Hybrid Method between the Discrete Wavelets Translate Technique and the Chaos System Based by the Least Significant Bit Algorithm to Encrypt and Hide a Digital Video File

Hasan Maher Ahmed
hasanmaher@uomosul.edu.iq
College of Computers Sciences and mathematics
University of Mosul, Mosul, Iraq

Received on: 20/06/2018 **Accepted on: 27/08/2018**

ABSTRACT

The use of computers today is the most important and widespread means of storing, retrieving and circulating information through local and international networks and smart phones. Thus it is possible to intercept information through different networks or access to computers, whether independent or connected with the network for the purpose of viewing its contents or stealing information or to tamper with, and in this light must ensure the protection, reliability and credibility of information and preservation of the emergence of various means of protection such as the use of encryption and techniques of hiding or coverage of information.

This research is based on a hybrid method between the Discrete Wavelets Translate technique (DWT) and the Chaos system based on the Least Significant Bit algorithm (LSB) to encrypt and hide a digital video file within another digital video that represents the cover by inserting the digital video file and segmenting it into a set of frames and then analyze each frame to its colors (red, green and blue) and then study the color values of each frame and the process of encryption based on the equation of the logistics function (chaotic functions), and the application of the Discrete Wavelets Translate technique on the color slides of the cover frame. The hiding process is done using the Least Significant Bit algorithm based on the logistic function by calculating the series of random locations of cover area.

The results showed that the hybridization of the Discrete Wavelets Translate technique and the chaos system based on the Least Significant Bit algorithm was an effective method for encrypting and hiding digital video files. After applying the work algorithms to a set of samples, the results showed consistency and compatibility in the encrypting and hiding process with the samples that was dealt with.

Keywords: LSB, Wavelets, Chaos, Logistic Function, Information Hiding, Data Encryption.

تهجين تقنية التحويل المويجي المتقطع ونظام الفوضى لتشفير وإخفاء ملف فيديو بالاعتماد على خوارزمية الخلية الثنائية الأقل أهمية

حسن ماهر أحمد
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2018/06/20 **تاريخ قبول البحث: 2018/08/27**

الملخص

أصبح استخدام أجهزة الحاسوب في الوقت الحاضر الوسيلة الأكثر أهمية وانتشاراً في خزن واسترجاع المعلومات وتداولها عبر الشبكات المحلية والعالمية والهواتف الذكية، فأصبح بالإمكان اعتراض المعلومات عبر شبكات الاتصال المختلفة أو الدخول إلى أجهزة الحاسوب سواء كانت مستقلة أم مرتبطة مع الشبكة بقصد الاطلاع

على محتوياتها أو سرقة المعلومات المهمة أو العبث بها، وفي ضوء ذلك يتوجب تأمين الحماية والوثوقية والمصداقية للمعلومات والمحافظة عليها فظهرت وسائل حماية متنوعة مثل استخدام التشفير وتقانات إخفاء المعلومات أو تغطيتها.

اعتمد في هذا البحث على طريقة مهجنة بين تقانة التحويل المويجي المتقطع ونظام الفوضى بالاعتماد على خوارزمية الخلية الثنائية الأقل أهمية لتشفير ملف فيديو رقمي وإخفائه داخل ملف فيديو رقمي آخر الذي يمثل الغطاء، وذلك بإدخال ملف الفيديو الرقمي وتقطيعه إلى مجموعة من الأطر المكونة منه ثم تحليل كل إطار إلى شرائحه اللونية (الأحمر والأخضر والأزرق) ثم دراسة القيم اللونية لكل شريحة وإجراء عملية التشفير بالاعتماد على معادلة الدالة اللوجستية (وهي إحدى الدوال الفوضوية)، وبتطبيق تقانة التحويل المويجي المتقطع على الشرائح اللونية للإطار الغطاء تتم عملية الإخفاء باستخدام خوارزمية الخلية الثنائية الأقل أهمية بالاعتماد على الدالة اللوجستية وذلك بحساب سلسلة المواقع العشوائية للبيانات.

أظهرت النتائج أن عملية التهجين لتقانة التحويل المويجي ونظام الفوضى بالاعتماد على خوارزمية الخلية الثنائية الأقل أهمية أسلوب فعال ومشجع لتشفير ملفات الفيديو الرقمي وإخفائه، فبعد تطبيق خوارزميات العمل على مجموعة من العينات أظهرت النتائج أيضاً الانسجام والتوافق في عملية التشفير والإخفاء مع العينات التي تم التعامل معها.

الكلمات المفتاحية: الخلية الثنائية الأقل أهمية، التحويل المويجي، الفوضى، الدالة اللوجستية، إخفاء المعلومات، تشفير البيانات.

1. المقدمة Introduction

أصبحت عملية تناقل البيانات عبر الإنترنيت سهلةً نتيجة التطور الكبير في تقانات الشبكات، وبات بإمكان الكثيرين الاتصال مع بعضهم البعض بسهولة وبسرعة, إلا أن استخدام الإنترنيت للاتصال ترافقه مشكلتان إحداهما توفير الأمنية (Security) والأخرى توفير عرض الحزمة (Bandwidth)؛ ولأن الإنترنيت بيئة عامة ومفتوحة فقد أصبح بإمكان غير المخولين مراقبة المعلومات المتناقلة بين أي طرفين واعتراضها أو الحصول عليها.

هناك تقانتان لتوفير الأمنية للمعلومات المتناقلة والحفاظ على سريتها أولهما التشفير (Encryption) وثانيهما الكتابة المغطاة (Steganography)؛ إذ إن العائق الرئيس للتشفير هو وجود البيانات بصورة غير مخفية، فعلى الرغم من إنه لا يمكن قراءتها فإنها ما تزال موجودة، فإذا كان هناك الوقت الكافي لشخص ما فإنه في النهاية يستطيع فتح شفرة البيانات، لذلك كان لابد من تطوير أمنية البيانات وإنشاء تقانات جديدة، ومن هنا ظهر نظام التغطية (Steganography).[8]

تعرف عملية إخفاء المعلومات بأنها تضمين بيانات سرية في أشكال مختلفة من الوسائط المتعددة الرقمية (Digital Multimedia) كملفات النصوص والصور والملفات الصوتية والفيديوية، ومع النمو السريع لتقانات الشبكات والاتصالات فإن تقانات إخفاء المعلومات أصبحت تستخدم بصورة واسعة لتحقيق أغراض متعددة منها حماية حقوق الطبع وتثبيت الملكية وتحقيق الاتصال بصورة سرية.[15]

ويمكن تعريف الكتابة المغطاة بأنها طريقة لإرسال بيانات سرية بتضمينها في وسائط تعد غطاءً أو حاملاً لها بصورة يتعذر بها تمييز وجود تلك البيانات، وقد تكون الأغطية ملفات نصية أو صورية أو صوتية أو فيديوية، ويمكن أن تكون البيانات السرية معلومات صريحة أو معلومات مشفرة التي يمكن تمثيلها بشكل سلسلة من الخلايا

الثنائية (Bits)، والهدف من الكتابة المغطاة هو نفي الشك بوجود تناقل بيانات سرية, وقد تفشل عملية الحفاظ على أمنية البيانات إن حصل شك بوجودها.[8]

تعتمد عمليات التشفير والإخفاء في عملهما على وجود بيانات مهمة يجب الحفاظ عليها كرسالة سرية أو كلمة سر (Password) أو مفتاح أمني وغيرها الكثير، إلا أن هناك معلومات أو أماكن مهمة لا يمكن الوصول إليها إلا عن طريق مجموعة متتابعة من الخطوات السرية كأن تكون أماكن وضع المفتاح السري أو اجتياز حواجز من الليزر الحارق عبر ممرات سرية أو قد تكون مجموعة من العتلات المتشابكة مع بعضها تعمل إذا وضعت على نمط معين، ففي مثل هذه الحواجز السرية لا يمكن اجتيازها بسهولة وإنما تحتاج إلى توثيق تلك الأحداث بملف فيديو والذي من خلاله يضمن فك جميع الحواجز، بعدها يجب طمر وتشفير الفيديو الرقمي عبر خوارزميات وقنوات سرية تضمن وصوله إلى الجهة المستلمة وذلك لوجود ضرورة لإخفاء عملية إرسال الفيديو الرقمي من طرف لآخر، وهو ما اعتمد عليه هذا البحث، وتم العمل على استخدام لغة Matlab 2017 لتنفيذ خوارزميات البحث.

حاول الباحثون استغلال تقانات الحاسوب وتوجيهها بشكل فعال في هذا المجال فتم انجاز بحوث ودراسات واسعة لربط هذه التقانات والوسائل مع ما يحتاجون إليه من أعمال؛ إذ قدم عدد من الباحثين عام 2016 بحثاً اقترحوا فيه طريقة لاخفاء المعلومات على أساس المجال المكاني، ووفقاً للطريقة المقترحة فإن الرسالة السرية هي مضمنة عشوائياً في مواقع النقاط الضوئية (Pixels) لصورة الغلاف باستخدام مولد الأرقام العشوائية الزائفة (PRNG)، وأن الطريقة المقترحة تعمل مع الطبقتين الأزرق والأخضر.[7]

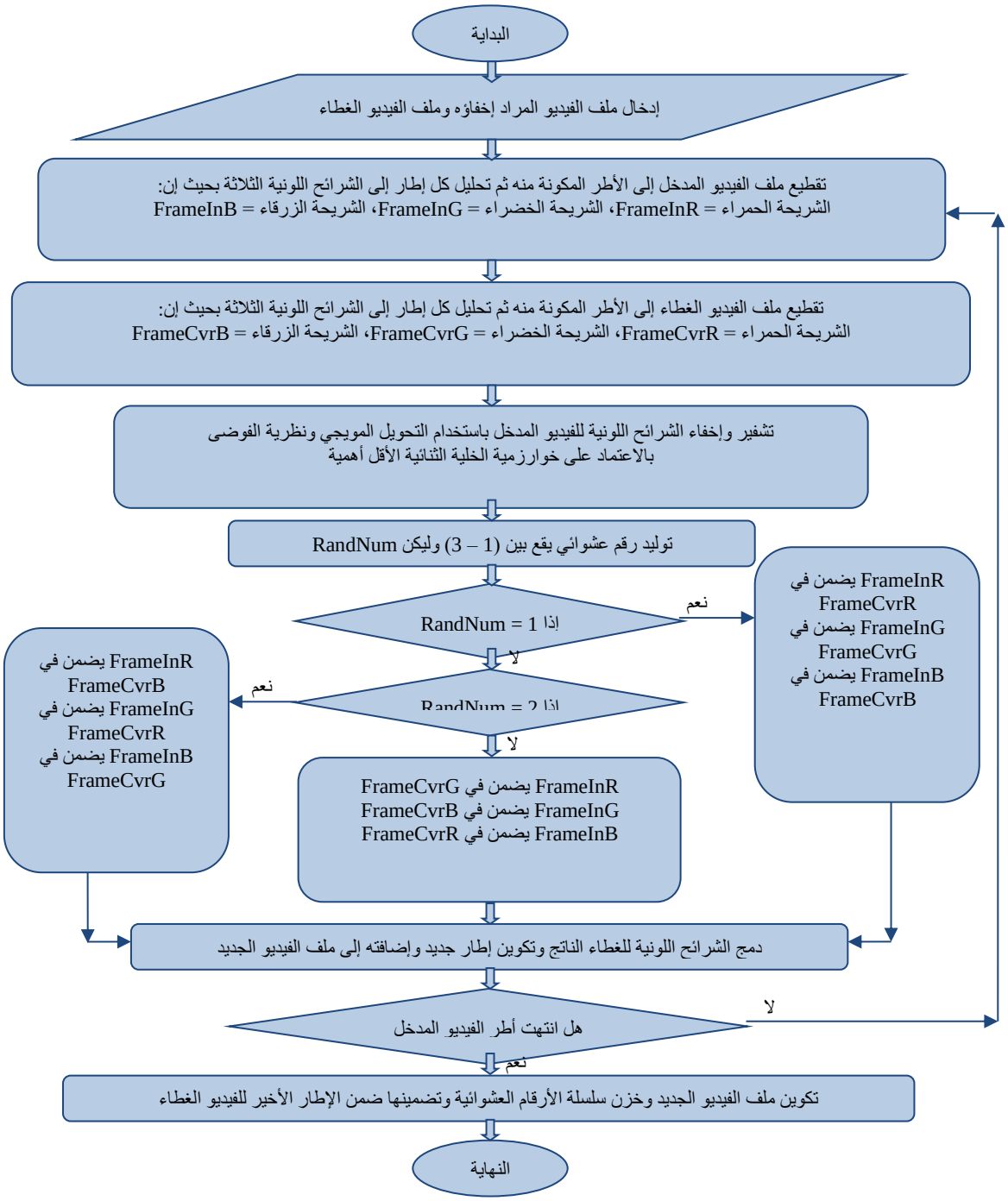
وقدم عدد من الباحثين عام 2017 بحثاً تضمن اقتراح تقانة جديدة لتشفير الصور تعتمد على الجمع بين خليط النقاط الضوئية (Pixels) والمربعات (S-box) من خوارزمية التشفير AES، ففي البداية تستخدم خارطة Arnold Cat لخلط مواضع النقاط الضوئية للصورة الرقمية في المجال المكاني تشفر الصورة الرقمية المختلطة عن طريق الاستبدال باستخدام S-Box.[13]

وفي عام 2018 قدم الباحث Dogan بحثاً اقترح فيه خوارزمية جديدة لإخفاء البيانات على أساس أزواج من النقاط الضوئية (Pixel) تعتمد على خارطة فوضوية؛ إذ عمل على انشاء نظام الاخفاء من خلال تطبيق وظيفة Modulo.[2]

2. المخطط العام للبحث General Research Plan

إن الهدف من البحث هو تشفير ملفات الفيديو الرقمي واخفاؤه بطريقة مهجنة بين تقانة التحويل المويجي المتقطع ونظرية الفوضى بالاعتماد على خوارزمية الخلية الثنائية الأقل أهمية (LSB)، وكما موضح في المخطط الانسيابي(1).

تم العمل على إدخال ملف الفيديو الرقمي ثم تقطيعه إلى الأطر المكونة منه (التي اعتمد أبعادها إلى 100*100) ليتم بعدها تحليل كل إطار إلى الشرائح اللونية الثلاثة (الأحمر والأخضر والأزرق) ولكل شريحة لونية تحلل قيمها اللونية، ليتم تشفير وإخفاء كل شريحة باستخدام تقانة التحويل المويجي المتقطع ونظرية الفوضى.



المخطط الانسيابي (1): المخطط العام للبحث

اعتمد ملف فيديو آخر غطاء لعملية الإخفاء (وأن أبعاد أطر الفيديو هي 1200*1200)، بحيث إن كل إطار من ملف الفيديو المدخل يقابل إطاراً من ملف الفيديو الغطاء، وبعد تحليل الأطر لكل من ملفي الفيديو إلى الشرائح اللونية الثلاثة اعتمد الاختيار العشوائي للشرائح اللونية الخاصة بالغطاء فمثلاً الشريحة الحمراء لإطار من الفيديو المدخل يمكن إخفاؤها في الشـــريحة الخضـــراء أو الزرقاء أو الحمراء للإطار المقابل له من الفيديو الغطاء وحسب الاختيار العشوائي، وهكذا بالنسبة للشريحة الخضراء والحمراء للإطار نفسه، وتسجل القيم العشوائية التي استخدمت لكل الأطر والاحتفاظ بها لتستخدم في عملية فك الإخفاء لاحقاً.

في بعض أنظمة إرسال واستقبال الملتيميديا يمكن التسامح ببعض الأخطاء في البيانات التي أعيد بناؤها، فيمكن استعمال مقياس الكفاءة مقياساً لجودة النظام، وتوجد عدة أنواع أهمها:[13]

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

$$MSE = (\sum_{MN}[I_i(m,n) - I_{21}(m,n)]^2)/(M*N) \quad \ldots\ldots\ldots\ldots (1)$$

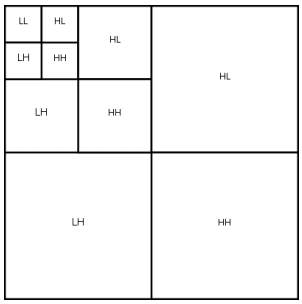
- قياس نسبة الضوضاء (Peak Signal–to–noise ratio): حسب المعادلة (2).

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

إذ تمثل R^2 قيم البيانات إذا كانت Floating Point أو Unsigned integer.

3. التحويل المويجي المتقطع Discrete Wavelets Translate (DWT)

يعمل التحويل المويجي على تقسيم الصورة إلى أربعة نماذج جزئية (Subsample)، الجزء الأول هو الصورة التي لها مرشـــح إمرار واطئ (Low Pass Filter) في كلا الاتجاهين الأفقي والعمودي أما الجزء الثاني فيحتوي على مرشــح إمرار واطئ في الاتجاه العمودي ومرشــح إمرار عالٍ (High Pass Filter) في الاتجاه الأفقي، أما الجزء الثالث فيحتوي على مرشح إمرار عالٍ في الاتجاه العمودي ومرشح إمرار واطئ في الاتجاه الأفقي، أما الجزء الرابع فيحتوي على مرشح إمرار عالٍ في كلا الاتجاهين الأفقي والعمودي، وكما في الشكل (1).[3]



الشكل (1): هيكلية البيانات في التحويل المويجي المتقطع

يعرف هذا التحويل بأنه الضــرب الداخلي للإشــارة مع مجموعة من المويجات التي تكونت بتوســيع ونقل دالة أحادية تسمى المويجة W(x)، كما في المعادلة (3).

$$W_{a,b} = (1/\sqrt{a}) * W(x - b/a) \quad \ldots\ldots\ldots\ldots (3)$$

إذ إن b يمثل معامل النقل الذي يحدد موقع المويجة، وa يمثل معامل التوسيع لترددات المويجة، فعندما تكون a صغيرة ($a < 1$) تكون الموجة منكمشة من الدالة الأحادية ويمكن تمثيل معظم الترددات العالية في الإشارة، أما عندما تكون a كبيرة ($a > 1$) فإن الموجة تنتشر وبالإمكان تمثيل معظم الترددات الواطئة في الإشارة، ويقصد بالتحويل المويجي تمثيل الإشارة بعمليتي الإزاحة والنقل للدالة الأساسية W(x) المعرفة باسم الموجة الأم (Mother Wavelet) ولغرض بناء الموجة الأم W(x) يحدد أولا دالة التقييس المعرفة بالمعادلة (4).[5][3]

$$\theta(x) = \sqrt{2}L(k)\theta(2x - k) \quad \ldots\ldots\ldots\ldots (4)$$

حيث L(k) تشير إلى مرشح الإمرار الواطئ، والدالة W(x) مرتبطة بـ $\theta(x)$ من خلال المعادل (5):

$$W(x) = 2\sum_h h(k)\,\theta(2x - k) \quad \ldots\ldots\ldots\ldots (5)$$

وأن h(k) تشير إلى مرشح الإمرار العالي، والشكل (2) يبين إطار من الفيديو تم تطبيق التحويل المويجي عليه.

الشكل(2): إطار من الفيديو الرقمي بعد تطبيق التحويل المويجي عليه

4. الفوضى Chaos

تعد نظرية الفوضـــى (Chaos Theory) من أحدث النظريات الرياضـــية الفيزيائية وتترجم أحياناً بنظرية الشـواش التي تتعامل مع موضـوع الجمل المتحركة (الديناميكية) اللاخطية التي تبدي نوعاً من السـلوك العشـوائي يعرف بالشواش، وينتج هذا السلوك العشوائي إما عن طريق عدم القدرة على تحديد الشروط البدائية تأثير الفراشة (Butterfly Effect)أو عن طريق الطبيعة الفيزيائية الاحتمالية لميكانيكية الكم[3]، وظاهرة الفوضـــى هي ظاهرة حتمية وتناظرية وهي عملية عشوائية تظهر في النظام الديناميكي غير الخطي بسبب الحساسية الشديدة للظروف الأولية وخارج مدارات انتشـــار على كامل المســـاحة ولقد اســـتخدمت في عدة مجالات منها إخفاء المعلومات لزيادة الأمن.[6]

إن أهم ما تمتاز به الدالة الفوضوية التعقيد العالي والتصرفات غير الخطية والحساسية المعتمدة على القيمة الابتدائية فعند إعطاء قيمة ابتدائية لنظام معين فمن المعروف أنه يمكن توقع الحالة المســـتقبلية للنظام إلا أنه في أنظمة الفوضى فإنّ توقع المدى البعيد يستحيل التنبؤ به.[4]

تعد نظم الفوضـــى حســـاســـة للشـــروط الابتدائية (Initial Conditions) وتعني أن أي جملتين متماثلتين تسـلكان مسـارات مختلفة كلياً ضـمن فضـائهما الطوري إذا اختلفت الشـروط الابتدائية ولو بشـكل ضـئيل، ومن الخصـــائص الأخرى قابلية التحويل (Transitive) وتعني أنه يمكن تطبيق تابع تحويل على أي مدة زمنية بحيث يقوم بمطها ومطابقتها مع مدة زمنية أخرى.[11]

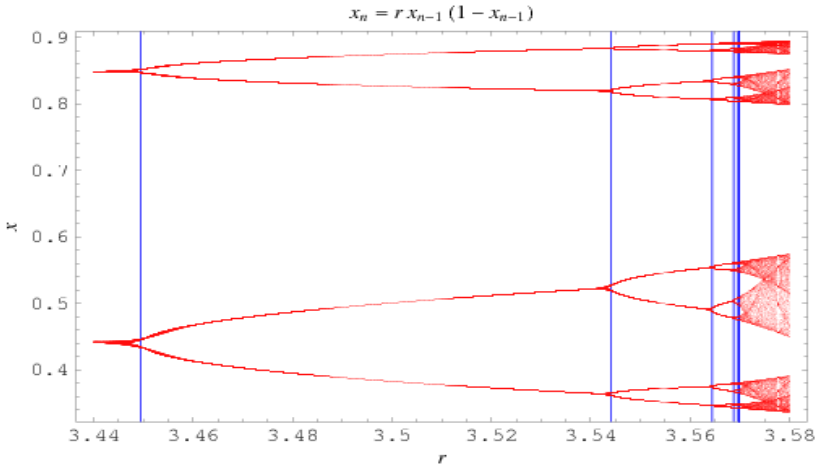
وتعد المسارات الدورية المتراصة (Periodic Orbits) ميزة أنظمة الاحتمالية للمتغيرات العشوائية، أي أن النظام يعمل باستقلالية كما أنه يكون على نحو محدد ومستقل وله مسارات دورية متراصة مع بعضها، كما أن كثافة القيم ثابتة في وقت محدد؛ وهذه الخاصية ضرورية في مجال التشفير والإخفاء، كما أن الدمج أو الخلط (Mixing) تعتبر ميزة الأنظمة التي يكون الانتشار في الفضاء ضمن مدة قصيرة بفاصل زمني صغير من الشرط الابتدائي، إذ إنه في الأنظمة الفوضوية تكون هذه المدة غير محددة بشرط ولكن عملها يكون اعتباطياً من قيم الشرط الابتدائي إذ يكون المسير قريباً من الشرط الابتدائي ولكن لا يتقاطع معه أبداً.[1] .

5. الدالة اللوجستية (Logistic Function)

توجد العديد من أنواع الدوال الفوضـــوية تمتاز كل منها بميزة عن غيرها، إذ تعد الدالة اللوجســـتية (Logistic Function) من أبسـط أنواع الدوال الفوضـوية المعروفة، فقد لوحظ اهتمام الكثير بها لما تمتاز به من خصـائص؛ إذ إن القيم المحددة التي تنشئها هذه الدالة هي قيم عشوائية تماماً في صـيغتها (على الرغم من أنها تقع ضـمن حدود معينة)، وهذه القيم لا تتكرر حتى بعد عدد من الدورات، وأهم صـفة لهذه الدالة هي حسـاسـيتها للقيمة الابتدائية بمعنى أن اثنين من القيم اللوجسـتية ولدت من شـروط ابتدائية مختلفة وغير مرتبطة إحصـائياً والأبحاث التي أجريت على الأنظمة الديناميكية للفوضـــى تدل على أن الدالة اللوجســتية تقف في حالة من الفوضـــى عندما تكون $3.5699456 < \mu \leq 4$ والأرقام التي تولدها هذه الدالة تكون غير دورية وغير متقاربة مما جعلها ذات أهمية عالية في مجال التشفير والإخفاء، أما التمثيل الرياضي للدالة فهو ممثل بالمعادلة (6).[10]

$$X_{n+1} = \mu(1 - X_n)X_n \quad \ldots\ldots\ldots\ldots\ldots (6)$$

إذ إن X_{n+1} هي عدد حقيقي يتراوح بين $(0 \geq X_{n+1} \geq 1)$, وX_n تمثل القيمة الابتدائية، و(μ) قيمة موجبة تتراوح قيمتها بين $(0 \leq \mu \leq 4)$ وكما في الشكل (3):[16]



الشكل(3): الرسم البياني التشعبي لسلوك الدالة اللوجستية

6. تشفير البيانات Data encryption:

إن تشفير البيانات هو من التطبيقات المهمة في مجال سرية المعلومات، وبما أن نقل البيانات الصريحة بين المرسل والمستلم يتم عبر قناة غير سرية فإن من الواجب نقل هذه البيانات على نحو غير مفهوم بالنسبة للمتطفل (الطرف الثالث غير المخول) وهذا ما يسمى بالتشفير والناتج معلومات مشفرة، أما عملية استرجاع البيانات الصريحة فتسمى بعملية فك التشفير[9][12]، استخدامت خوارزمية التشفير الفوضوي لتشفير أطر الفيديو الرقمي (السري) وتتلخص بما يأتي:

1-لكل شريحة لونية تحلل قيمها اللونية وتحول الى مصفوفة أحادية ذات طول (n).

2-إعطـاء القيمـة الابتـدائيـة لكـل من X_0 , μ (واللـذان يعـدان مفتـاحـا التشـــفير), بحيـث إن: $0 \leq X_0 \leq 1$، μ ∋ {4,3.5}، وإن هذه القيم يجب الاتفاق عليها بين المرسل والمستقبل.

3-اسـتخدام المعادلة $X_{n+1} = \mu(1 - X_n)X_n$ لتوليد سـلسـلة الأرقام الحقيقية (R) ذات حجم (n)، وكمثال للقيم العشوائية ولدت الأرقام الآتية لأحد أطر الفيديو الرقمي السري:

R=[0.9870 0.0513 0.1947 0.6273 0.9351 …. 0.2425 0.7348 0.7794 0.6876 0.8591 0.4840]

4-تحويل السلسلة (R) إلى سلسلة ذات أرقام ثنائية باستخدام المعادلة (7).

$$R_i = \begin{cases} 0 \; if \; R_i < 0.5 \\ 1 \; if \; R_i \geq 0.5 \end{cases} \quad \ldots\ldots\ldots (7)$$

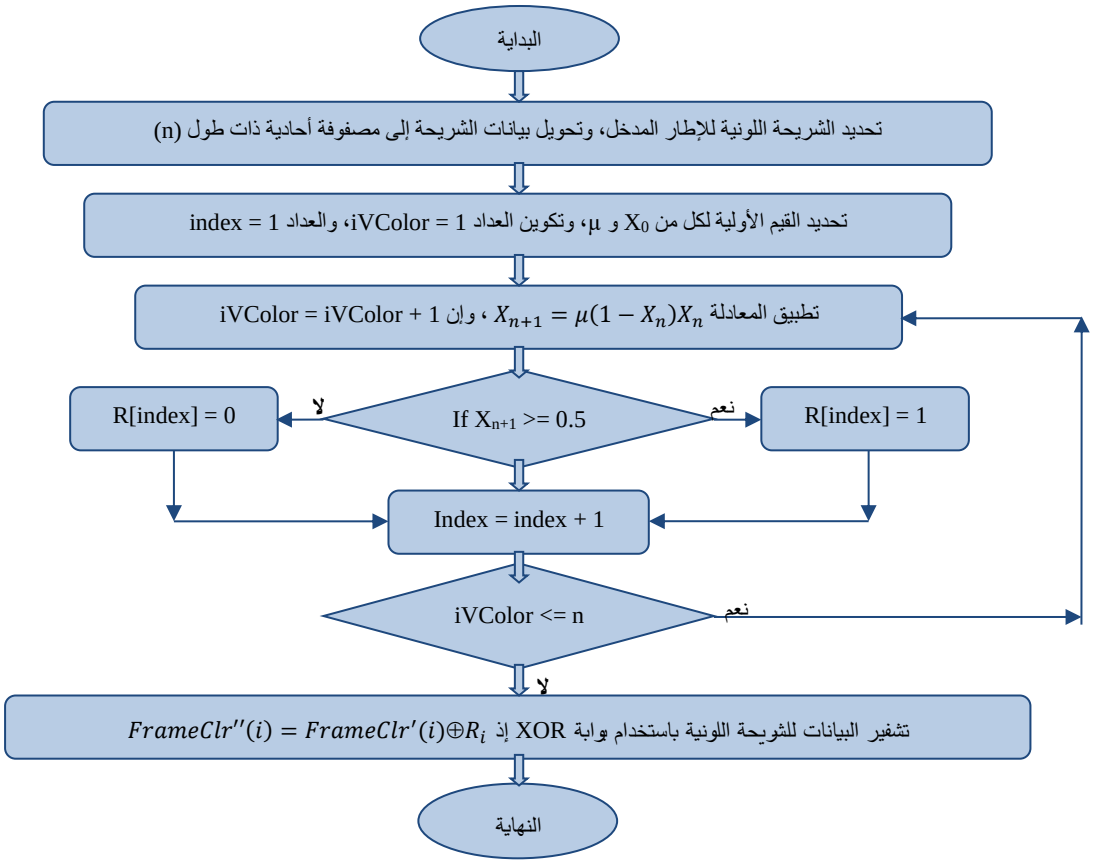
إذ إن n , ... ,i=0,1,2، وكمثال على ذلك:

R=[1 0 0 1 1 ..... 0 1 1 1 0]

5-إجراء عملية التشفير باستخدام البوابة XOR حسب المعادلة (8).

$$FrameClr''(i) = FrameClr'(i) \oplus R_i \quad \ldots\ldots\ldots\ldots\ldots (8)$$

إذ إن $0 \geq i \geq m-1$ ، وكما في المخطط الانسيابي(2).



المخطط الانسيابي(2): خوارزمية التشفير الفوضوية

7. إخفاء المعلومات Information Hiding

بعد إجراء عملية التشفير على ملف الفيديو الرقمي السري استخدمت خوارزمية الإخفاء الفوضوية للإخفاء التي ستنفذ على النحو الآتي:

1-تنفيذ التحويل المويجي المتقطع (DWT) على الإطار الغطاء (Cover).

2-إعطاء القيمة الابتدائية لـ (μ ،X_0) والتي تمثل بذرة الدالة اللوجستية وتعد المفتاح الأول للإخفاء.

3-تنفيذ الدالة اللوجستية $X_{n+1} = \mu(1 - X_n)X_n$ لـ (n-1) من المرات لتكوين السلسلة الآتية:

$X=\{X_1, X_2, X_3, \ldots\ldots\ldots , X_{n-1}\}$

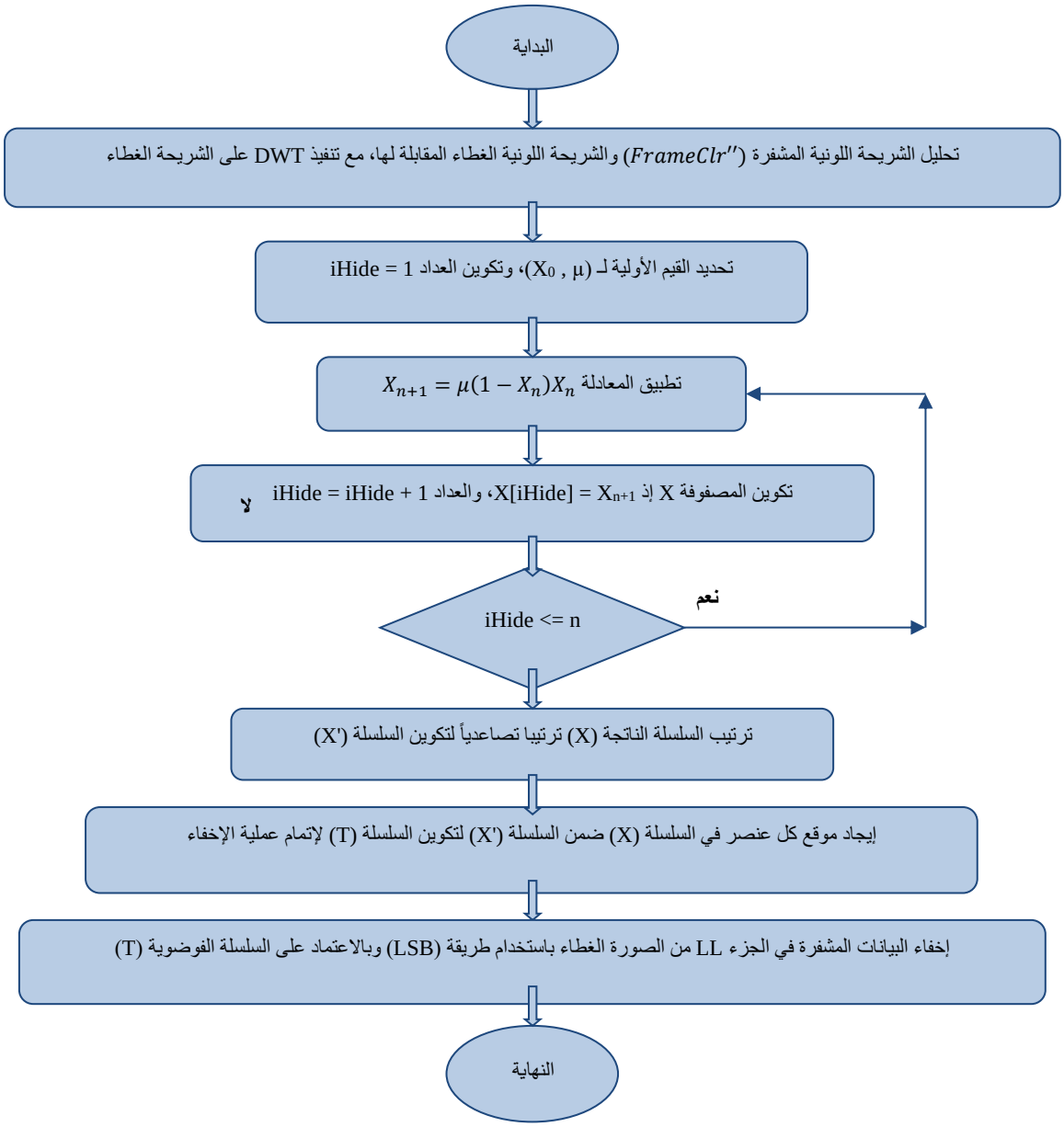
4-ترتيب السلسلة الناتجة ترتيباً تصاعدياً لتكوين سلسلة جديدة (X'):

$X'=\{X'_0, X'_1, X'_2, X'_3, \ldots\ldots\ldots , X'_{n-1}\}$

5-إيجاد موقع كل عنصر موجود في السلسلة (X) ضمن السلسلة (X') لتكوين سلسلة التحويل (T) التي تعد مفتاحاً للإخفاء: $T=\{ t_0, t_1, t_2, t_3, \ldots\ldots, t_{n-1}\}$

6-إخفاء البيانات المشفرة في الجزء LL من الإطار الغطاء باستخدام طريقة (LSB) وبالاعتماد على السلسلة الفوضوية (T).

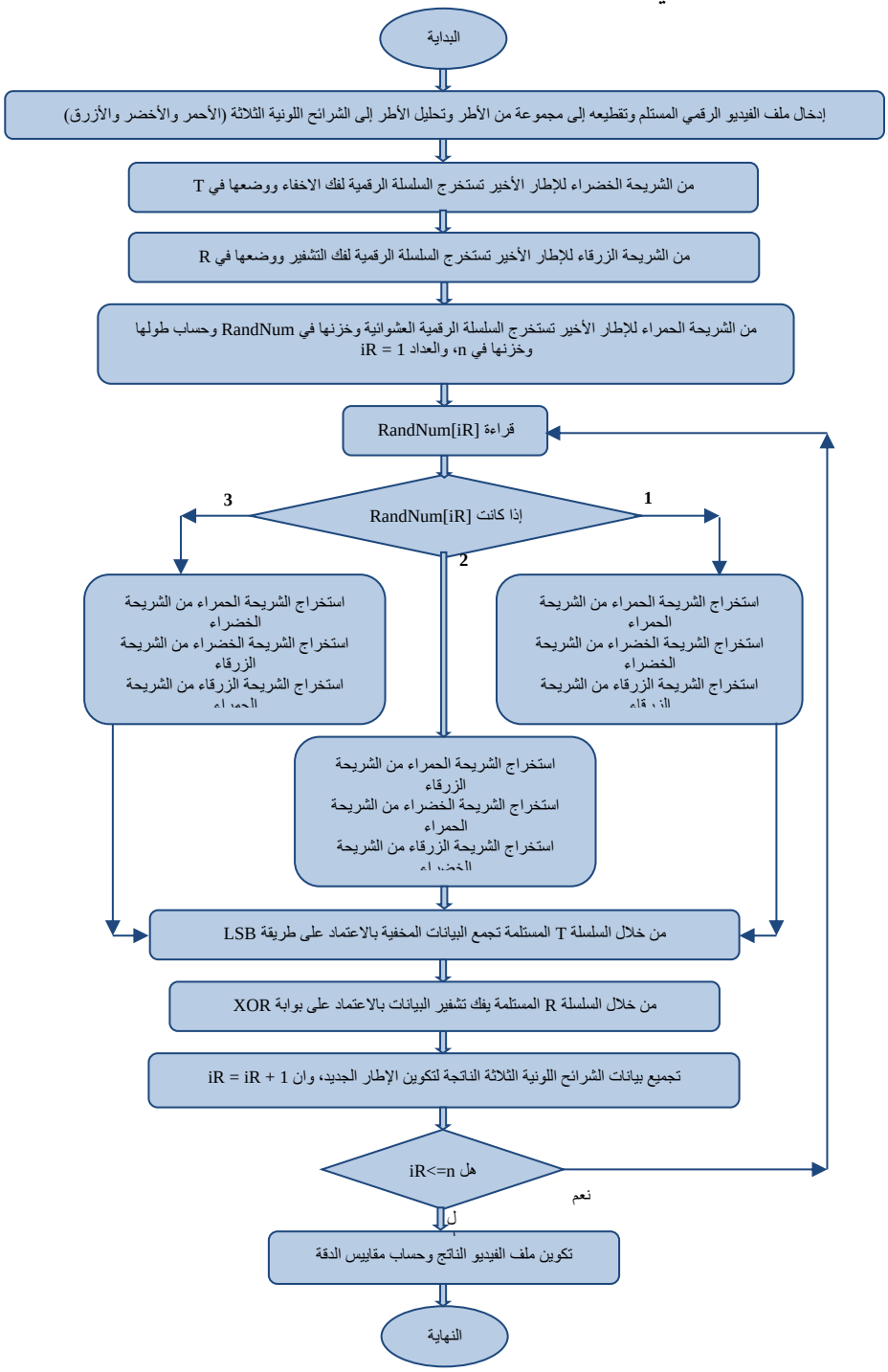
إن السلسلة (T) التي تكونت من هذه الخوارزمية (والتي ستحدد أرقام المواقع (Bytes) المستخدمة في الإخفاء) ستحتوي على قيم تتراوح بين (n,1) مرتبة بشكل عشوائي وغير متسلسل، وكما في المخطط الانسيابي (3).



المخطط الانسيابي (3): خوارزمية الاخفاء الفوضوية

8. خوارزمية الاسترجاع Recovery algorithm:

إن المرسل والمستقبل سيتفقان مسبقاً على قيم (X_0 , μ) الابتدائية المستخدمة في عمليتي التشفير والإخفاء، وذلك عن طريق قناة مخفية ذات سرية جيدة[14]، وأيضاً يتفق على استلام السلسة R التي تمت عملية التشفير بالاعتماد عليها، والسلسلة T التي من خلالها تمت عملية الإخفاء.



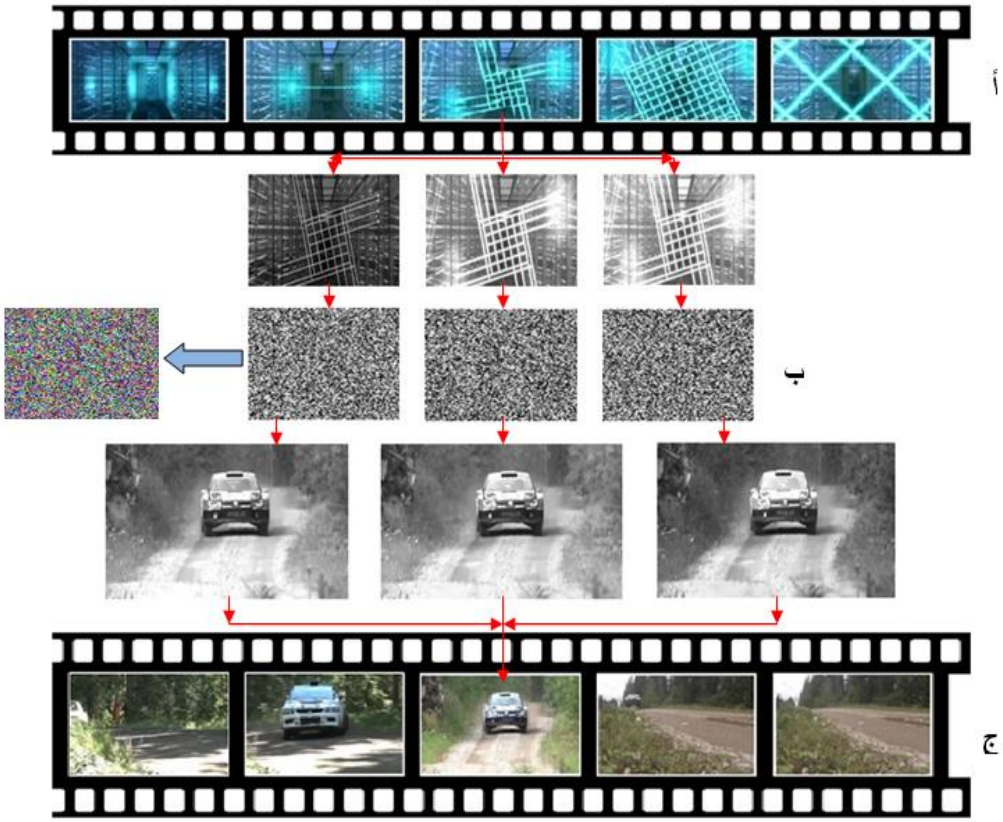
المخطط الانسيابي(4): خوارزمية الاسترجاع

تبدأ عملية الاسترجاع بإدخال المستلم الفيديو الرقمي وتقطيعه إلى مجموعة من الأطر، وتحلل بعدها الأطر إلى الشرائح اللونية الثلاثة (الأحمر والأخضر والأزرق)، والخطوة المهمة هي سحب سلسلة الأرقام العشوائية من

الشريحة الحمراء من الإطار الأخير للفيديو الغطاء المرسل (والأرقام هي إما 1 او 2 او 3) وخزنها بصيغة مصفوفة أحادية بحيث إن عدد الأرقام يمثل عدد أطر الفيديو السري التي من خلالها يتعرف المستلم على المواقع الصحيحة للشرائح اللونية المخفية داخل الشرائح اللونية للفيديو الغطاء، بعدها تتم عملية فك الإخفاء بالاعتماد على القيم الأولية المرسلة (μ , X_0) والسلسلة T التي تسحب من الشريحة الخضراء من الإطار الأخير للفيديو الغطاء المرسل لتظهر الشرائح اللونية المشفرة بحيث إن كل إطار يحتوي على شرائحه اللونية المشفرة، إذ تستخدم السلسلة R والقيم الأولية (μ , X_0) والتي تسحب من الشريحة الزرقاء من الإطار الأخير للفيديو الغطاء المرسل لإتمام عملية فك التشفير، وتجميع الشرائح اللونية ثم الأطر لتكوين الفيديو الرقمي المسترجع، وكما في المخطط الانسيابي(4).

9.التطبيق والنتائج Application and results:

طبقت خوارزميات العمل على مجموعة عينات مختلفة من ملفات الفيديو الرقمي والشكل (5أ) يوضح أنموذجاً من أطر ملف فيديو رقمي سري حللت إلى شرائحها اللونية الثلاثة ثم شفرت باستخدام خوارزمية التشفير كما في الشكل (5ب)، ثم أخفيت الأطر المشفرة داخل أطر ملف الفيديو الغطاء وكما في الشكل (5ج).

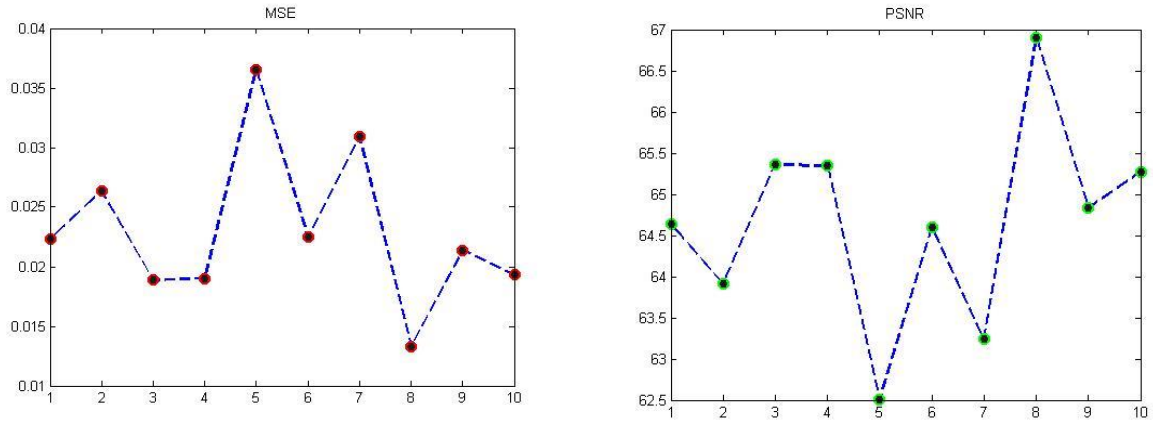


الشكل(5): نتائج تنفيذ خوارزميات العمل: أ- أطر من الفيديو المدخل ب- الشرائح اللونية المشفرة
ج- أطر من الفيديو الغطاء

بعد أن طبقت جميع خطوات العمل والحصول على نتائجها قيمت النتائج النهائية بوساطة الاختبارات الإحصائية التي تستخدم طرائق رياضية، حيث طبقت مقاييس الكفاءة على مجموعة عينات (أطر) مختلفة من الفيديو الرقمي والحصول على النتائج وكما في الجدول (1)، أما الشكل (6) فيوضح الرسم البياني للنتائج.

الجدول(1): نتائج مقاييس الدقة على أطر مختلفة

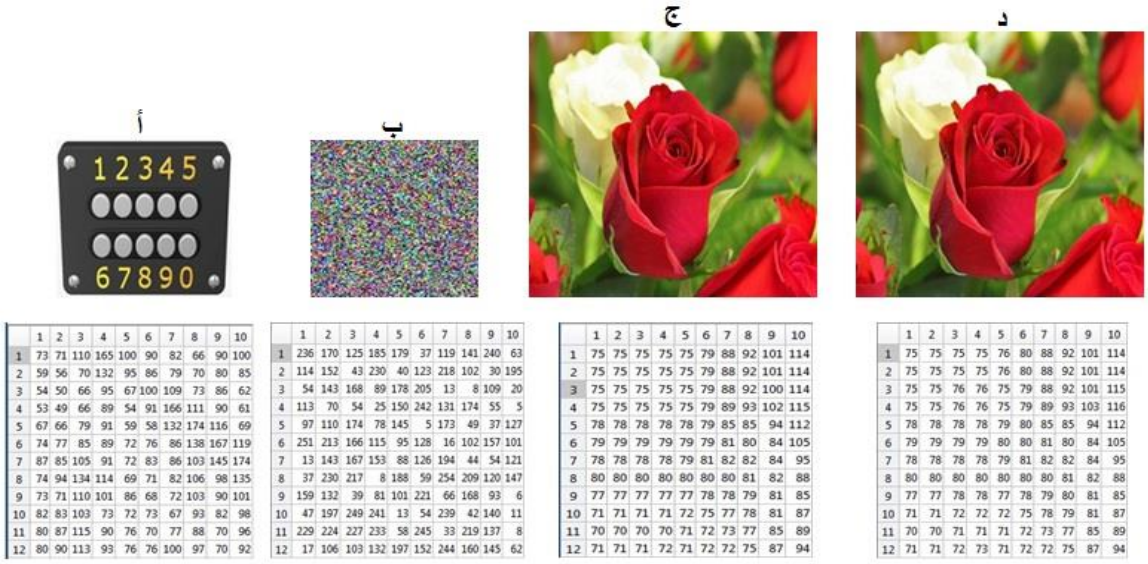
Frame No.	MSE	PSNR
1	0.0223	64.6422
10	0.0264	63.9094
20	0.0189	65.3609
30	0.0190	65.3431
40	0.0365	62.5113
50	0.0225	64.6035
60	0.0309	63.2373
70	0.0133	66.9066
80	0.0214	64.8330
90	0.0193	65.2744



الشكل(6): الرسم البياني لنتائج مقاييس الدقة والكفاءة

بعد الحصول على النتائج المطلوبة ومقارنتها مع الأعمال السابقة استدل على أن عملية التهجين حققت نتائج أفضل وسرية أعلى، فبمجرد أن يحاول المهاجم فك الاخفاء باستخلاص البيانات من الفيديو الرقمي الغطاء سيحصل على بيانات مبعثرة نتيجة تقانة الفوضى المستخدمة في الإخفاء والحصول على بيانات مشفرة يصعب فهمها نتيجة عملية التشفير الفوضوية، فضلا عما تميز به العمل وهو التعامل مع بيانات كبيرة الحجم؛ إذ كلما كانت كمية البيانات كثيرة زادت صعوبة تشفيرها وإخفائها، والشكل (7) يوضح مثالاً آخر لإطار من ملف فيديو سري شفر وأخفي في إطار لملف الفيديو الغطاء مع عرض لجزء من البيانات والأرقام لكل مرحلة.

كما أن تغيير البت الأقل أهمية هي من أقوى الخوارزميات الموجودة في فن الإخفاء التي تترك أثراً بسيطاً جداً في ملف الغطاء، ويتعسّر على العين البسيطة استكشاف التأثير، وبالتالي يستعصى فك رموزها حاسوبياً إذا ما أُخذ بنظر الاعتبار التفنن في الإخفاء، وإضافة اللمسات التشفيرية، واستخدام ملفات غير متوافرة النسخ.



	1	2	3	4	5	6	7	8	9	10
1	73	71	110	165	100	90	82	66	90	100
2	59	56	70	132	95	86	79	70	80	85
3	54	50	66	95	67	100	109	73	86	62
4	53	49	66	89	54	91	166	111	90	61
5	67	66	79	91	59	58	132	174	116	69
6	74	77	85	89	72	76	86	138	167	119
7	87	85	105	91	72	83	86	103	145	174
8	74	94	134	114	69	71	82	106	98	135
9	73	71	110	101	86	68	72	103	90	101
10	82	83	103	73	72	73	67	93	82	98
11	80	87	115	90	76	70	77	88	70	96
12	80	90	113	93	76	76	100	97	70	92

	1	2	3	4	5	6	7	8	9	10
1	236	170	125	185	179	37	119	141	240	63
2	114	152	43	230	40	123	218	102	30	195
3	54	143	168	89	178	205	13	8	109	20
4	113	70	54	25	150	242	131	174	55	5
5	97	110	174	78	145	5	173	49	37	127
6	251	213	166	115	95	128	16	102	157	101
7	13	143	167	153	88	126	194	44	54	121
8	37	230	217	8	188	59	254	209	120	147
9	159	132	39	81	101	221	66	168	93	6
10	47	197	249	241	13	54	239	42	140	11
11	229	224	227	233	58	245	33	219	137	8
12	17	106	103	132	197	152	244	160	145	62

	1	2	3	4	5	6	7	8	9	10
1	75	75	75	75	75	79	88	92	101	114
2	75	75	75	75	75	79	88	92	101	114
3	75	75	75	75	75	79	88	92	100	114
4	75	75	75	75	75	79	89	93	102	115
5	78	78	78	78	78	79	85	85	94	112
6	79	79	79	79	79	79	81	80	84	105
7	78	78	78	78	79	81	82	82	84	95
8	80	80	80	80	80	80	80	81	82	88
9	77	77	77	77	77	78	78	79	81	85
10	71	71	71	71	72	75	77	78	81	87
11	70	70	70	70	71	72	73	77	85	89
12	71	71	71	72	71	72	72	75	87	94

	1	2	3	4	5	6	7	8	9	10
1	75	75	75	75	76	80	88	92	101	114
2	75	75	75	75	76	80	88	92	101	114
3	75	75	76	76	75	79	88	92	101	115
4	75	75	76	76	75	79	89	93	103	116
5	78	78	78	78	79	80	85	85	94	112
6	79	79	79	79	80	80	81	80	84	105
7	78	78	78	78	79	81	82	82	84	95
8	80	80	80	80	80	80	80	81	82	88
9	77	77	78	78	77	78	79	80	81	85
10	71	71	72	72	72	75	78	79	81	87
11	70	70	71	71	71	72	73	77	85	89
12	71	71	72	73	71	72	72	75	87	94

الشكل (7): نتائج مراحل التنفيذ على احد اطر الفيديو السري، أ–الاطار السري وجزء من بياناته، ب–الاطار السري المشفر وجزء من بياناته، ج–الاطار الغطاء قبل الاخفاء، د–الاطار الغطاء بعد الاخفاء

10.الاستنتاجات Conclusions:

من خلال تطبيق الخوارزميات المقترحة لتشـفير وإخفاء ملفات الفيديو الرقمي باسـتخدام عمليات التهجين المقترحة، تم التوصل إلى الاستنتاجات الآتية:

1–أظهرت النتائج أن اسـتخدام عمليات التهجين المقترحة أدوات فعالة ومشـجعة لتشـفير وإخفاء ملفات الفيديو الرقمي، إذ طبقت خوارزميات العمل على أكثر من مقطع فيديو رقمي، ويمكن اعتبار عمليات التهجين كفوءة وتعطي نتائج جيدة ويمكن الحصـول على بيانات قريبة من البيانات الأصـلية، إذ أثبتت النتائج قوة وكفاءة الطريقة المقترحة.

2–إن عمليات التهجين والتقانات المقترحة تمتلك مرونة عند التعامل معها إذ يمكن تطبيقها على أطر الفيديو الرقمي بحجمها الكامل أو بتقسيمها إلى مجاميع (blocks).

3–كان للفوضـى الأثر الكبير في زيادة سرية الطريقة المقترحة وذلك بحساسيتها للقيمة الابتدائية لدالة الفوضـى المستخدمة (الدالة اللوجستية)، وأن نسبة الخطأ فيها يمكن اعتبارها قليلة، وبهذا يمكن الحصول على بيانات لا تختلف كثيراً عن البيانات الأصلية.

4–أدى اسـتخدام تقانة التحويل المويجي المتقطع (DWT) إلى زيادة قوة وسـرية الطريقة المقترحة، فمن خلال النتائج التجريبية تبين أن اسـتخدام تقانة التحويل المويجي المتقطع في الإخفاء لا يؤدي إلى تحطيم الفيديو الغطاء مما يعني التماثل الكبير بين ملف الفيديو قبل الإخفاء وبعده.

5–تبين من ملاحظة نتائج مقاييس الدقة والمبينة في الجدول (1) والتي طبقت على مجموعة غير متسلسلة من أطر الفيديو الرقمي الاسـتقرارية في قيمة مربع الخطأ (MSE) لجميع الأطر المطبقة وأن قيمها كانت قليلة جداً، في حين أنه لوحظت نسـبة الإشـارة إلى الضـوضـاء (PSNR) مرتفعة مما يدل على خزن البيانات بطريقة فوضوية التي تعكس إلى ما يهدف إليه البحث.

11.التوصيات Recommendations:

إن ما تم بني في هذه الخوارزميات يمكن أن يكون نقطة انطلاق لأفكار وأعمال مستقبلية ذات أهداف مشتركة، وعليه اقترحت الأعمال المستقبلية الآتية:

1-يمكن استخدام تقانات الذكاء الاصطناعي مثل الشبكات العصبية الاصطناعية في عمليات التهجين لإيجاد السلاسل الرقمية العشوائية في عمليات الإخفاء.

2-تقسيم أطر الفيديو إلى مجاميع وتطبيق الدالة الفوضوية باستخدام رتب وقيم أولية مختلفة لعمل مجموعة على وفق شروط وقواعد معينة.

3-إمكانية العمل مع الزمن الحقيقي (Real Time) في عملية إدخال ومعالجة الفيديو الرقمي التي تستخدم غالباً عبر شبكات الاتصالات بين البيانات المرسلة والمستقبلة.

4-يمكن استخدام دوال فوضوية أخرى في عمليات التشفير والإخفاء، أو يمكن استخدام دالة فوضى لعملية التشفير واستخدام دالة فوضى أخرى لعملية الإخفاء.

5-يمكن الاعتماد على طرائق أخرى لعملية الإخفاء بدلاً من خوارزمية الخلية الثنائية الأقل أهمية (LSB).

المصادر

[1] Chengqing L., Bingbing F., Jinhu L.U., 2018, 'Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy', International Journal of Bifurcation and Chaos c World Scientific Publishing Company.

[2] Dogan S., 2018, "A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map", I. J. Computer Network and Information Security,1, 1-9 Published Online January in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2018.01.01.

[3] Gourav T., Nath P. R., 2017, "Secret Information Transmission within Color Image using Wavelet Transformation", Gourav Tiwari et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 8 (3) , 2017, 394-400, ISSN: 0975-9646.

[4] H. Khodadadi, O. Mirzaei, 2017, "A stack-based chaotic algorithm for encryption of colored images", Journal of AI and Data Mining Vol 5, No 1, 2017, 29-37.

[5] Jerry D. G., 2000, 'Hand Book Of Image And Video Processing', Academic Press Series in Communications, Networking, and Multimedia, Copyright by Academic Press.

[6] Khaled H., 2018, "A New Technique for Secure Image Communication via Chaotic Circuit", IJCST Vol. 9, Iss ue 1, Jan - March ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print).

[7] Marwa E. M., Abdelmgeid A., Fatma O., 2016, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3.

[8] MUHALIM A., 2003, "INFORMATION HIDING USING STEGANOGRAPHY", Department of Computer System & Communication Faculty of Computer Science and Information system UNIVERSITI TEKNOLOGI MALAYSIA.

[9] Philipp J., 2015, "Analysis and Design of Symmetric Cryptographic Algorithms", Submitted to the Faculty of Computer Science and Mathematics of the University of Passau in Partial Fulfilment of the Requirements for the Degree Doctor Rerum Naturalium.

[10] Reatrey P., Sorawat C., Jaruwit P., 2018, "A Single, Triple Chaotic Cryptography Using Chaos in Digital Filter and Its Own Comparison to DES and Triple DES", International College King Mongkut's Institute of Technology, 978-1-5386-2615-3/18/$31.00 ©IEEE.

[11] Sankaran K. S. and Krishna B. V. S., 2011, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images', International Journal of Information and Education Technology, Vol. 1, No. 2, June.

[12] Saumya A., Ajay P., Romesh S., 2017, "Framework for Visual Cryptographic based Encryption and Decryption", International Journal of Computer Applications (0975 – 8887) Volume 163 – No 3, April.

[13] Shabieh F., Tariq S., Nazeer M., Nargis B., Adnan J., and Sidra A., 2017, "An Image Encryption Technique based on Chaotic S-Box and Arnold Transform", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6.

[14] Sumath C. P., Santanam T. and Umamaheswar G., 2013, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December.

[15] Tekalp A. M., 2015, 'Digital Video Processing', Second Edition, Copyright ©Pearson Education, Inc., ISBN-13: 978-0-13-399100-0, ISBN-10: 0-13-399100-8.

[16] Xue W., Liu S., Zhang M., Li X., 2017, "The Application of a Novel Fractional-order Hyper-chaotic System in Image Encryption", Department of Automation, Tianjin University of Science and Technology, 1038 Dagunanlu Road, Hexi District, Tianjin 300222, PR China.v.