جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل/ كلية العلوم للبنات
قسم علوم الحاسوب

تقنية العلامة المائية للصور الرقمية بالاعتماد على مبدأ الهوموفونك

مشروع مقدم إلى مجلس كلية العلوم للبنات في جامعة بابل وهو جزء من متطلبات شهادة البكالوريوس في علوم الحاسبات

مقدم من قبل الطالبة

رفل حيدر هلال

بإشراف

أ.د.محمد عبد الله ناصر

2024م 1445هـ

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

قَالُواْ سُبْحَـٰنَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ

أَنتَ ٱلْعَلِيمُ ٱلْحَكِيمُ

صدق الله العلي العظيم

(سورة البقرة: الآية 32)

الشكر والتقدير

أتقدم بخالص الشكر والتقدير إلى كل من ساهم في إنجاح هذا البحث، من أساتذة ولاسيما الدكتور الفاضل المشرف على هذا البحث (أ.د.محمد عبدالله ناصر)، وزملاء الأصدقاء، شكراً لكم على دعمكم وتشجيعكم المستمر.

رفل

الاهداء

الى أبي وأمي الحبيبين، لقلوبكما الطيبة التي ألهمتاني، ولرعايتكما الدائمة التي لا تنتهي،هذا البحث يهدي إليكما، باعتزازي وامتناني العميق .

وإلى أساتذتي الأعزاء، الذين ساهموا في توجيهي وتشجيعي خلال رحلة التعلم، هذا البحث هو ثمرة جهودكم الدؤوبة وعلمكم الثري أشكركم من القلب على كل شيء.

رفل

اقرار المشرف

أشهد إن إعداد هذا المشروع (**تقنية العلامة المائية للصور الرقمية بالاعتماد على مبدأ الهوموفونك**) قد جرى تحت إشرافي في قسم علوم الحاسوب في كلية العلوم للبنات / جامعة بابل وهو جزء من متطلبات نيل شهادة البكالوريوس في علوم الحاسبات من قبل طالبة المرحلة الرابعة **(رفل حيدر هلال)** للعام الدراسي 2023-2024م.

توقيع المشرف

اسم المشرف : أ.د.محمد عبدالله ناصر

ألمرتبه العلمية : استاذ

التاريخ: / /2024 م

الخلاصة

شهد العالم سيما في السنوات الأخيرة نموا هائلا في تطبيقات الوسائط المتعددة، يأتي كنتيجة طبيعية لثورة الإنترنت الهائلة وتطبيقاته. اذ ان التقدم السريع في الانترنت سهّل عملية تبادل المعلومات بمختلف انواعها، فاصبحت عملية تراسل المعلومات أسرع واكثر دقة في الوصول الى المكان المقصود. من جانب اخر، ظهرت الحاجة الى توفير وسيلة فعّالة لحماية حقوق الملكية الفكرية للأعمال الرقمية مثل الصور والفيديوات والمستندات الإلكترونية، وتتبع مصدر الأعمال الرقمية والتأكد من مصداقيتها وأصالتها، بالاضافة الى مراقبة كيفية استخدامها وتحليل سلوك المستخدمين، وهذا يوفر رؤى قيمّة لتحسين الخدمات وفهم السلوكيات والاهتمامات.

العلامة المائية الرقمية هي أحد الحلول المقترحة لتحقيق وضمان الحاجات انفة الذكر، والتي ممكن ان تكون شكلا أو صورة أو نص او فيديو توضع على المستند الاصلي لتوفير حماية للحقوق الفكرية او التأكد من مصداقية واصالة الرسائل المرسلة أو لاغراض اخرى كثيرة.

هذا المشروع يقدّم نظرة عامة حول العلامات المائية الصورية لحماية صور اخرى مختلفة. الهدف هو تطوير خوارزمية فعّالة وقوية للعلامة المائية يمكنها تضمين العلامات المائية واستخراجها مع الحفاظ على جودة الصورة العالية. اذ يقدم طريقة مقترحة لاضافة علامة مائية صورية (Watermark) لحماية صورة معينة (Cover) من خلال استبدال البتات الأقل أهمية (LSB) لصورة الغلاف بعدد مماثل من بتات اكثر أهمية (MSB) مأخوذة من صورة العلامة المائية. والجدير بالذكران الطريقة المقترحة لا تؤثر على بتات صورة الغلاف مطلقا، اذ نقوم الخوارزمية المقترحة بالبحث عن بتات العلامة المائية المراد اخفاؤها في بتات صورة الغلاف وبشكل متسلسل لحين الحصول على ما يشابهها ،وبالتالي تقوم بخزن موقع تلك البتات في مصفوفة احادية تسمى (Index vector) يتم ارفاق تلك المصفوفة مع صورة الغلاف وارسالها الى الطرف الاخر ليقوم بدوره باعتماد تلك المصفوفة في استرجاع العلامة المائية من صورة الغلاف المستلم.

اثبت النتائج التجريبية حصول الطريقة المقترحة على نتائج جيدة وفقا للمعايير المعتمدة في قياس كفاءة هذا النوع من الانظمة وهما مقياس (PNSR) ومقياس (MSE). واخيرا، فقد تم تنفيذ هذا العمل باستخدام لغة ماتلاب (MATLAB).

Abstract

In recent years, the world has witnessed tremendous growth in multimedia applications, which comes as a natural result of the massive Internet revolution and its applications. As the rapid progress in the Internet has facilitated the process of exchanging information of various types; also, the process of exchanging information has become faster and more accurate in reaching the intended place. On the other hand, there has been a need to provide an effective means to protect the intellectual property rights of digital works such as images, videos, and electronic documents, and to track the source of digital works and ensure their credibility and authenticity, in addition to monitoring how they are used and analyzing users' behavior. This provides valuable insights to improve services and understand behaviors and interests.

The digital watermark technique is one of the proposed solutions to achieve and ensure the aforementioned needs, which may be a form, image, text, or video placed on the original document to provide protection for intellectual rights, ensure the credibility and authenticity of sent messages, or for many other purposes.

This project provides an overview of image-based watermarking to protect various other images. The aim is to develop an effective and robust watermarking algorithm that can embed and extract watermarks while maintaining high image quality. It presents to add a watermark to protect another image (Cover) by replacing the least significant bits (LSB) of the cover image with equal number of most significant bits (MSB) taken from the watermark image. It is worth noting that the

proposed method does not affect the cover image bits at all, as the proposed algorithm searches for the bits of the watermark that are to be hidden in the cover image bits in a sequential manner until something similar is obtained, and thus it stores the location of those bits in a vector array called (Index vector). Attach this vector in the cover image and send it to the other party, so that it can rely on the vector to retrieve the watermark from the received cover image.

The experimental results demonstrated that the proposed method obtained good results according to the standards adopted in measuring the efficiency of this type of systems, which are the (PNSR) and the (MSE) performance metrics. Finally, this work was implemented using the MATLAB language.

قائمة المحتويات

الفصل الاول

مدخل عام

1-1 المقـــــــدمة

في العصر الرقمي، أثارت سهولة إنشاء المحتوى الرقمي ومعالجته وتوزيعه مخاوف كبيرة بشأن حماية حقوق النشر والتحقق من الملكية وسلامة البيانات. ومع توافر الصور الرقمية على نطاق واسع على شبكة الإنترنت وسهولة النسخ والتوزيع غير المصرح به، أصبح من الضروري تطوير تقنيات فعالة لحماية ملكية الصور الرقمية وسلامتها. لقد برزت تقنية العلامات المائية (Digital Watermarking) كحل واعد لمعالجة هذه المخاوف من خلال تضمين المعلومات المخفية في الوسائط الرقمية.

تتضمن العلامة المائية للصور الرقمية عملية تضمين معرف فريد أو رسالة سرية، تُعرف بالعلامة المائية (Watermark)، في الصورة المضيفة (Cover). ويمكن لاحقًا استخراج هذه العلامة المائية أو اكتشافها للتحقق من صحة الصورة أو ملكيتها أو سلامتها. تضمن تقنية العلامة المائية القوية وغير المحسوسة بقاء المعلومات المضمنة سليمة حتى في ظل وجود العديد من الهجمات وعمليات معالجة الصور، مع الحفاظ على الجودة المرئية للصورة ذات العلامة المائية [1].

2-1 بيان مشكلة البحث او المشروع

تواجه تقنيات العلامات المائية الحالية تحديات تتعلق بالأمان والمتانة وقدرة الحمولة. غالبًا ما تعتمد طرق وضع العلامات المائية التقليدية على تقنيات التضمين المباشرة التي تجعل العلامة المائية عرضة للكشف أو الإزالة أو التعديل بواسطة المستخدمين الضارين. بالإضافة إلى ذلك، قد تعاني هذه التقنيات من تغييرات ملحوظة في الصورة، مما يقلل من الجودة البصرية وتجربة المستخدم.

للتغلب على هذه القيود، هناك حاجة إلى تقنيات مبتكرة وقوية للعلامات المائية التي توفر أمانًا معززًا ومقاومة للهجمات وتحسين سعة الحمولة. يقدم مفهوم الهوموفونك (Homophonic Concept) أسلوبًا جيدا لوضع العلامات المائية على الصور الرقمية. ومن خلال الاستفادة من الغموض الذي تخلقه ، وبالتالي يصبح من الممكن

تضمين المعلومات بطريقة أقل عرضة للكشف أو الإزالة من قبل أطراف غير مصرح لها [2].

3-1 أهداف البحث او المشروع

الهدف الأساسي من هذا المشروع هو استكشاف وتطوير تقنية العلامة المائية للصور الرقمية على أساس مفهوم الهوموفونك. وان الأهداف المحددة هي كما يلي:

1. تطوير تقنية جديدة للعلامة المائية تعتمد على مفهوم الهوموفونك والذي يضمن المتانة وعدم القدرة على الإدراك وتعزيز سعة الحمولة.
2. تنفيذ تقنية العلامات المائية المقترحة باستخدام أدوات معالجة الصور الرقمية المتقدمة ولغات البرمجة.
4. تقييم أداء وفعالية تقنية العلامة المائية المطورة من خلال التجارب والتحليلات المكثفة.

4-1 أهمية البحث او المشروع

يحمل المشروع الذي تم إجراؤه العديد من الآثار والفوائد لمختلف أصحاب المصلحة والتطبيقات. إن تقنية العلامة المائية المقترحة المبنية لديها القدرة على [7،10] :

1. تعزيز حماية حقوق الطبع والنشر: من خلال تضمين معرفات فريدة أو معلومات ملكية، يمكن أن تساعد التقنية المقترحة في حماية حقوق الطبع والنشر للصور الرقمية، وتثبيط النسخ أو التوزيع أو التعديل غير المصرح به.
2. التأكد من سلامة البيانات: يمكن استخدام العلامة المائية للتحقق من صحة وسلامة الصور الرقمية المرسلة، مما يتيح للمستخدمين اكتشاف أي تعديلات غير مصرح بها أو محاولات تلاعب.
3. تحسين مصادقة المحتوى: يمكن للتقنية المقترحة أن توفر طريقة موثوقة وقوية لمصادقة المحتوى، مما يمكّن المستخدمين من التحقق من أصالة وصحة الصور الرقمية.

4. تسهيل توزيع الوسائط الرقمية: يمكن لتقنية العلامات المائية أن تتيح توزيعًا آمنًا ويمكن تتبعه للصور الرقمية، مما يضمن حصول المالكين الشرعيين على الائتمان المناسب والعائدات مقابل عملهم.

وغير ذلك من الفوائد التي لا يتسع المجال لذكرها.

5-1 الهيكل العام للمشروع

تم تنظيم المشروع في خمسة فصول. يقدم الفصل الأول مقدمة لموضوع البحث، ويعرض بيان المشكلة، ويحدد الأهداف، ويسلط الضوء على أهمية الدراسة.

يستعرض الفصل الثاني الأدبيات ذات الصلة بتقنيات وضع العلامات المائية على الصور الرقمية، والخوارزميات المعتمدة، وعمليات معالجة الصور. يقدم هذا الفصل فهمًا شاملاً للمنهجيات الحالية ونقاط القوة والضعف فيها.

يعرض الفصل الثالث تفاصيل تقنية العلامة المائية المقترحة بناءً على مفهوم الهوموفونك. ويصف المنهجية والخوارزميات والتقنيات

يتضمن الفصل الرابع التطبيق العملي لمراحل تنفيذ الطريقة المقترحة واهم النتائج المستحصلة.

الفصل الخامس يستعرض الاستنتاجات التي توصلنا اليها، بالاضافة الى طرح افكا او تصورات عن اعمال مستقبلية ممكن تطويرها.

اخيرا المصادر المعتمدة.

الفصل الثاني

المفاهيم الاساسية للمشروع

2.2 المقدمة عامة

أحد أسباب نجاح المتسللين(**Intruders**) هو أن معظم المعلومات التي يحصلون عليها الحصول عليها من النظام يكون في شكل يمكنهم قراءته وفهمه. المتسللين قد يمكنهم الكشف عن المعلومات للآخرين، أو تعديلها لتشويه صورة فرد أو التنظيم أو استخدامه لشن هجوم. أحد الحلول لهذه المشكلة هو من خلال استخدام إخفاء المعلومات (**Information Hiding**) [3]

فإخفاء المعلومات هي أحدى التقنيات العالية الأمنية التي تستعمل لإخفاء المعلومات المهمة مختلفة الهيئات داخل وسائط مختلفة (**Media**) بهيئة لا تشعر نظام الرؤيا البشري **Human Visual System) HVS**)بوجودها. بصورة عامة يوجد اتجاهين لإخفاء المعلومات هي [1] :

أولا : الإخفاء (**Steganography**) :- ويعني إخفاء المعلومات المهمة والمختلفة الهيئات داخل وسائط أخرى بطريقة لا تسمح للمتطفل باكتشافها .

ثانيا : العلامة المائية (**Watermarking**) :- تُعدُّ العلامة المائية الرقمية (**Digital Watermarking**) وسيلة فعالة لحماية حقوق النسخ (**Copyright**) للوسائط الرقمية مثل صورة(**Image**)،صوت(**Audio**)وغيرها ،إذْ يتم إخفاء المعلومات السرية داخل إشارات رقمية .إن أحدى المساوئ الشائعة في معظم طرائق الإخفاء الموجودة هي التشويه(**Distortion**) الظاهر في صوره الغطاء الذي يبدو كضوضاء **(Noise)** نتيجة لإخفاء البيانات. وعلى الرغم من أنّ هذا التشويه يكون في بعض الأحيان قليلاً جدا ولكنه غير مقبول في بعض الحالات مثل الصور الطبية (**Medical Images**) والصور الحربية (**Military Images**) .كما ان أحدى تطبيقات إخفاء البيانات هي تقنيات العلامة المائية الرقمية (**Digital Watermarking Applications**) وفيها توجد علاقة قويه بين

الرسالة وصورة الغطاء ، بحيث إنّ الرسالة تدعم (تضيف) معلومات مكملة (اضافيه) لصورة الغطاء مثل عنوان الصورة (**Image Caption**) أو بصمة المؤلف (**Author Signature**) لذا فإنّ التشوهات يجب أن تكون اقل ما يمكن.إنّ المتطلبات الأساسية لأي نظام إخفاء هي التحصين وعدم القدرة على الاكتشاف والسرية و عدم الرؤيا والسعة ولكن لا يمكن الحصول على نظام يجمع هذه المتطلبات بصورة مثالية .لذا يجب أن تكون هنالك موازنة مقبولة بين هذه العناصر(المتطلبات) تحدد من قبل التطبيق .على سبيل المثال ، إن إخفاء المعلومات قد يتسامح فيما يخص التحصين و لكن يطلب سعة كبيرة قدر الإمكان و اقل إدراك (بدون حدوث تشويه واضح في صورة الغطاء).على حين لا تحتاج العلامة المائية الرقمية إلى سعة كبيرة وإلى تقليل الإدراك و إنما تحتاج إلى زيادة في التحصين .

2-2 إخفاء المعلومات (Information Hiding)

تقنيات الإخفاء مثل إخفاء المعلومات العلامة المائيه (**Digital Watermarking**) كان إخفاء المعلومات المبكر فوضويًا. قبل الهواتف قبل البريد، قبل الخيول، تم إرسال الرسائل قدم. إذا أردت إخفاء رسالة، فلديك اثنتين الخياران: أن يحفظه الرسول، أو يخفيه على الرسول. في حين تلقت تقنيات إخفاء المعلومات اهتماما هائلا في الآونة الأخيرة، وتطبيقه يعود إلى العصر اليوناني. بحسب اليونانية المؤرخ هيرودوت، اليوناني الشهير استخدم أثناء وجوده في السجن، أسلوبًا غير عادي أرسل رسالة إلى صهره. حلق رأسه من العبد أن يرسم رسالة على فروة رأسه ثم انتظر هيستياوس حتى ينمو الشعر مرة أخرى رأس العبد قبل إرساله إلى صهره. القصة الثانية جاءت أيضًا من(Herodotus) ، الذي يدعي أن جنديًا يُدعى ديميراتوس) (Demeratus يحتاج إلى ذلك أرسل رسالة إلى (Sparta that Xerxes) ينوي إرسالها غزو اليونان. في ذلك الوقت، كانت وسيلة الكتابة هي مكتوبة على لوح مغطى بالشمع. تمت إزالة (Demeratus) الشمع من اللوح كتب الرسالة السرية على الخشب الأساسي، استردت اللوحة باستخدام الشمع لجعله يبدو كقرص فارغ وأخيراً أرسل المستند دون أن يتم اكتشافه. لطالما كانت الأحبار غير المرئية طريقة شائعة إخفاء المعلومات. كان الرومان القدماء يكتبون بين السطور باستخدام أحبار غير مرئية تعتمد على السهولة المواد المتاحة مثل عصائر الفاكهة

ولبن. عند تسخينها، فإن الأحبار غير المرئية سوف تفعل ذلك أغمق، وأصبح مقروء بصورة عامة يمكن تصنيف إخفاء المعلومات على نوعين رئيسيين هما [4].:

الإخفاء (Steganography) :- وهو علم وفن الاتصال بطريقة تخفي وجود الرسالة (هدف التصنت) داخل رسالة أخرى أو أي وسط حامل بحيث لا يمكن للعدو اكتشافها .إنّ الكلمة(Steganography)مشتقة من الكلمتين الإغريقيتين (Stegein)و (Grajein) والترجمة الحرفية لها هي الكتابة المخفية (Covered Writing).

العلامة المائية الرقمية (Digital Watermarking) : -وتعني إخفاء المعلومات متعددة إلهيات(Multi Media Information)ولكن قد تكون مرئية(تحول بعض المعلومات لتشكل صفة في الغطاء مثل حق النسخ (Copyright) أو تكون غير مرئية،و لا يمكن إزالتها.

2-3 العلامة المائية الرقمية Digital Watermarking

هي قطعة من المعلومات موجودة (مخفية) في البيانات المقصود حمايتها (ادعاء الملكية) بحيث من الصعب جدا إن تزال العلامة المائية من البيانات المضافة إليها [3] .

2-3-1 الفرق بين العلامة المائية والتشفير[3]

يعتبر علم الإخفاء قديم جدا ، ويعتمد على إرسال المعلومات بطريقة مخفية لا تحدث أي تغير ملحوظ على المعلومات المرسلة ، بينما تحدث التعمية(التشفير) تغييرا جذريا للمعلومة المراد إرسالها في عملية مكشوفة يمكن رؤيتها وملاحظتها بسهولة. للتعمية Encryption أهمية في إخفاء المعلومات المهمة التي تخص إفراد أو مؤسسات أو دولا، إلا أن الرسائل المشفرة قد تتعرض لكسر من منطلق امن وحماية الوطن . وفي حالة عدم التمكن من كسرها ، فانه لايسمح لها بالمرور إلى الجهة المراد إرسالها إليها. وهذا بدوره حفز العلماء والمختصين إلى اختراع أوالبحث عن وسائل أخرى لإرسال المعلومات وبطريقة سرية لاتلفت الانتباه وصعب كشفها ، لذا عمدوا إلى وسيلة تعرف بعلم إخفاء المعلومات Steganography . هناك طرق متعددة لإخفاءالمعلومات عُرفت عبرالتاريخ، ومنها على سبيل المثال كتابة الرسائل بالحبر الخفي أو

باستخدام طرق أخرى مثل سائل الليمون أو غيره من الأحبار الخفية. وقد تطور هذا العلم تطوراً كبيراً في الوقت الحاضر لما له من أهمية ولاختلافه عن علم التعمية الذي يمكن ملاحظة الرسالة المشفرة في حالة إرسالها بينما في حالة إخفاء المعلومات تُخفى المعلومة المراد إرسالها في معلومة أخرى بطريقة لاتثير الشك ، وكذلك تستخدم العلامة المائية التي من شانها إخفاء المعلومات التعريفية للمصدر، حيث تستخدم حاليا في المحاكم الشرعية لمقاضاة المزورين أو المخربين ،فقد صممت بطريقة يصعب (في الغالب) على المعتدي اكتشافها أو التخلص منها.

2-3-2 خصائص العلامة المائية الرقمية [8،11]

هناك العديد من المتطلبات لتقنية العلامة المائية المثالية. يعتمد ذلك على التطبيق الذي يستخدم فيه، ولكن يجب أن يكون هناك توازن بين هذه المتطلبات لأن هناك علاقة بينهما حيث أن الزيادة في أحدهما قد تؤدي إلى نقصان الآخر. في تطبيق حماية حق المؤلف يتعلق الأمر بمتانة المتطلبات، بينما في تطبيق المصادقة يركز على موقع المنطقة التي تم العبث بها وما إذا كان العبث مقصودًا أم غير مقصود. هذه المتطلبات هي:

1- القوة Robustness : تشير إلى القدرة على اكتشاف العلامة المائية بعد إجراء عمليات معالجة الإشارات والمتمثلة بعمليات القطع ، الضغط ،الترشيح وغيرها وبالتالي فان العلامة المائية الرقمية لابد من إكسابها مرونة ضد هذه المعالجات وذلك لمنع اكتشافها أو إزالتها وليس كل التطبيقات العلامة المائية الرقمية تتطلب القوة ،على سبيل المثال العلامات الرقمية المستخدمة في التلفزيون والإرسال الإذاعي ففي هذين التطبيقين تتركز حاجة العلامة المائية الرقمية في عملية الإرسال فقط (أي لاتتجاوز إذاعة أو قناة معينة على الأخرى)[4] .

2- يجب أن تكون غير قابلة للمسح بشكل إحصائي أي التحليل الإحصائي غير قادر على أنتاج أي فائدة من وجهة نظر المهاجم (المهاجم هو الشخص الذي يحاول إزالة أو أتلاف العلامة المائية الرقمية).

3- يجب تثبيت أكثر من علامة مائية لعدم انجاز أي فائدة من وجهة نظر المهاجم .

4- الغموض Imperceptibility : عند وضع أكثر من علامة مائية رقمية يجب إن تكون غير محسوسة لمنع اكتشافها بسهولة وان هذا المفهوم يكون مستند على خصائص النظام السمعي أو

البصري للإنسان ،حيث النظام السمعي أو البصري غير قادر على التمييز بين البيانات التي تحتوي على معلومات مخفية بداخلها وبين التي لاتحتوي على معلومات وبالتالي يكون المهم تصميم طرق العلامة المائية الرقمية بحيث تستغل هذا التأثير[1] .

5- السعة والكمية Capacity and Mount: حيث إن علامة مائية تتكون من ثلاث كلمات أفضل من علامة مائية تتكون من كلمة واحدة وذلك لتوفير سرية أكثر وفي نفس الوقت يجب إن تتناسب مع كمية البيانات الأصلية .

6- الكفاءة : إجراء موازنة بين القوة والغموض ، حيث إن هنالك image، audio يكون من الصعوبة إضافة علامة مائية رقمية لها على سبيل المثال صورة من نوع binary color يكون من غير المعقول إضافة علامة مائية رقمية في منطقة محددة بحيث تؤدي إلى تغير واضح في ألوان الصورة أو أنها تسبب noise ملحوظة عند إضافتها في موجة معينة .

7- الكلفة : يجب إن تتوازن كلفة العلامة المائية مع كلفة البيانات الأصلية على سبيل المثال كلفة طباعة كتاب معين يجب إن تتوازن مع كلفة العلامة المائية الرقمية المراد إضافتها له .

2-3-3 تمثيل العلامة المائية الرقمية

تتمثل العلامة المائية الرقمية بعدة طرق منها :

1. باستخدام الصور (Image)
2. باستخدام النص (Text).
3. باستخدام الصوت (Audio).
4. باستخدام الفيديو (Vedio).

2-3-4 طرق تصنيف العلامة المائية الرقمية[3,4]

1- من ناحية الظهور:-

أ- **علامة مائية مرئية visible watermarking** :

العلامة المائية المرئية أو المحسوسة تكون ممثلة عادة بال Watermark في الصورة image أو النص text وان محاولة رفعها من الصورة يؤدي إلى تشويه الصورة الأصلية وتستعمل عادة مع الخرائط والرسومات وفي البرمجيات .

ب- غير مرئية invisible watermark :

العلامة المائية الغير محسوسة تستعمل بصورة واسعة مع العلامة المائية من نوع audio ،video كذلك image وهذا النوع فقط للشخص الذي قام بوصفها يستطيع معرفتها أو الوصول إليها ولقد تم اللجوء إلى النوع هذا وذلك لجعل عملية تتبع المهاجم بصورة أكثر سرية حيث تكون ذات فائدة لاتصدق في مسار الفايلات كما أنها تقوم ببرهنة قانونية ضد من يقوم بعملية نسخ غير قانوني .

2- من ناحية قوة الخوارزمية في تضمين العلامة المائية :-

أ- ضعيفة (سهلة الكشف والتدمير) :

العلامة المائية الضعيفة يكون هذا النوع ذو قوة محددة ويمكن تغييره بسهولة إذا حصل تغيير للكيان الذي يحتوي على هذا النوع ويستخدم بصورة كبيرة في التحويل.

ب- قوية (صعبة الكشف والتدمير) :

العلامة المائية القوية في هذا النوع تكون الخوارزمية المبينة على أساسها تتمتع بخصائص جيدة بحيث من الصعب الوصول إليها وبالتالي لايمكن بناء خوارزمية معالجة لها والتي تؤدي إلى إزالة العلامة المائية ألا من قبل الشخص الذي قام بوصفها. تستخدم بصورة كبيرة في تطبيقات إل finger printer، copy write production .

3- تصنيف العلامة المائية من ناحية المدخلات والمخرجات :-

أ- العلامة المائية الخاصة أو الغير محجوبة Private watermarking

العلامة المائية الخاصة أو الغير محجوبة . إن الأنظمة التي تعمل بهذا النوع تتطلب على الأقل البيانات الأصلية وكذلك البيانات التي تحتوي على العلامة المائية وكذلك تحتاج إلى public key لاستخلاص العلامة المائية .يمتاز هذا النوع بالقوة ولكنه صعب الاسترجاع خصوصا في حالة فقدان الكيان الأصلي .

ب- العلامة المائية النصف خاصة أو محجوبة semiprivate watermarking or semi blind :

العلامة المائية النصف خاصة أو محجوبة . في هذا النوع يتم استرجاع العلامة المائية بطريقة مشابهة للنوع السابق . وان الطريقة الأولى والثانية تستخدم في عدة تطبيقات (أثبات المالك الحقيقي ، سيطرة النسخ) .

ت- العلامة المائية أو تسمى بالعمياء (المحجوبة) Public Watermarking Or Blind:

العلامة المائية أو تسمى بالعمياء (المحجوبة) . في هذا النوع يتطلب فقط إل watermarking object والمفتاح الذي تم استخدمه لاسترداد العلامة المائية .لذلك تعتبر هذه الطريقة من أصعب الطرق وتحتاج إلى محاولات لاسترجاعها لذلك سميت بالعمياء .

2-3-5 صفات العلامة المائية الرقمية[2]

أ- صعبة التقليد

ب-مستحيل للإزالة بدون تحطيم الوسط (البيانات الأصلية) .

2-3-6 الهيكل المثالي لنظام العلامة المائية الرقمية

يتكون نظام علامة مائية رقمية من جزئيين رئيسين:

1. **وحدة تضمين العلامة المائية** :- في هذه المرحلة يثم تضمنين العلامة المائية (watermarking)داخل المضمّن فيه (Cover).

3- **وحدة استخلاص وكشف العلامة المائية** :- تتضمن هذه المرحلة تحديد فيما إذا كانت الصورة(او وسط اخر) تحتوي على علامة مائية بواسطة مفتاح معين .عند تحديد وجود العلامة المائية بصورة صحيحة إذا من الممكن استخلاص المعلومات المخفية.

4-2 التشويهات والهجمات Distortions And Attacks

هناك عدة ضوضاء وهجمات قد تصيب العلامة المائية، نذكر منها على سبيل المثال [6]. :

1- الضوضاء المضافة Additive Noise :-

ربما ينشا في التطبيقات من استخدم المحولات Digital/Analog، Analog/Digital أو من أخطاء الإرسال . على أي حال فان المهاجم يمكن إن يقدم شكل من الضوضاء الملحوظ [3] .

2- الترشيح Filtering :-

الترشيح بمرور منخفض على سبيل المثال لايقدم تشويه مؤثر على الصورة خصوصا إذا كانت العلامة غير مرئية لكن يمكن أن يؤثر على الأداء بشكل مثير ويقصد بالأداء عمليات استرداد العلامة المائية الرقمية لان إمرار الصورة على ترشيح يؤدي إلى تغير في بعض قيم الصورة [3].

3- القص Cropping :-

هذا الهجوم أكثر شيوعا بسبب اهتمام المهاجم بجزء صغير من مادة العلامة المائية مثل أجزاء لصورة معينة أو إطار فيديو متسلسل لذلك ومن اجل البقاء تحتاج العلامة المائية إلى الانتشار فوق الإبعاد عندها يأخذ هذا الهجوم بنظر الاعتبار[4] .

4- الضغط Compression:-

يتضمن عملية تقليص البيانات الأصلية الحاوية على علامات مائية رقمية وبالتالي فأن العلامة المائية الرقمية يمكن إن تتعرض إلى تشويه نتيجة لهذا الإجراء .هذا الهجوم غير مقصود الذي يظهر غالبا في تطبيقات متعددة الأوساط (الصوت والأفلام والصور) عند ضغطها لإرسالها عبر الانترنيت إذا العلامة المائية تتطلب مقاومة مستويات مختلفة من الضغط[4].

5- العلامة المائية الرقمية المضاعفة Multiple Watermark :-

المهاجم من المحتمل إن يضيف علامة مائية لمعلومات تحتوي مسبقا على علامة مائية ويدعي بالملكية ،الحل الأسهل هو بوضع بصمة وقت للمعلومات المخفية .

6- التوسط الإحصائي Statistical Averaging :-

المهاجم ربما يخمن العلامة المائية وعلية يتخلص من العلامة المائية ، هذا سوف يكون خطرا إذا كانت العلامة المائية غير معتمدة فعليا على البيانات [4] .

5-2 تقنييات تضمين العلامة المائية

في السنوات الأخيرة، أصبحت التطبيقات التي تستخدم الصور ذات التدرالرمادي أو تم تمديد مقاطع الفيديو إلى مقاطع الفيديو الملونة. كل إطار اللون

في تسلسل فيديو يحتوي على ثلاثة مكونات، أحمر (R)، أخضر (G) والأزرق (B)، في مساحة ألوان RGB. بدلا من ذلك، الإنار (Y) ومكونات التلون (U و V) في YUV

يمكن إنشاء المجال من مصدر RGB. قناة Y يمثل الكثافة الإجمالية ومعظم المعلومات حول الإطار وتمثل قنوات U وV اللون معلومة

باستخدام DCT ثم يقوم بتضمينه في دفق بت MPEG-2. يتم استخراج العلامة المائية لهذه الطريقة من فك التشفير

الفيديو بطريقة عمياء. تشونغ وآخرون. تقدم أيضاً

تقنية العلامة المائية لفيديو MPEG-2 عن طريق استغلال تقنية الطيف المنتشر بالتسلسل المباشر. هذه التقنية يركز على قوة تضمين العلامة المائية ومساحتها التضمين للحفاظ على جودة الفيديو الذي يحمل علامة مائية. يقوم باستخراج العلامة المائية من بت MPEG-2 الذي يحمل العلامة المائية دفق دون الاعتماد على تسلسل الفيديو الأصلي.

يقوم المؤلفون أيضًا بإجراء فك تشفير جزئي لتدفق البتات المضغوطة كما في طريقة Hartung et alومع ذلك، فإن أسلوبهم يستخدم مستويات رمادية متعددة تعتمد على المشهد العلامات المائية التي توفر المزيد من المعلومات الإدراكية وتحسين الجودة المرئية للفيديو الذي يحمل علامة مائية. يتم بعد ذلك تضمين العلامة المائية للطيف المنتشر عن طريق التعديل معاملات DCT. وتظهر نتائجهم التجريبية أن هذا المخطط قوي لعدة أنواع من الهجمات. في خوارزمية العلامة المائية للفيديو التي يمكن تنفيذها في تم تصميم نطاق VLC لتدفق بتات الفيديو MPEG-2. ومع ذلك، على الرغم من أنه يستغل علامة مائية تعتمد على الإطار للتعامل مع هجوم تقدير العلامة المائية (WEA)، فإنه يفعل ذلك لا تنظر في الهجمات الهندسية [3].

6-2 اهم تطبيقات العلامة المائية [3,7]

1.وقاية حق النشر أو التأليف watermarking for spy right protection :

إن وقاية حق النشر أو التأليف هو على الأرجح تمثل معظم التطبيقات للعلامة المائية البارزة في الوقت الحاضر وتتضمن عملية طمر المعلومات عن المصدر الرئيسي وعلى هذا النمط فان مالك حق النشر أو التأليف الأصلي للبيانات يمنع الإطراف الأخرى بالمطالبة بحقوق النشر أو التأليف وبالتالي فان العلامة المائية الموضوعة تدل على المالك الشرعي فقط[7] .

2.العلامة المائية لحماية النسخ watermarking for copy protection :

إن الهدف من هذه التقنية هو منع النسخ الغير مخول حيث إن الصفة المرغوب فيها توزيع أنظمة الوسائط المتعددة هو وجود طرق لحماية النسخ وان هذه الطريقة صعبة الانجاز في الأنظمة المفتوحة (عدد المستخدمين يكون غير محدد) على أي حال فان التقنية تتركز بين الأقراص المدمجة CD وبين مشغلات الأقراص DVD حيث إن الموزع الرئيسي القابلية للأقراص يضع علامة مائية حول القرص كان تكون text معين ومشغل الأقراص تكون له على قراءة النص text بحيث يتعرف على النسخ الأصلي للأقراص من النسخ الغيرأصلي وبالتالي فانه يمنع أي عملية استنساخ غير مخول ممكن إن تحدث بإظهار رسالة معينة أو غيرها أو ممكن يبرمج مشغل الأقراص بحيث يقوم بعملية النسخ لثلاث مرات وبعدها يمنع الاستنساخ[7].

3. بصمة الإصبع لتتبع اثر المهاجم Fingerprinting for traitor tracking :

إن الهدف من هذا التطبيق هو نقل معلومات حول المستلم الشرعي أي أنها تتضمن عملية تعشق أو تتداخل معلومات خاصة عن المستلم الشرعي مع العلامة المائية أي أن المستلم يترك بصمة داخل العلامة المائية وفي كلتا النسختين (النسخة الموجودة في الموزع الأصلي والنسخة الموجودة مع المستلم) وذلك لإثبات المالك في حالة التعرض لعملية النسخ الغير مشروع على سبيل المثال استخدامها في شبكة الاتصالات العالمية Word wide Web (WWW) حيث إن الشبكة تبحث عن سراق صور العلامة المائية وان هذا التطبيق أيضا يتطلب قوة عالية مقابل معالجة اعتيادية للبيانات حيث إن عملية الاسترداد تتم بفصل العلامة المائية عن المعلومات الشخصية[3] .

4.التخويل authentication :

تستخدم هذه التقنية مع العلامة المائية الضعيفة وتستخدم بصورة رئيسية في عملية الإرسال حيث إن العلامة المائية تكون بمثابة الإشارة لعملية الإرسال الصحيح والتأكد من وصول نفس النسخة الأصلية . على سبيل المثال صورة تحتوي علامة مائية يتم إرسالها مع الخوارزمية التي تم بناء العلامة المائية على أساسها . إما المستلم فانه يقوم بتطبيق خوارزمية معاكسة لخوارزمية البناء فإذا تمكن من استخراج العلامة المائية فهذا يعني إن عملية الإرسال تمت بصورة صحيحة ولم تتعرض لأي هجوم وإلا فانه يتم إعادة إرسالها من جديد .

5. العنونة labeling :-

الرسالة المخفية التي يمكن إن تحتوي على علامات التي تسمح لإضافة أطارت إلى الصورة أو الصوت ، وهذا مفيد بشكل خاص في التطبيقات الطبية حيث تمنع هذه الطريقة الأخطاء الخطرة [7].

6.مراقبة الإذاعة والإعلام Broadcast and publication Monitoring :

يستخدم هذا التطبيق بصورة خاصة في إل TV Channel وال Radio Channel حيث يتم وضع علامة مائية لكل قناة أو إذاعة وبما انه توجد هنالك مراقبة على البث يتم منع أي تلاعب أو محاولة سرقة بث قناة من قناة أخرى[7]

7.يمكن إن تعمل مع الوسائط المتعددة multimedia[6]

العلامة المائية الرقمية تعمل مع الصور بشكل جيد لأنها تحتوي على الكثير من التفصيلات الدقيقة التي يمكن إن تخفي فيه علامة مائية . أجهزة إعلام الفيديو والتسجيل الصوتي مرشحين متازين أيضا. للعلامة المائية الرقمية ضوضاء خلفية كافية دائما موجودة في الملفات السمعية. وغير مسموعة إلى الإذن البشرية ، وكذلك الفيديو فهو عبارة عن سلسلة من الصور الثابتة .

7-2 مقاييس تقييم الأداء [5]

هناك العديد من المقاييس المستخدمة لتقييم تقنيات وضع العلامات المائية على الفيديو ولكن في طريقة النظام المقترحة سنستخدم نسبة الذروة للإشارة إلى الضوضاء (PSNR) وارتباط التطبيع (NC).

1- نسبة الإشارة إلى الضوضاء (PSNR): يقيس هذا المقياس دقة الطريقة. يقوم بالمقارنة بين الغلاف الأصلي والإطار الذي يحمل العلامة المائية للتحقق مما إذا كانت العلامة المائية قد تم إتلاف الغلاف الأصلي أم لا.

$$\mathbf{PSNR} = \mathbf{10log_{10}}[\frac{\mathbf{(IMAX)^2}}{\mathbf{MSC}}] \qquad \mathbf{(2.1)}$$

حيث هو الحد الأقصى للمستوى الرمادي لكل إطار (Imax=255)، MSC هو متوسط مربع الخطأ ويمكن وصفه بالمعادلة التالية.

$$\boldsymbol{MSC} = \frac{\mathbf{1}}{\boldsymbol{mn}} \sum_{\boldsymbol{i=0}}^{\boldsymbol{m-1}} \sum_{\boldsymbol{j=0}}^{\boldsymbol{n-1}} (\boldsymbol{p1(i.j) - p2(i.j)})^{\mathbf{2}} \qquad \mathbf{(2.2)}$$

حيث p1 (i, j) , p2 (i, j) تمثل الإطارين، m, n تمثل أبعاد الإطارين. يجب أن تحتوي خوارزمية التضمين الجيدة على نسبة PSNR أكبر من 30%.

2-الارتباط التطبيعي (NC): يقيس هذا المقياس درجة قوة الطريقة. إنه يقارن بين علامتين مائيتين للتحقق من كيفية تحمل العلامة المائية للهجمات وللتحقق من الارتباط بينهما كما هو موضح في المعادلة (2.3).

$$\mathrm{NC} = \frac{\sum_{i=1}^{M} W_i W_{i'}}{\sqrt{\sum_{i=1}^{M} W_i{}^2} \sqrt{\sum_{i=1}^{M} W_{i'}{}^2}} \qquad \textbf{(2.3)}$$

حيث w هي العلامة المائية الأصلية و wهي العلامة المائية المستخرجة. قيمة NC بين 0 و 1.

الفصل الثالث

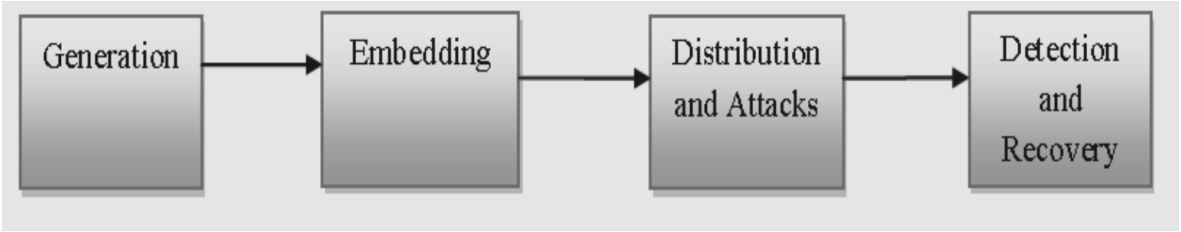
نظام العلامة المائية الرقمية

1-3 المقدمة

بات واضحا وفي ظل التطور التكنولوجي السريع والتحول الرقمي الذي يشهده عصرنا الحالي، أصبحت العلامة المائية وتضمين البت الأقل أهمية لا يمكن إغفالها. تعتبر العلامة المائية أحد الآليات الرئيسية التي تحمي الملكية الفكرية وغير من التطبيقات ذات الصلة وبالتالي فهي تضمن سلامة المحتوى الرقمي، ومع ذلك، فإن تضمين البت الأقل يشكل تحدياً مستمراً لأنظمة حماية الملكية الفكرية والأمان السيبراني. في هذا البحث، سنقوم بتحليل أهمية العلامة المائية وتأثير تضمين البت الأقل على فعاليتها، مع التركيز على كيفية مواجهة التحديات التي تطرأ عند استخدام هذه التقنيات والسبل الممكنة لتحسينها.،علما ان تم تنفيذ هذا العمل من خلال ماتلاب(MATLAB).

2-3 الهيكل العام للنموذج الاساسي للمشروع المقترح

يتألف النموذج الأساسي للعلامة المائية المقترح من أربع مراحل رئيسية كما هو مبين في الشكل (3-1) أدناه ، وبحسب الوظائف المبينة لكل مرحلة:



الشكل(3-1) النموذج الاساسي للمشروع المقترح

1- توليد العلامة المائية (Watermark Generation):

تعد عملية توليد العلامة المائية عملية حيوية في حماية المحتوى الرقمي وتحديد هويته ، اذ يتم توليد العلامة المائية عادةً عن طريق تضمين بيانات مميزة في الملف الرقمي، وقد تكون هذه البيانات مرئية أو غير مرئية للمستخدمين العاديين، وتختلف طرق توليد العلامات المائية باختلاف نوع الوسيط الرقمي ومتطلبات الحماية المطلوبة. في مشروعنا المقترح يتم استخدام صورة ملونة كعلامة مائية.

2- تضمين العلامة المائية (Embedding Process)

تضمين العلامة المائية هو عملية أساسية في حماية المحتوى الرقمي وتأمين حقوق الملكية الفكرية. يستخدم هذا الإجراء لتعزيز الأمان والثقة في الوثائق والصور الرقمي. في هذه المرحلة ، يتم تضمين العلامة المائية في وسائط التغطية (Cover)، الذي هو عبارة عن صورة ملونة ايضا يتم اختيارها من بين مجموعة مكبيرة من الصورة المتاحة، علما ان عملية التضمين ترتبط ارتباطا مباشراً بخوارزمية الاستخراج التي تُعتمد في الطرف الاخر(طرف المستلم)، وبالتالي فإن خوارزمية التضمين هي عبارة عن مزيج من العلامة المائية مع الوسائط المختارة ، وبالتالي فإن نتيجة هذه العملية يمكن التعبير عنها بصياغية رياضية وكما يلي:

$$WM= E (CI, WI)$$

حيث ان:

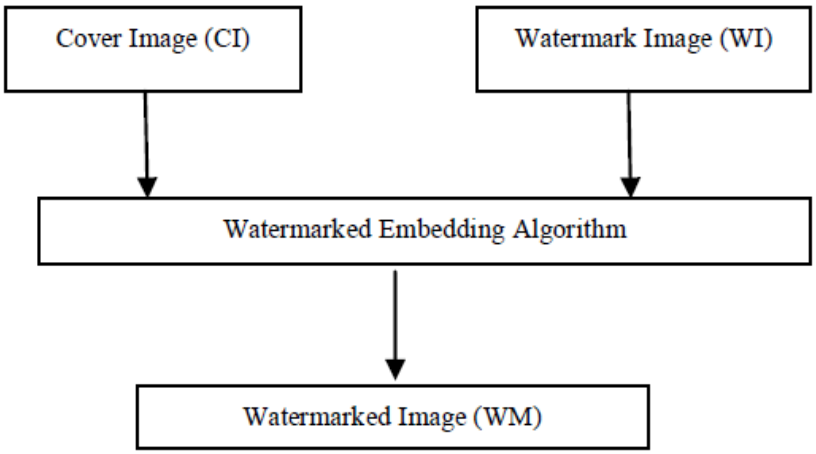
CI :هي الصورة الاصلية .

WI : هي العلامة المائية.

E :هي خوارزمية التضمين.

WM: الوسائط المتضمنة للعلامة المائية (**Watermarked Image**

كذلك يمكن النظر الى عملية اضافة العلامة المائية كم مبين في الشكل (3-2)، كذلك بالامكان التعبير عن عمل عملية التضمين كما في الخوارزمية (3-1) ادناه، اذ يتم تحويل كل من صورة الغلاف وصورة العلامة المائية الى مصفوفة احادية لبكسلات تلك الصورة، اي ان كل موقع فيها يمثل بكسل وكما موضخ :



الشكل(3-2) عملية تضمين العلامة المائية (Embedding Process)

Algorithm (3-1): Watermark Embedded Algorithm

Start

Input: Watermark Image Vector (Wi), Cover Image Vector (Cj), n:No.of Bits, index_array

Output: Watermarked Image (WM)

Process:

k=0 // k: index of index_array

For each pixel (i) in Wi Do

For each pixel (j) in C Do

If n_MSB of pixel (i) = n_LSB Y then

Index_array [i]= j

k=k+1

End IF

End For

End For

End

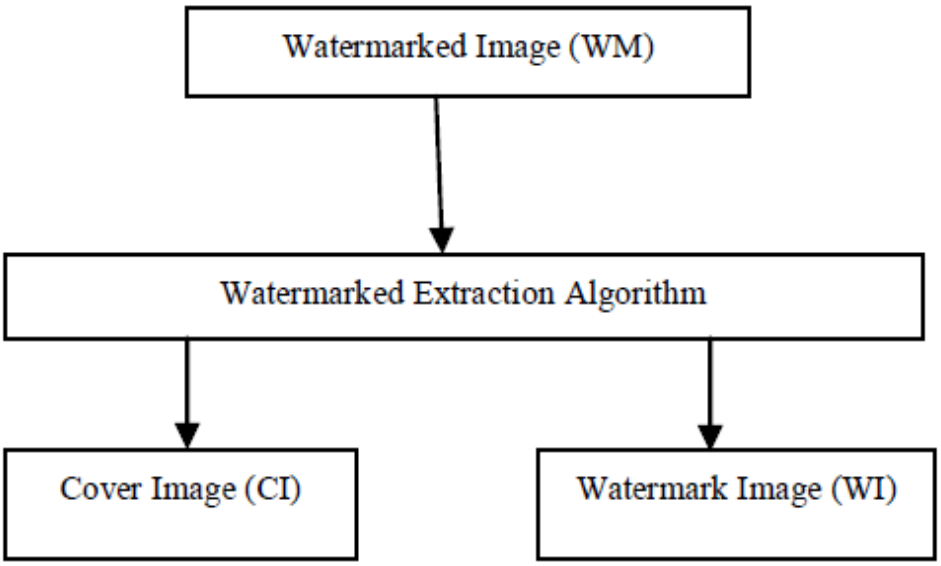
3- التوزيع/(الهجوم على) العلامة المائية (Distribution/Attacks)

يمكن اعتبار عملية التوزيع بمثابة نقل للإشارة عبر قناة العلامة المائية. وقد تكون الهجمات المحتملة في قناة البث متعمدة أو غير مقصودة، وكما لاحظنا فانه ليس هناك عملية تضمين بالمعنى الحقيقي او الفيزياوي وانما يتم البحث عن قيمة بتات العلامة المائية (n_MSB) في بكسلات صورة الغطاء (تحديدا في البتات الاقل اهمية n_LSB) لبكسلات، وبالتالي حينما يتحقق الشرط (نجد البتات المشابهة) تقوم الخواررزمية المقترحة بخزن موقع وجودها (رقم البكسل) لصورة الغلاف الذي وجد بها قيمة الـ n_MSB لصورة العلامة المائية في مصفوفة خاصة سميت بالـ index_array والتي سيتم ارسالها الى الطرف الثاني بشكل منفصل ليتم اعتمادها في استرجاع الملامح المهة (n_MSB's) لصورة العامة المائية وبالتالي تحقيق غاية تلك التقنية.

4- الكشف والاسترجاع (Detection and Recovery)

تسمح عملية الكشف بتحديد هوية المالك وبالتالي تحقيق الهدف الذي من أجله تم استخدام تقنية العلامة المائية، وتوفر المعلومات للمستلمين المقصودين. الشكل (3-3) يوضح عملية الاسترجاع التقليدي بشكل عام، وخوارزمية (3-2) توضح عملية استرجاع العلامة المائية بالاعتماد على مصفوفة المواقع (inde)وبالتالي تحقيق المطلوب منها.

بالامكان التعبير عن عمل عملية الاسترجاع كما في الخوارزمية (3-2) ادناه، اذ يتم اعتماد مصفوفة المواع المشار اليها اعلاه في تكوين او بناء العلامة المائية وكما مبين في الخوارزمية.



الشكل(3-3) عملية استخراج العلامة المائية (Extraction Process)

Algorithm (3-2): Extraction Algorithm

Start

Input: Watermarked Image (WM), index_array [k] , Cover Image Vector (Cj)

Output: Extracted Watermarked Image (WM')

Process:

WM'=empty

k=0 // k: index of index_array

For k=1 to end of index_array Do

Get x=n_LSB of pixel (k) in Cj

WM'= WM'+x

End For

Rebuild WM' image

If WM' = WM then

"Verified"

Else

Not Verified

End if

End

3-3 المقاييس المستخدمة لقياس كفاءة النظام

لابد من الاشارة هنا الى ان مربع الخطأ (Mean Square Error) ونسبة الضوضاء (peak signal-to-noise ratio) هما مقاييس مهمة في تقييم جودة العلامة المائية. إليك شرح مختصر لكل منهما:

1. مربع الخطأ (MSE):

- يقيس مربع الخطأ الفرق بين القيم الفعلية للعلامة المائية والقيم المتوقعة.
- يحسب عن طريق تقدير متوسط مربع الفرق بين قيم العلامة المائية الأصلية والقيم المتوقعة (عادةً باستخدام خوارزميات الاسترجاع أو التعويض).

2. نسبة الضوضاء (PSNR):

- تقيس نسبة الضوضاء الفعالة إلى إشارة العلامة المائية.
- تُعبر عن قوة الإشارة مقارنة بمستوى الضوضاء في العلامة المائية، حيث يفضل أن تكون نسبة الإشارة إلى الضوضاء عالية لضمان جودة عالية للعلامة المائية.

تستخدم هذه المقاييس لتحسين وتقييم أداء تقنيات العلامات المائية، حيث يهدف الباحثون إلى تحسين MSE وزيادة PSNR للحصول على علامات مائية ذات جودة عالية ومقاومة للتلاعب والضوضاء.والآخر هو نسخة مشوهة من جودته التي يجري تقييمها ، ثم يمكن أيضا اعتبار MSE قياس جودة الإشارة.

افترض أن

$$x = \{ x_i \mid i = 1, 2, \cdots, N\}$$

$$y = \{ y_i \mid i = 1, 2, \cdots, N\}$$

حيث ان x,y هما طولان محددان ، منفصلان الإشارات (مثل الصور المرئية) ، حيث N هو عدد عينات الإشارة (بكسل ، إذا كانت الإشارات صور) و xi و yi هي قيم عينات i في x و y ، على التوالي. MSE بين الإشارات x ، y

$$MSE(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2$$

في MSE ، سنشير في كثير من الأحيان إلى إشارة الخطأ ei = xi - yi وهو الفرق بين الأصل و إشارات مشوهة. إذا كانت إحدى الإشارات هي الإشارة الأصلية للجودة مقبولة (أو perhaps pristine) ، و الآخر هو نسخة مشوهة من جودتها التي يجري تقييمها ، ثم يمكن أيضا اعتبار MSE قياس جودة الإشارة. غالباً ما يتم تحويل MSE إلى مقياس نسبة الإشارة إلى الضوضاء (PSNR) من الذروة إلى الذروة(peak-to-peak signal-to-noise ratio)

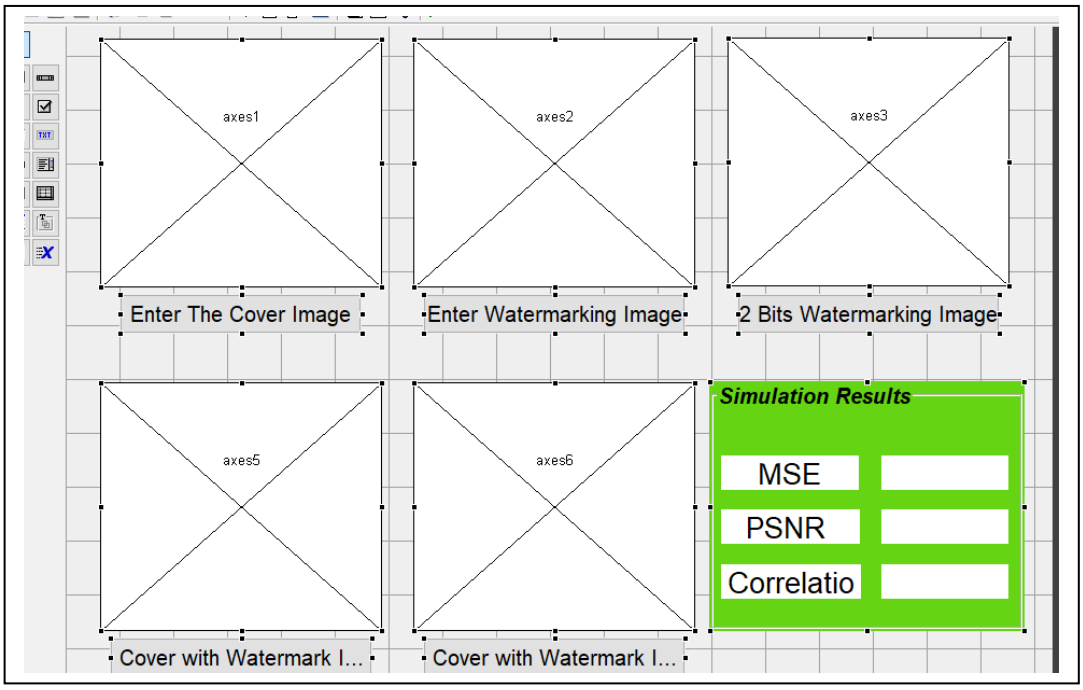
$$PSNR = 10\log_{10}\frac{L^2}{MSE}$$

حيث L هو النطاق الديناميكي لشدة البكسل المسموح بها للصورة. على سبيل المثال ، الصور التي لديها تخصيصات 8 بت / بيكسل بمقياس رمادي ، $L = 2^8 - 1 = 255$ تكون مفيد إذا كانت الصور مختلفة تتم مقارنة النطاقات الديناميكية لها ، ولكنها لا تحتوي على أي معلومات جديدة تتعلق بالمشاريع الصغيرة والمتوسطة

4-3 توثيق تنفيذ النظام المقترح

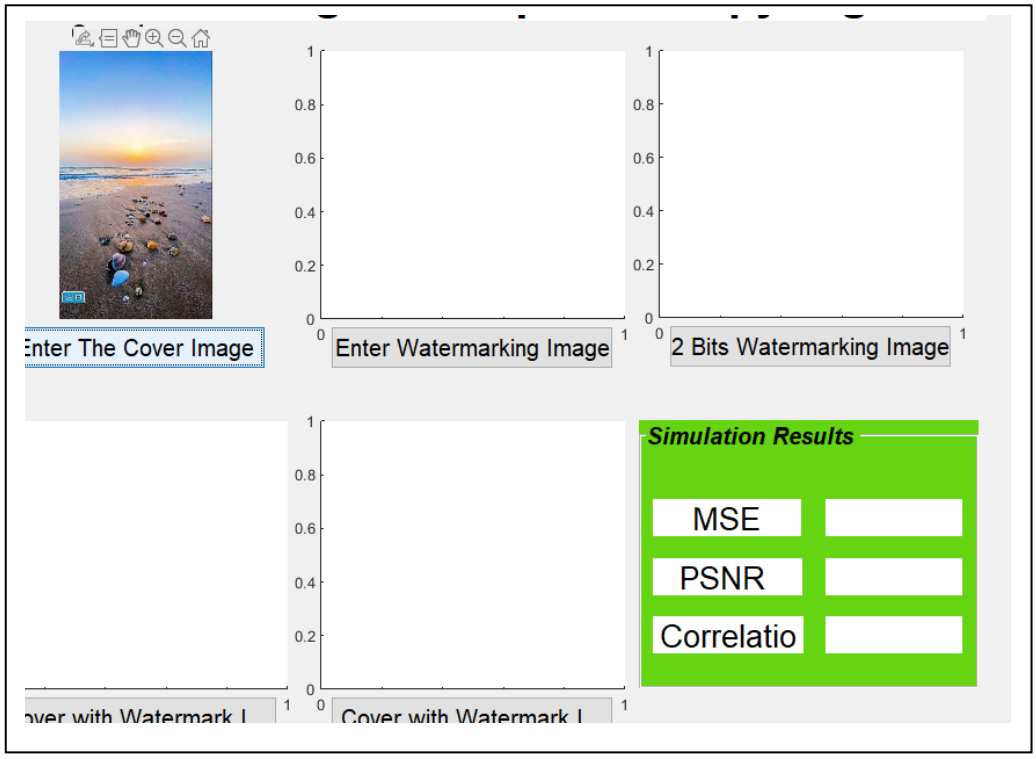
في هذا المقطع، سنستعرض البرنامج العملي الذي صمم باستخدام الماتلاب لتنفيذ المشروع المقترح.عند البدء بالتنفيذ ستظهر الواجهة التالية:

1.الواجهة الرئيسية للمشروع:



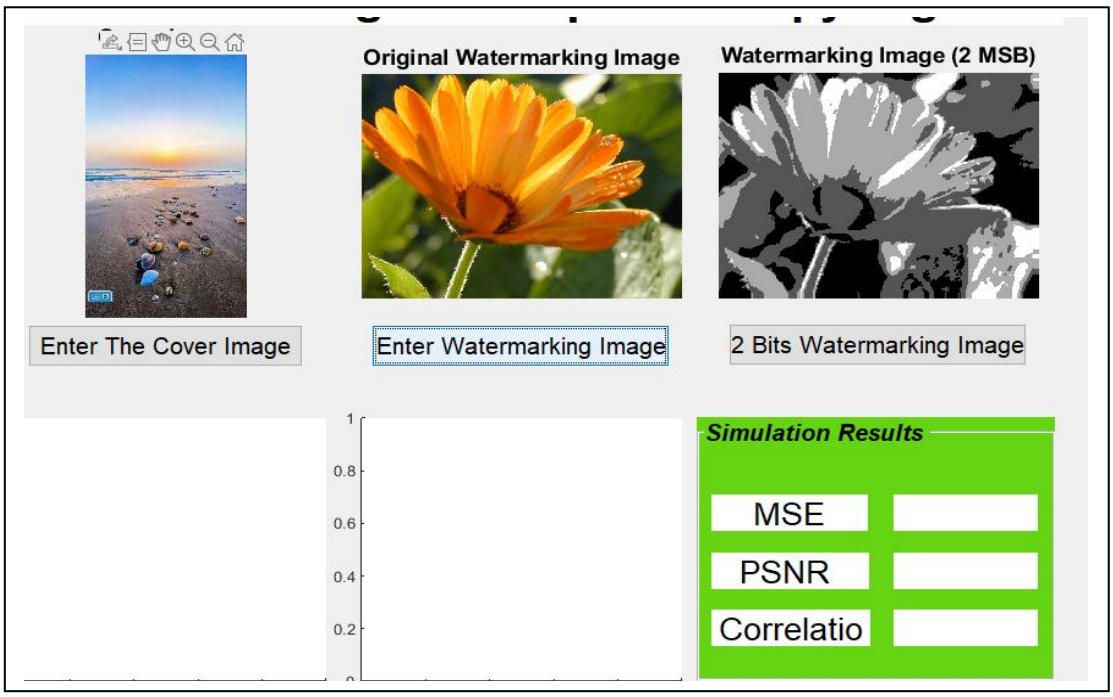
الشكل(3-4) الواجهة الرئيسية للمشروع

2- بحسب واجهة المشروع اعلاه(الشكل 3-4)، بالامكان اختيار صورة الغطاء(Cover image) عند الضغط على الخيار المعنى، اذ ستظهر لك واجهة لاختيار صورة الغطاء ،بعد اختيارها تكون واجهة المشروع كما يلي:



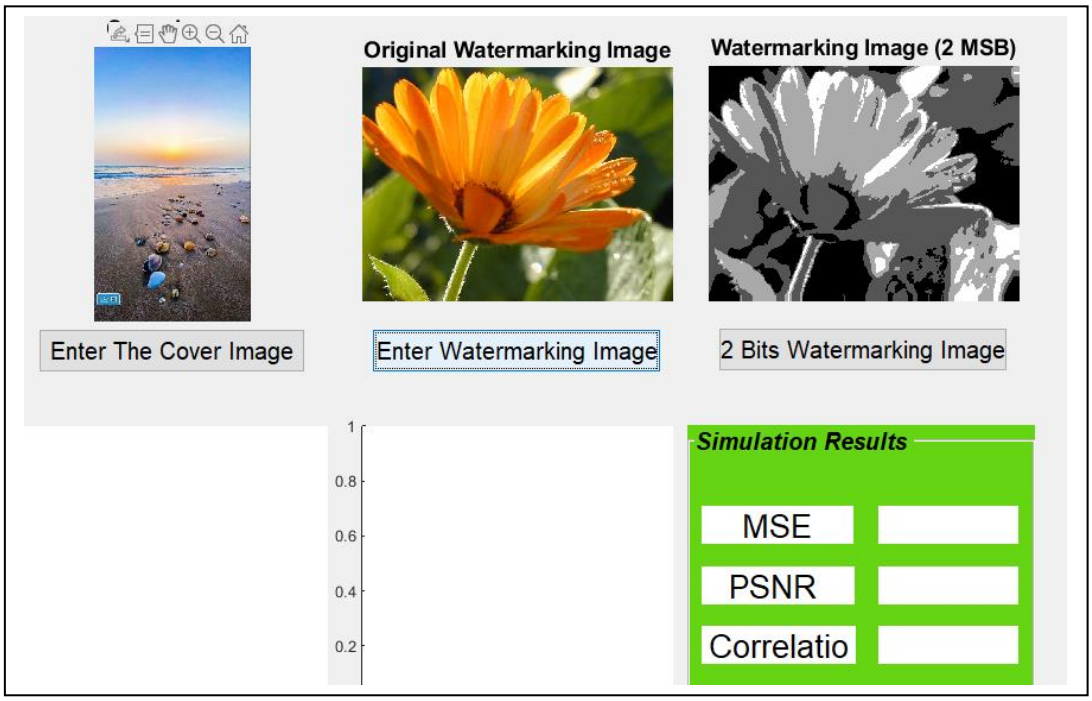
الشكل(3-5) اختيار صور الغطاء(Cover Image)

3- بالامكان اختيار صورة العلامة المائية من خلال ضغط الخيار المخصص لذلك كما يظهر في الواجهة الرئيسية(الشكل 3-4). اذ ستظهر لك واجهة لاختيار صورة العلامة ،بعد اختيارها تكون واجهة المشروع كما يلي:



الشكل(3-6) اختيار صور العلامة المائية(Watermark Image)

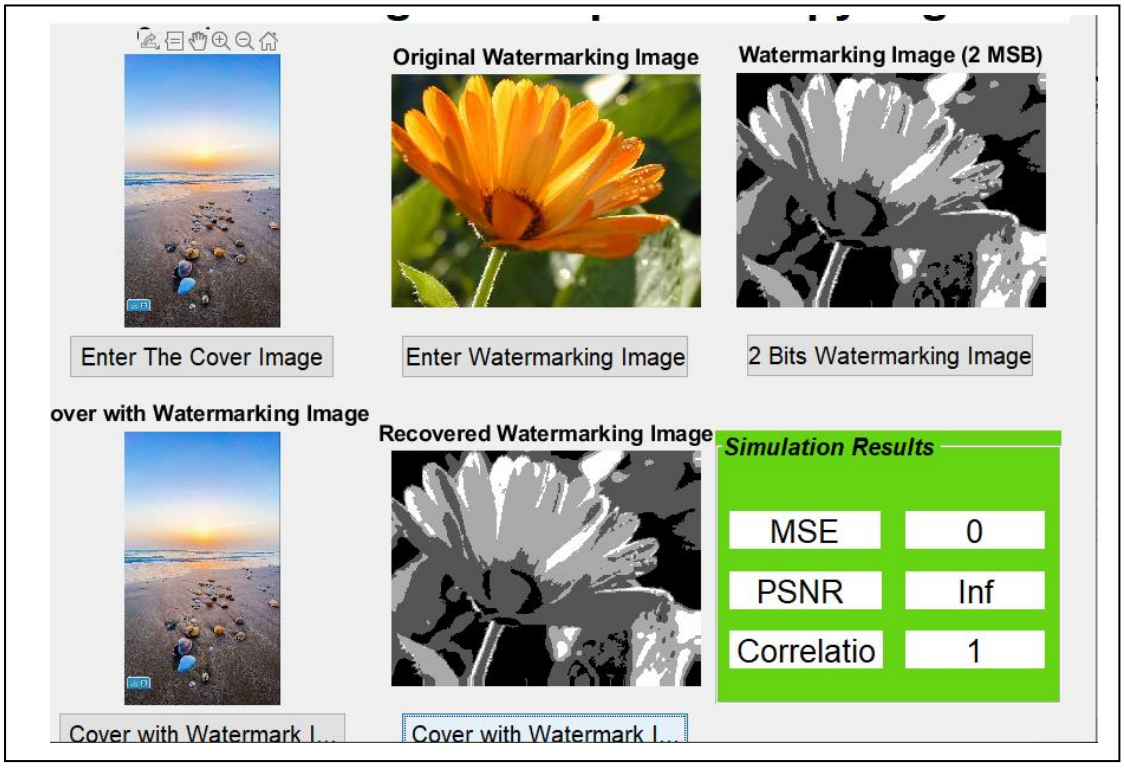
4-بعد ان تم ادخال كافة متطلبات النظام (صورة الغلاف،صورة العلامة المائية، عدد البتات n) ،بالامكان الان اجراء عملية تضمين العلامة المائية الرقمية (Embedding Process) من خلال اختيار الزر الظاهر في الواجهة الرئيسية



الشكل(3-7) ناتج عملية تضمين العلامة المائية(Embedding Watermark Process)

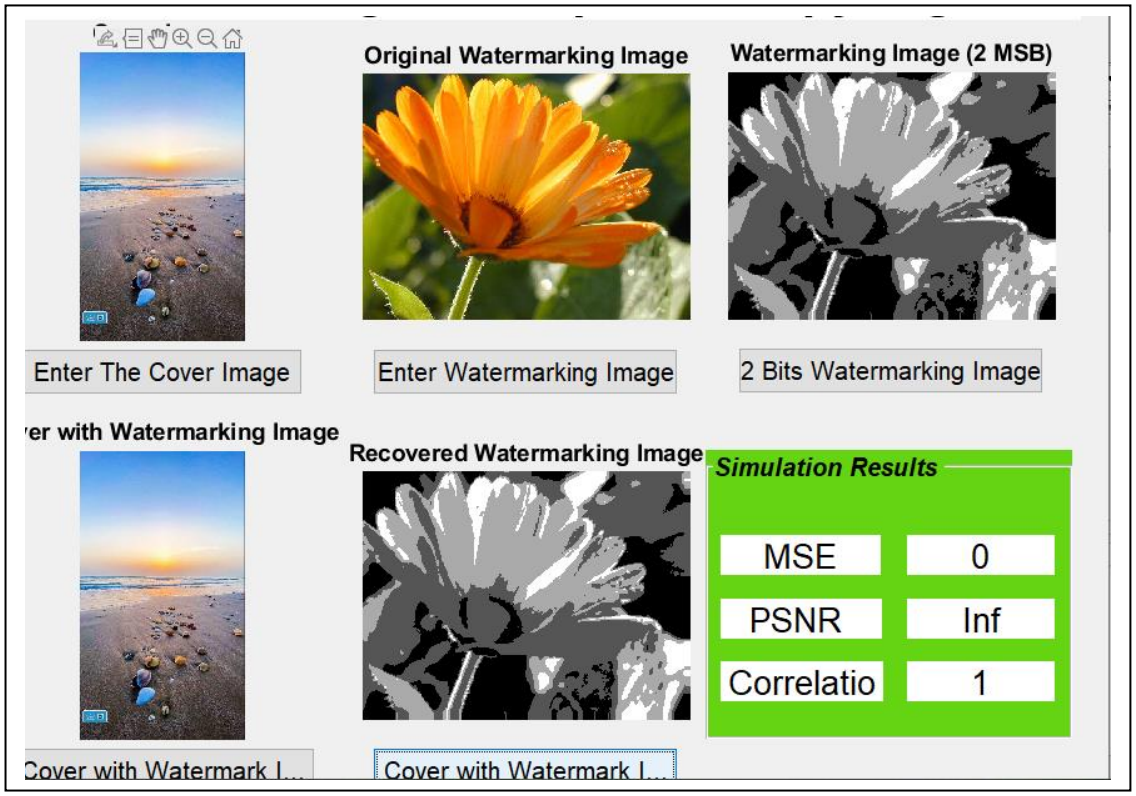
المعني بهذه العملية، وبالتالي ستظهر لنا نتيجة هذا الاجراء كما مبين في الشكل (3-7) ادناه.

5- بالامكان استرجاع صورة العلامة المائية الرقمية التي تم تضمينها في صورة الغلاف (مع حدوث بعض الضياع الذي يتناسب مع عدد البتات النتي تم اعتمادها كبتات اقل اهمية في صورة الغلاف والتي هي ايضا عدد البتات الاكثر اهمية في صورة العلامية المائية). لاحظ الشكل ادناه(الشكل 3-8)



الشكل(3-8) ناتج عملية استرجاع العلامة المائية(Extracting Watermark Process)

7-واخيرا ،توجد امكانية احتساب المعيارين(PSNR , MSE) مع كل عملية تضمين واسترجاع وبحسب قيمة المتغير (n) . لاحظ الشكل (3-9).



الشكل(3-9) يوضح احتساب قيمتي الـــ PSNR ,MSE

الفصل الرابع

الاستنتاجات والتوصيات

1-5 الاستنتاجات

هناك عدة استنتاجات ممكن ادرجاتها كما يلي:

1. ان تضمين العلامة المائية يعتبر إجراءً فعّالاً لحماية المحتوى الرقمي من الاستخدام غير المصرح به وتقليل فرص القرصنة الرقمية. كما أنه يسهل تتبع الملكية الفكرية وتحديد مصدر الأصل، مما يعزز الثقة في الأعمال الفنية والوثائق. ومع ذلك، يجب مراعاة التوازن بين حماية المحتوى والحفاظ على جودته وسهولة استخدامه، وتحديد السياسات والتقنيات المناسبة لتضمين العلامة المائية دون التأثير السلبي على تجربة المستخدم.
2. إن العدد المتزايد من البيانات الرقمية القابلة للتبادل عبر وسائل الاتصالات الحديثة يوّلد حاجات ملحة و جديدة من أجل حمايتها، كما ان وثائق الوسائط المتعددة وتحديدا الصور هي اكثر المتأثرين بذلك.
3. يتوقع المستخدمون لهذا النوع من التقنيات أن الحلول القوية ستضمن حماية حقوق النشر وتضمن أيضًا صحة مستندات الوسائط المتعددة.
4. الطريقة المقترحة حققت اختيارا عشوائيا بالاضافة الى سلامة الوسط الناقل (cover) نظرا للمبدأ الذي تعتمد عليه (مبدأ الهوموفونك المقترح).

2-5 التوصيات

بالامكان اقتراح عدة توصيات منها:

1- تطوير نظام مقترح يعمل على كافة انواع الوسائط المتعددة سواء كانت نص، صورة، صوت او فيديو.
2- استكشاف وتطوير تقنيات جديدة لتضمين العلامات المائية في الصور والفيديوهات والملفات الرقمية الأخرى بطرق تجعلها صعبة التلاعب بها.

3- تحليل ودراسة تأثير تضمين العلامات المائية على جودة الصورة أو الفيديو ومقارنتها مع الصور أو الفيديوهات التي لا تحتوي على علامات مائية.

4- استكشاف التقنيات المتقدمة للكشف عن العلامات المائية وتحليلها بشكل رقمي للكشف عن التلاعب بها أو إزالتها تطبيقات تضمين العلامات المائية في مجالات مختلفة: دراسة استخدامات تضمين العلامات المائية في مجالات مختلفة مثل حقوق الطبع والنشر، والأمان السيبراني، وتتبع السلع المزيفة، والتوقيع الرقمي..

5- دراسة مدى فعالية وأمان التقنيات الحالية المستخدمة في تضمين العلامات المائية واقتراح تحسينات أو تطويرات مستقبلية.

المصادر

المصادر

[1]. Received 28 August 2023, accepted 21 September 2023, date of publication 27 September 2023, date of current version 3 October 2023.Digital Object Identifier 10.1109/ACCESS.2023.3319669

[2]. Imran, N., Hameed, S., Hafeez, Z., Faheem, Z., Waseem, M., Latif, U., & Amin, M. S. (2021, December). Image Watermarking Approach Using LSB and Laplacian Filter. In Journal of Physics: Conference Series (Vol. 2129, No. 1, p. 012015). IOP Publishing.

[3] Rakhra, M., Kumar, R., & Walia, H. (2021, September). A Review on Data hiding using Steganography and Cryptography. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1-4). IEEE.

[4] Janu, N., Kumar, A., Dadheech, P., Sharma, G., Kumar, A., & Raja, L. (2021, April). Multiple watermarking scheme for video & image for authentication & copyright protection. In IOP Conference Series: Materials Science and Engineering (Vol. 1131, No. 1, p. 012020). IOP Publishing.

[5] Yadav, U., Sharma, J. P., Sharma, D., & Sharma, P. K. (2014). Different watermarking techniques & its applications: a review. International Journal of Scientific & Engineering Research, 5(4), 1288-1294.

[6] Thampi, S. M. (2008). Information hiding techniques: a tutorial review. arXiv preprint arXiv:0802.3746.

[7] Kulkarni, G., & Kuri, S. (2017, December). Robust digital image watermarking using DWT, DCT and probabilistic neural network. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1-5). IEEE.

[8] CV, L. P., & NR, N. R. (2017, April). Digital watermarking scheme for image authentication. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 2026-2030). IEEE.

[9] Ahmaderaghi, B., Kurugollu, F., Del Rincon, J. M., & Bouridane, A. (2018). Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. IEEE Transactions on Computational Imaging, 4(1), 46-59.

[10] Liu, S., Pan, Z., & Song, H. (2017). Digital image watermarking method based on DCT and fractal encoding. IET image processing, 11(10), 815-821.

[11] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., & Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. IEEE access, 6, 10269-10278.