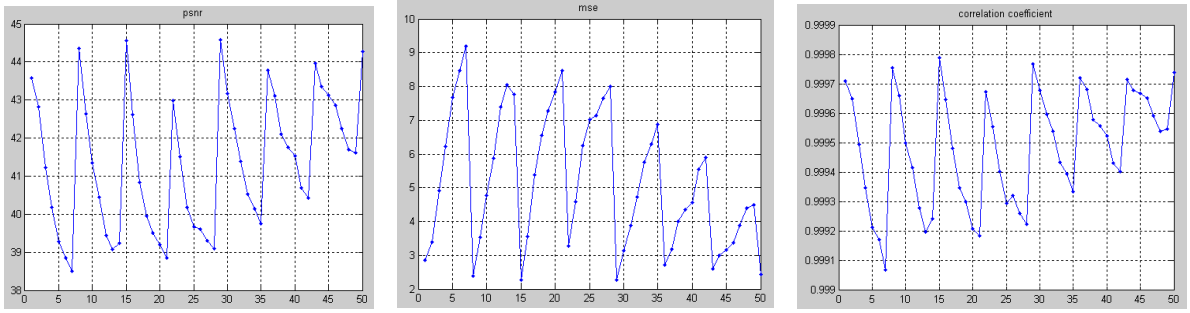
$$Corr = \frac{\sum(I-\mu_I)(O-\mu_O)}{\sqrt{\sum(I-\mu_I)^2\sum(O-\mu_O)^2}} \quad \ldots\ldots\ldots\ldots (10)$$

ومعامل الارتباط يمكن أن يأخذ القيم بين (-1 و+1)، إذ أن الإشارة (+ أو -) لمعامل الارتباط تمثل اتجاه العلاقة، وقد تمت الاختبارات بين ملف الفيديو المدخل وملف الفيديو المشفر والمكبوس وكما موضح في الشكل (5)، وأيضا تمت الاختبارات بين ملف الفيديو المدخل وملف الفيديو بعد الاسترجاع وكما في الشكل (6).

من خلال متابعة الشكل(5) والشكل(6) تبين بان معامل الارتباط كان قريبا من الصفر في الشكل (5) وهذا يدل على انه لا توجد علاقة خطية بين ملف الفيديو المدخل وملف الفيديو المشفر والمكبوس أو أنها توجد علاقة خطية ضعيفة جدا، وأما في الشكل (6) فان معامل الارتباط (بين ملف الفيديو المدخل وملف الفيديو بعد فك التشفير وفك الكبس) قريب من الواحد وهذا يدل على وجود علاقة خطية قوية جدا وقد تكون مثالية.



الشكل (5): تطبيق مقاييس الدقة على ملف الفيديو قبل وبعد التشفير والكبس



الشكل (6): تطبيق مقاييس الدقة على ملف الفيديو المدخل وملف الفيديو بعد الاسترجاع

وأما قيمة مربع الخطأ (MSE) ففي الشكل (5) كانت قيمها كبيرة جدا وهذا يدل على انه لا يوجد ارتباط بين ملفي الفيديو، وفي الشكل (6) فان قيم مربع الخطأ صغيرة جدا وهذا يدل على انه يوجد ارتباط بين ملفي الفيديو، والجدول (1) يوضح نتائج التنفيذ على 10 عينات متنوعة من ملفات الفيديو الرقمي المدخلة.

Video NO.	*Encryption Operation*		*Compression Operation*		*Compression Ratio*	*NO. of Frames*	*Dimension of Frames*	
	MSE	PSNR	MSE	PSNR			Height	width
Video1	1.3962e+04	6.6814	4.1203e+03	11.9815	1.89804	92	300	300
Video2	1.1377e+04	7.5707	2.8919e+03	13.5190	2.12476	20	300	300
Video3	7.9527e+03	9.1256	3.5802e+03	12.5918	2.19106	102	300	300
Video4	9.3162e+03	8.4384	4.1367e+03	11.9643	2.08143	120	300	300
Video5	1.0306e+04	7.9998	4.0038e+03	12.1061	2.08516	143	300	300
Video6	8.5195e+03	8.8267	3.5058e+03	12.6829	2.24880	88	300	300
Video7	1.2760e+04	7.0724	3.8236e+03	12.3061	2.06485	114	300	300
Video8	9.2516e+03	8.4686	3.3574e+03	12.8708	2.25410	51	300	300
Video9	9.8087e+03	8.2147	4.0155e+03	12.0934	2.05042	45	300	300
Video10	1.0723e+04	7.8275	3.8581e+03	12.2671	2.11644	58	300	300

الجدول (1): نتائج التنفيذ على 10 عينات متنوعة من الفيديو الرقمي

8-الاستنتاجات Conclusions:

بعد تطبيق خوارزميات التشفير والكبس وتطبيق خوارزميات فك التشفير وفك الكبس وبعد الحصول على النتائج وقيم مقاييس الدقة تبين بان عملية تشفير وكبس ملفات الفيديو الرقمي أعطت نتائج تناسبت مع متطلبات البحث العملية، ومن خلال التطبيق العملي تم التوصل إلى ما يلي:

1- إن التشفير باستعمال بوابة XOR بين الإطار المدخل والمقطع الصوتي (مفتاح التشفير) تطابقت مع هدف البحث للوصول إلى السرية، فضلاً عن أن هذه الخاصية تجعله مناسباً لتطبيقات إرسال الملفات الفيديوية عبر وسائط النقل (كالانترنت).
2- إن تطبيق الشبكة العصبية الاصطناعية (شبكة انتشار الخطأ خلفيا) مع الخوارزمية الجينية لكبس ملفات الفيديو الرقمي أعطت نتائج متوافقة مع متطلبات البحث، وذلك عبر نتائج زمن التنفيذ والنسبة المئوية للكبس ومقاييس الدقة، فمن خلال ملاحظة النتائج في الجدول رقم (1) تبين أن نسبة الكبس كانت متقاربة للملفات التي تحتوي على 20 اطار مع الملفات التي تحتوي على 143 اطار إذ ان ابعاد الاطر هي 300*300 وان حجم الفيديو الناتج اصبح اقل من نصف حجم الفيديو الاصلي، من جهة اخرى فان الزيادة في الارقام الناتجة لقيم الـMSE تدل على كفاءة التشفير والكبس تقابلها الارقام المنخفضة الناتجة لقيم الـPSNR والتي تدل على الترابط بين الملفات الناتجة والاصلية.
3- بعد استعمال الخوارزمية الجينية لحساب قيم الأوزان تبين أنها أداة كفوءة وفعالة في الوصول الأسرع إلى النتائج المطلوبة لما لها من ميزات تساعد في تسهيل معالجة البيانات الفيديوية وتحضيرها لعملية الكبس من خلال الوصول الأمثل للأوزان المعتمدة.
4- إن عملية العنقدة وتقسيم الأطر إلى مجموعة من العناقيد (النقاط الضوئية المتجانسة) أدت إلى إعطاء الخوارزمية كفاءة في سرعة المعالجة التي تمت على كبس الأطر وتشفيرها، إذ أن الزمن المطلوب لكبس إطار واحد من أطر الفيديو الرقمي هو 10 ثانية تقريبا.
5- إن جودة استرجاع الفيديو واضح المعالم وعند نسبة كبس جيدة عند استعمال عملية التشفير والكبس على الفيديو المستعمل.

المصادر References

1- Asbun E., Thesis, Submitted to the Faculty of Purdue University, In Partial Ful_llment of the Requirements for the Degree of Doctor of Philosophy, 2000.
2- Han B., Wu D., Zhang H., Thesis, Department of Electrical and Computer Engineering, University of Florida Gainesville, FL 32611, Cisco Systems, Santa Clara, Provider: citeseer, 2013.
3- Kin C. Y. S., Coker B., Thesis, Electrical Engineering cedyue@stanford.edu, Computer Science bcoker@stanford.edu, 2017.
4- Choudhary R., Abrol P., Thesis, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 6, Issue 6, June 2, ISSN: 2278 – 1323, 2017.
5- Zhang X., Wu X., Thesis, Fellow, IEEE, MANUSCRIPT SUBMITTED TO IEEE TRANSACTIONS ON IMAGE PROCESSING, arXiv:1801.07987v2 [cs.CV] 19 Mar, 2018.

6- Gloe T., Fischer A., Kirchner M., Thesis, Journal: Digital Investigation ISSN: 17422876, Volume: 11 Issue: -Supplement_1 Pages: S68-S76 Provider: Elsevier DOI: 10.1016/j.diin.2014.03.009, 2014.
7- Xu D., Wang R., Shi Y. Q., Thesis, Journal: Information Forensics and Security, IEEE Transactions on ISSN: 15566013, Volume: 9 Issue: 4 Pages: 596-606 Provider: IEEE Publisher: IEEEDOI: 10.1109/TIFS.2014.2302899, 2014.
8- Srikanth P., Mehta A., Yadav N., Singh S., Singhal S., Thesis, IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June ISSN (Online): 2277-5420, 2017.
9- Um H. Y., Thesis, Submitted to the Faculty of Purdue University, Purdue University West Lafayette, Indiana, 2006.
10- Anand A. and Suganthi L., Thesis, Energies, 11, 728; doi:10.3390/en11040728, 2018.
11- Xie L., Yuille A., Thesis, Center for Imaging Science, The Johns Hopkins University, Baltimore, MD, USA, arXiv:1703.01513v1 [cs.CV] 4 Mar, 2017.
12- Li M., Gu S., Zhang D., Thesis, arXiv:1801.04662v1 [cs.CV] 15 Jan, 2018.
13- Pradeep S. A., Manavalan R., Thesis, International Journal of Engineering Research Volume No.2, Issue No. 6, pp : 386-392, 2013.
14- Beale M. H., Hagan M.T., Demuth H. B., "Neural Network Toolbox", User's Guide, by The MathWorks, Inc., www.mathworks.com, 2014.
15- Suganuma M., Shirakawa S., Nagao T., Thesis, arXiv:1704.00764v2 [cs.NE] 11 Aug, 2017.
16- Mohammadi M., Mehrolhassani M. A., Thesis, Under review as a conference paper at ICLR, 2017.
17- Kaviani M., MirRokni S. M., Thesis, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.6, June, 2017.
18- Wang F., Junlan L., Liu S., Zhao X., Zhang D., Tian Y., Thesis, Journal: Mechatronics, IEEE / ASME Transactions on ISSN: 10834435, Volume: 19 Issue: 3 Pages: 916-923 Provider: IEEE Publisher: IEEE DOI: 10.1109/TMECH.2013.2260555, 2014.