مجلة العلوم الإنسانية لجامعة أم البواقي
ISSN 1112-9255/E-ISSN 2588-2414
المجلد10 العدد01 – جوان 2023

OEB Univ. Publish. Co.

الستيغانوغرافي وحماية الملكية الفكرية في العصر الرقمي

Steganography and intellectual property protection in the digital age

حمزة معمري*

[1] جامعة الجزائر2 أبو القاسم سعد الله، hamza.mammeri@univ-alger2.dz

تاريخ التسليم:15-1-2023 تاريخ التقييم: 3-2-2023تاريخ القبول:25-4-2023

الملخص

استخدم البشر منذ القدم شتى أنواع وسبل حماية ممتلكاتهم الجامدة والمنقولة، وانتشرت بذلك عملية إخفاء أو التسري في نشر بعض الرسائل والحوارات لأغراض متعددة، سلمية أحيانا وعسكرية حربية في غالبيتها، فتعددت الطرق والوسائل وحتى الوسائط، غير أنها تميزت ببساطتها، فمن استخدام الرسائل المشفرة عبر الحمام الزاجل، إلى الوشم على رؤوس العبيد، ثم الكتابة المشفرة في الحربين العالميتن 1 و2 .

غير أن ظهور التكنولوجيات الحديثة و وسائل الاتصال المتطورة ساعد في الانتشار المذهل وغير المسبوق للملفات والرسائل الالكترونية اختصارا للوقت والجهد والمسافات، وعجزت الترسانة القانونية المستحدثة لحماية الممتلكات الفكرية بكل أنواعها ووسائطها (نصية، مرئية، صوتية...) بل أخذت منعرجا خطيرا وكبيرا لم تشهده البشرية من قبل بفعل العجز عن مواكبة هذه التيارات الوافدة من المعلومات المتعددة ومراقبتها ، غير أن اختراع تقنية التخفي أو إخفاء المعلومات (STEGANOGRAPHY) كحل لتشفير أو إخفاء بعض المعلومات الرقمية بتقنية عالية ومن خلال ذلك حماية الملكية الفكرية في الوسط الرقمي الذي لم يعد بالإمكان تداركه بالوسائل التقليدية والقانونية فقط أعطى بصيصا من الأمل في تدارك ما لم يتمكن من تداركه.

الكلمات المفتاحية: إخفاء المعلومات، التشفير الرقمي، الملكية الفكرية، الستيغانوغرافي، العصر الرقمي.

Abstract

Since ancient times, humans have used various types and means to protect their inanimate and movable property, and thus the process of concealment or secrecy has spread in the dissemination of some messages and dialogues for various purposes, sometimes peaceful and military in most of them. The carrier, to tattoos on the heads of slaves, and then the encrypted writing in World Wars 1 and 2.

However, the emergence of modern technologies and advanced means of communication helped in the astonishing and unprecedented spread of files and electronic messages in shortening the time, effort and distances, and the newly developed legal arsenal was unable to protect intellectual property of all kinds and media (text, visual, audio...) but took a dangerous and big turn that it did not witness However, the invention of stealth technology (STEGANOGRAPHY) as a solution to encrypt or hide some digital information with high technology and through that protect intellectual property in the digital medium, which can no longer be remedied by means. Conventional and legal only.

.

Keywords : hiding information, Digital Encryption, Intellectual Property,

Steganography**.**

***المؤلف المرسل:** حمزة معمري، **الإيميل:** hamza.mammeri@univ-alger2.dz

1.مقدمة:

رغم الاستخدام الواسع لعملية التشفير من طرف عديد الدول والمجتمعات والجيوش قديما وحديثا، إلا أن الغاية القصوى والوحيدة من هذه التقنية القديمة – إن صح التعبير – كان منحصرا في التغلب على الخصم وكيفية اختراق صفوفه وإضعافه، وهو ما تغير حاليا بتغير المعطيات والذهنيات والمجتمعات، وسيطرت التقنية وتحول التواصل بين الأفراد معتمدا في أساسه على شبكة الانترنت التي أضعفت إلى حد كبير جدا استخدام الوسائط الورقية الذي بات منحصرا في مجالات جد خاصة.

وهو ما طرح تساؤلات جمة فيما يخص الحفاظ على الخصوصية الشخصية وحقوق المؤلف والحقوق المجاورة في هذا الفضاء الرقمي.

واندرجت أسئلة البحث حول السؤال الرئيسي التالي:

كيف يمكن استغلال التكنولوجيات الحديثة للنشر الرقمي في حماية الملكية الفكرية باستخدام تقنية الستيغانوغرافي، وكذا حماية الممتلكات الرقمية لمراكز البحث وأنظمة المعلومات.

1.1 **الإشكالية وتساؤلات الدراسة الفرعية:** في ظل تزايد النداءات العالمية الموجهة لحماية الملكية الفكرية في ضوء تنامي ظاهرة الانتشار السريع و المتنامي لنشر الأعمال في شتى الوسائط (نصية، صوتية وعلى شكل صور وفيديو) عبر الفضاء الرقمي، ظهرت تقنية الستيغانوغرافي كمنفذ لحصر ومراقبة هذه الظاهرة التي عجزت الترسانة القانونية عن وضع حد لها ومراقبتها باستخدام الطرق التقليدية التي لم تعد تجدي نفعا.

–فهل يمكن أن تكون تقنية الستيغانوغرافي حلا ومخرجا لما آلت إليه وضعية حماية الملكية الفكرية عبر الفضاء الرقمي؟

للإجابة على إشكالية الدراسة تم طرح مجموعة من الأسئلة الفرعية تمثلت في:

- هل هناك مخاطر على نقل المعلومة في الفضاء الرقمي؟
- هل هناك من سبل وطرق للوقاية والحد من الاستخدام السلبي للنشر الإلكتروني؟
- كيف يمكن تطوير تقنية الأمن المعلوماتي في الحفاظ على سرية وأمن المعلومات.

2.1 فرضيات الدراسة:

للإجابة على الإشكالية العامة للدراسة فقد تم وضع الفرضية التالية :

–يمكن أن يكون لتقنية الستيغانوغرافي دورا مهما في تطوير مجال الملكية الفكرية عبر الفضاء الرقمي.

وقد انبثقت عن هذه الفرضية الرئيسية الفرضيات الفرعية التالية:

1- تعدد وتطور مخاطر نقل المعلومة في الفضاء الرقمي بما لا يمكن حصره .

2- تعدد الجهود الدولية للحد من هذه المخاطر المتعلقة بالاستخدام السلبي للنشر الإلكتروني

3- تنامي سبل الوقاية وحماية الملكية الفكرية والأمن المعلوماتي عبر الفضاء الرقمي باستخدام تقنية الستيغانوغرافي.

3.1 أهمية الدراسة:

تكتسي الدراسة أهمية كبيرة من خلال تسليطها الضوء على أهم ما يؤرق أخصائي أمن المعلومات والنشر الإلكتروني في الفضاء الرقمي، والذي أبان عن مخاطر جمة لم تستطع الترسانة القانونية ولا الوسائل التقليدية من الحد منها ومراقبتها، فكان في تقنية الستيغانوغرافي الحل الوحيد والمخرج الأوحد للحد من تنامي هذه الظاهرة باستخدامها أساليب قديمة في استعمالها حديثة في تقنياتها.

4.1 أهداف الدراسة:

تهدف هذه الدراسة لتسليط الضوء على جملة من الأهداف وهي:

- تسليط الضوء على تنامي ظاهرة اختراق حقوق الملكية الفكرية عبر الفضاء الرقمي.
- معرفة التقنيات المستخدمة للحد من الاستخدام السلبي لتقنية النشر الإلكتروني.
- التعريف بتقنية الستيغانوغرافي ومجالات استخدامها في الأمن المعلوماتي وحماية الملكية الفكرية في الفضاء الرقمي.

5.1 منهج الدراسة:

تم استخدام المنهج الوصفي في هذه الدراسة حيث تسعى لوصف الوسائل والتقنيات المستخدمة قديما وحديثا في نشر المعلومة وبثها وكيف انحرفت بعد ذلك بعض الطرق لتأخذ منعرجا خطيرا بات يهدد الأمن المعلوماتي والنشر الإلكتروني.

2. التشفير :

2.1 التشفير أو إخفاء المعلومات (Cryptography):

عُرف التشفير أو إخفاء المعلومات منذ القدم، إذ لم يتوانى الفراعنة القدماء في استخدامه وكذلك اليونان والإغريق والصينيين والعرب، وهو عبارة عن كتابة مبهمة أو إخفاء لكلمات معينة أو رموز مشفرة متبادلة بين جهتين بحيث لا يعلمها الطرف الثالث، إلا أنه بإمكانه معرفة التواصل بينهما[1]،

[1] من مدونة البحث العلمي [على الخط] متاحة على الرابط التالي: https://educad.me/ [شوهد يوم: 20-06-2022]

وهو منتشر بكثرة في عصرنا الحالي لتعدد الوسائط والتقنيات، فهو موجود في كلمات المرور الخاصة بالحواسيب وبطاقات الائتمان البنكية والمالية وفي البريد الإلكتروني والملفات.

صورة رقم 01 لرموز وكلمات مستعملة قديما في عملية التشفير

3.1 الحاجة إلى التشفير وعمي البيانات:

أدخلت تقنية المعلومات والاتصالات نوعا جديدا من التهديد على سرية وأمن المعلومات، وأدى الانتشار السريع للمعلومة وحرية اقتناءها وتصفحها ضرورة العمل على أمنها والحفاظ على سريتها، حيث مكنت سهولة اختراقها من طرف العارفين بخبايا هذه التقنية عاملا سلبيا يكتب عليها، وهو ما استدعى التدخل الفوري لكبح هذه التصرفات والحد منها باستخدام أحدث ما توصلت إليه التكنولوجيا في حماية الممتلكات الفكرية

3. مجالات التشفير:

تتنوع وتختلف مجالات استخدام عملية التشفير باختلاف الحاجة إليها، وإن اقتصر استخدامها سابقا على المجال الحربي والعسكري، غير أن التكنولوجيا وتعدد مصادر المعلومات واختلافها والازدهار المذهل الذي عرفته مختلف وسائل الاتصال، مهد الطريق أمام تنوع مجالات استخدام التشفير دون استثناء، إلا أن معظمها تصب في خانة السيطرة على المعلومة والاستحواذ عليها لأغراض ربحية (عسكرية، تجارية، علمية، ثقافية...)، فهي في النهاية تسعى للسيطرة الاقتصادية وجني المال، وغالبا ما يتم التشفير دون علمنا بذلك.

4. التشفير في عصر المعلومات:

أدى التطور المذهل الذي عرفته البشرية باختراع الكمبيوتر وشبكة الانترنت، تحولا جذريا مس جميع المفاهيم والمعطيات، وانتقلت الحروب التي كانت تستخدم فيها الجيوش والآلات العسكرية الكبيرة والأسلحة والذخائر، إلى أخرى مغايرة تماما، إذ لم يكن يتصور أن تستخدم في الصراع بين الدول قنوات غير مرئية وجد متطورة تعتمد في الأساس على المعلومة وكيفية بثها والسيطرة عليها.

ولما كان استخدام عملية التشفير أو عمي البيانات يحتاج إلى مفتاح أو كلمات يتم الاتفاق عليها بين المرسل والمرسل إليه لغرض فك الرموز وإعادة قراءتها وهو ما يطلق عليه بالتشفير المتماثل (Symmetric) (الألوسي، زينة رجب، 2022) والذي يتم ببساطة بمفتاح واحد والذي من عيوبه إمكانية تعرف أو التقاط الطرف الثالث للمفتاح المتعارف عليه مما يسهل عليه فك الرسالة وقراءتها، أما التشفير الثاني وهو ما يطلق عليه بالتشفير غير المتماثل (Asymmetric) (الألوسي، زينة رجب، 2022) حيث يتم استخدام مفتاحان أحدهما عام لتشفير الرسالة والآخر خاص لفك التشفير، حيث تعتبر هذه التقنية أكثر أمانا وانتشارا من سابقتها.

1.4 العلامة المائية (watermark):

تعرف العلامة المائية على أنها إشارة رقمية يتم إدخالها في الملفات الرقمية لتحميل ملفات خاصة بحقوق الملكية دون الإنقاص من جودة الصورة الأصلية (منصور، وفاء و خضرا، ياسر سعيد، 2022) ، وهي نفس التقنية الموجود في الأوراق النقدية لدول العالم، إذ أن المدقق في الصورة الموجودة على غلاف الورقة النقدية يرى بما لا شك فيه صورة أو علامة مائية رقمية تميل للاختفاء أو تعمد إخفاؤها، وكلما كانت شديدة الدقة والإخفاء كلما ارتفعت قوة الحماية من الاستنساخ أو التزوير.

الصورة رقم (02) العلامة المائية في عملة 100 دولار الأمريكية[2]

2.4بصمة الأصبع (Fingerprint):

رغم أن بدايات استخداماتها ترجع لعدة سنوات خلت[3]، إلا أنها تعتبر كأحدث الطرق والوسائل التكنولوجية لحماية البيانات الشخصية ولتسهيل عملية الدخول للمواقع الحساسة وحتى لتفادي تكرار استخدام الرمز السري الذي قد يتعرض للنسيان أو التلف أو حتى تجنب إعادة إدخال البيانات الشخصية على أحد مواقع الويب.

غير أن الاستخدام المفرط لتكنولوجيات الإعلام والاتصال خاصة الانترنت، ضاعف من مخاطر تلف البيانات الشخصية وانتحالها من طرف أفراد متخصصين في هكذا مجالات، وهو ما استوجب استحداث تقنية مضادة لحماية الإنتاج الفكري ونشر المعلومات والبيانات الشخصية والمصرفية.

5.الحماية الفكرية:

تشير الملكية الفكرية إلى الإبداعات التي ينتجها العقل– كل شيء– بدءا من المصنفات الأدبية إلى الاختراعات وبرامج الحاسوب مرورا بالعلامات والإشارات التجارية.[4]

وهي بذلك، تمس كل ما له علاقة بالإبداع الإنساني الفكري، الذي هو ملك ذاتي وللبشرية جمعاء، ولذلك جاءت القوانين والتشريعات لحمايته من الانتحال والتشويه والسرقة.

1.5 أنواع الملكية الفكرية:

تختلف أنواع وفئات الملكية الفكرية باختلاف المنتج، فهي:

1.1.5 الملكية الصناعية:

وهي الملكية الفكرية التي يوجد لها تطبيق صناعي بما في ذلك الرسوم و الاختراعات والرسوم والنماذج الصناعية والعلامات التجارية والبيانات الجغرافية[5]، كما أنها تشمل حتى المنتجات الزراعية المصنعة أو الطبيعية.

2.1.5 الملكية الفكرية:

وهي تشمل حقوق المؤلِّف المالية والتي بإمكانه التنازل عليها، والمعنوية والتي يقصد بها حقه في نسبة المؤلَّف له بأي شكل من الأشكال.

2.5. حماية الملكية الفكرية:

[3] Empreinte digitale.Wikipédia : l'encyclopédie libre. https://fr.wikipedia.org/wiki/Empreinte_digitale

[4] المنظمة العالمية للملكية الفكرية.[على الخط] متاح على الرابط: https://www.wipo.int/edocs/pubdocs/ar/wipo_pub_450_2020.pdf . (شوهد يوم : 18.09.2022)

[5] نفس المرجع السابق.

أخذت حماية الملكية الفكرية منذ فترة من الزمن شكلان متميزان:

1.2.5. براءات الاختراع: براءة الاختراع هي وثيقة حماية استئثارية تمنح لمن توصل إلى اختراع[6]جديد أو تطوير أو تحديث مغاير في منتوج ما، وهي تمنح لصاحب هذه البراءة الحق في منع الغير من استغلالها والاستفادة منها بأي طريقة من الطرق كإعادة تسويقها وبيعها.

2.2.5 حقوق المؤلف والحقوق المجاورة:

حق المؤلف مصطلح قانوني يصف الحقوق الممنوحة للمبدعين في مصنفاتهم الأدبية والفنية، وبتطور الأوضاع تطورت بذلك الحقوق المجاورة للمؤلف لتشمل : حقوق الممثلين والموسيقيين وحقوق منتجي التسجيلات الصوتية، وكذا حقوق هيئات الإذاعات في برامجها الإذاعية والتلفزيونة(رحايلي، محمد و بلهوشات الزبير، 2015)

وقد أخذت عملية نشر وبث المعلومات بمختلف أشكالها منعرجا خطيرا باستخدام شبكة الإنترنت ومنصات التواصل الاجتماعي، التي لم تتمكن القوانين والمراسيم واللوائح التشريعية من محاصرتها وتقييدها أو الحد من استعمالها لغير أغراضها.

6. النشر الإلكتروني:

ارتبط النشر الإلكتروني بأزمة الانفجار المعلوماتي الذي ميز نهاية القرن الماضي وبداية القرن ال21 والذي عرف رواجا وانتشارا رهيبا مس جميع ميادين العلوم والتكنولوجيا، وكانت الزيادة المتأخرة التي مست تكلفة الطبع الورقي أدت لارتفاع تكاليف ميزانيات المكتبات التي لم تعد بالإمكان مواجهتها، الأمر الذي أضر بسمعة الكتاب المطبوع بتحوله لسلعة ليست في متناول الجميع.

وعرف النشر الإلكتروني رواجا كبيرا باختراع تقنية الويب والشبكة العنكبوتية (الانترنت)، وبظهور شبكات التواصل الاجتماعي أخذت ظاهرة النشر الالكتروني منعرجا خطيرا استعملت فيه أحدث وآخر ما توصلت إليه تكنولوجيات التشفير والتجسس واختراق المعلومات، كما أصبحت عملية نشر الصور الفيديوهات واستنساخ المؤلفات وبيعها سوقا رائجة جد مربحة للسرعة الفائقة التي تصاحب عملية البث والترويج، وكذا صعوبة حصر ما يتم نشره عبر هذه القنوات.

7.التحول في عملية التشفير وإخفاء المعلومات:

[6]مكتب البراءات السعودي.[على الخط]،متاح على الرابط:
https://www.pnu.edu.sa/ar/Deanship/Research/Documents/.pdf (شوهد يوم: 22.09.2022)

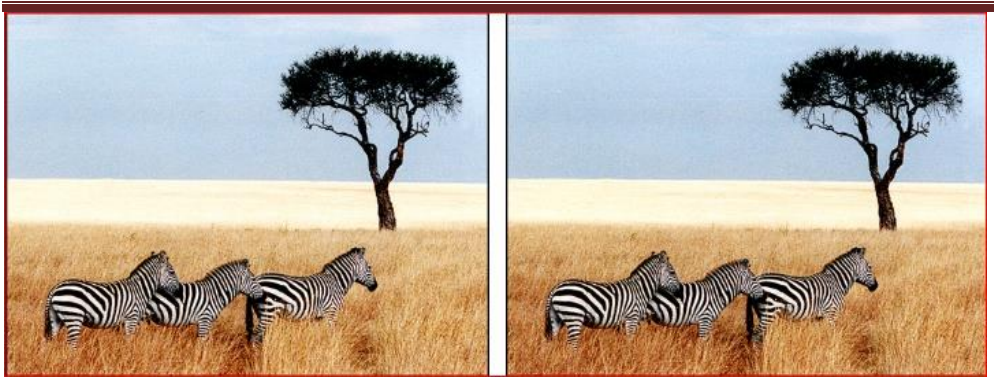
انتقلت عملية التشفير وإخفاء المعلومات من الطريقة التقليدية التي تم طرحها سابقا، للتحول هي أيضا إلى ظاهرة رقمية طغى عليها الطابع التكنولوجي في الاستخدام والاستغلال والنشر والبث، وتحولت بذلك حتى الأغراض المستخدمة لها، فاستغلت الدوائر الحكومية وقطاعات الحربية والجوسسة وكبريات الشركات العالمية العابرة للقارات هذه الطفرة التكنولوجية لتمرير رسائلها المشفرة باستخدام تقنية الستيغانوغرافي خاصة في مجال الصور المرسلة ذات خاصية JEPG.

1.7. الستيغانوغرافي (Steganography):

تعرف تقنية الستيغانوغرافي بأنها عملية إخفاء للمعلومات لكن في الفضاء الرقمي وباستغلال بعض الثغرات واستخدام تكنولوجيات الإعلام الآلي في تمرير رسائل مخفية داخل نصوص أو صوت أو صورة، دون الإضرار بخاصية الملف المرسل حتى لا يتم الكشف عنه، وهي بين كل ذلك سلاح ذو حدين، ففي حين أن الكثيرين يقومون باستخدامها لتمرير الرسائل المشفرة والنصوص غير المرئية التي قد تستخدم لأغراض مختلفة، إلا أنه وبخلاف كل هذا فإن تقنية الستيغانوغرافي وبخاصيتها الفريدة تعتبر من أرقى الطرق والتكنولوجيات التي قد تكون الحل الذي انتظره المكتبيون والمؤلفين وحتى الناشرين في حماية منتجاتهم الفكرية في هذا الفضاء الرقمي.

2.7 مجالات استخدام تقنية الستيغانوغرافي :

تسمى الحاوية التي تحمل الرسالة أو الكتابة المخفية برسالة (ستيغو Stego)، وبما أن تقنية الألوان المستخدمة في نظام الويندوز والفيستا (windows and vista) (Urbanovich, N., & Plaskovitsky, V. (2011)) يتم فيها تقديم لون الرموز في نظام (RGB) في 08 بتات (bits)، من الرقم 0 إلى 255، مما يساعد في التلاعب بالأرقام الخاصة بتكوين الألوان، دون أن يضر ذلك بجودة الصورة الحاوية للرسالة أو النص المشفر.



الصورة على اليسار هي الصورة الأصلية بينما تحمل الصورة على اليمين النص المخفي

وهو ما يفتح المجالات العديدة للاستخدام الواسع لهذه التقنية، لما تتميز به بإمكانية إدخال النص المخفي بالتلاعب بنظام الألوان المكون من (0 إلى 255) ما يضفي عليها نوعا من المرونة في تمرير النصوص والرموز والكلمات المخفية دون لفت أدنى انتباه أو شك، الأمر الذي يوسع من استخدامها إذ هي لا تعتمد على تشفير النص بل بتمرير كلمات أو رموز مخفية في وعاء حاو.

3.7 بين التشفير وتقنية الستيغانوغرافي:

للكشف عن التفريق بين علم التشفير وتقنية إخفاء المعلومات أو ما يطلق عليه ب (الستيغانوغرافي) فإننا نكتفي بعرض الجدول التالي الذي يفصل في مميزات كل منهما:

	علم التشفير	علم الإخفاء
من حيث العلم بوجود الرسالة	يعلم وجود الرسالة	لا يعلم وجود الرسالة
من حيث الاتصال	يمنع الأطراف الآخرين من معرفة محتوى الاتصال	يمنع الآخرين من معرفة وجود الاتصال
من حيث الشيوع	تقنية شائعة	تثنية غير شائعة

جدول مقارنة بين علم التشفير و علم إخفاء المعلومات (شاكر، سارة علاء، 2010)

4.7 تقنية الستيغانوغرافي و الحماية الفكرية:

إذا كانت الحماية الفكرية قد تعرضت في الآونة الأخيرة لبعض الهزات الارتدادية التي مست أركانها بالاستخدام المفرط للوسائط الرقمية التي لم تتمكن القوانين والشرائع من حصرها، إلا أن تقنية الستيغانوغرافي أعطت بعضا من بصيص الأمل الذي قد يساعد في ضبط وحصر الاستخدام غير القانوني للأوعية الفكرية وذلك باستخدام التمثيل الثنائي للأحرف النصية كحاوية لوضع المعلومات

من أجل حماية منشئي حقوق الطبع والنشر للمستندات[7] ، بحيث بالإمكان تمرير رقم الإيداع القانوني ووضعه ضمن صورة من الصور بتقنية التلاعب بالألوان دون أن يتم التعرف عليه ولا حتى ملاحظته، وهو ما يساعد في ترقية مجال الحماية الفكرية عبر الفضاء الرقمي الذي عرف نوعا من حالة التسيب والانفلات.

وقد تساعد العلامة المائية مثلا والتي هي من أنواع تقنية الستيغانوغرافي في التعرف على ملكية حقوق النشر وحمايتها، بحيث يجب أن تكون هذه الأخيرة المضمنة قوية جدًا وآمنة وإلا فلن تتمكن من تحمل تعديلات المعالجة والهجمات المتعمدة في قناة الاتصال(Yershov, A., & Rusakov, P. 2010.)

8.الآفاق المستقبلية لتقنية الستيغانوغرافي في مجال الحماية الفكرية:

إذا كانت تقنية الستيغانوغرافي و معها علم الإخفاء مجالا واسعا ورحبا لا يمكن حصره كونه يتخذ من الفضاء الرقمي طريقة للانتشار والتوسع، فما هي آفاقه المستقبلية خاصة في مجال الحماية الفكرية، التي أخذت منعرجا حاسما بالاعتماد شبه الكلي في نشر المعلومة على تكنولوجيات الإعلام والاتصال.

إذ أظهرت الدراسات أنه يجب أن يتم تصميم كل حل ليناسب صعوبة معينة في حقوق الملكية الفكرية وأن يستند إلى حالة دراسة ملموسة .(Hamza, R., & Pradana, H. 2022) ، فالانتقال من العلامات المائية النصية إلى الصورة الثابتة والمتحركة والصوتية يختلف اختلافا متباينا، مما يعطي إشارة بضرورة الاستخدام الأنسب واللائق لكل تقنية وما يناسبها في إخفاء المعلومة.

و إن كانت معظم القنوات التلفزيونية (رياضية كانت، ثقافية، أخبارية ...) تستخدم نظام التشفير و خفي المعلومات، فإن المستقبل يدعو لاستخدام هذه التقنية في عمي وإخفاء البيانات والمعلومات في مجال الحماية الفكرية والذي يمكن أن تتبناه المكتبات في حماية مقتنياتها ومصادرها الرقمية من الضياع والسرقة أو حتى من التقليد والاستنساخ.

فهو إذا مجال واسع وفسيح، وإن كانت استخداماته قديما وحديثا ترتكز في الميادين التجارية والعسكرية، غير أن للحماية الفكرية والمكتبات ومراكز المعلومات حظ أوفر وكبير في الاستعانة به

7

بعد أن تجاوزت المعلومة حدود الفضاء الورقي الذي كان بإمكان مراكز المعلومات ممثلة في (المكتبات ومراكز التوثيق) من حصره والتحكم فيه ولو نسبيا، الأمر الذي لم يعد ممكنا حاليا باستخدام نفس الطرق والأساليب والوسائل القديمة، ما يجعل توسيع استخدام هذه التقنية في مجالات النشر والطبع وحقوق المؤلف والحقوق المجاورة من أولى الأولويات التي لا تحتمل التأخير.

إذ يتضمن أحد استخدام إخفاء المعلومات علامة مائية تخفي معلومات حقوق النشر عن طريق تراكب الملفات التي لا يمكن اكتشافها بالعين المجردة بسهولة.[8]

1.8 الاستخدام غير اللائق لتقنية الستيغانوغرافي:

إذا كانت إيجابيات تقنية الستيغانوغرافي أو إخفاء المعلومات والتي تهمنا في هذا المقام تنحصر في كيفية حماية الملكية الفكرية، والاستعانة بها في الاستخدام الأفضل لموارد ومصادر مراكز المكتبات والمعلومات، إلا أن الخوف من تجاوز هذه الحدود إلى استخدامات غير لائقة يطرح نفسه وبشدة كتمرير رسائل منافية للأخلاق أو معاداة للوحدة الوطنية، أو التلاعب بالصور والفيديوهات الموجهة للأطفال بتمرير صور ونصوص بداخلها منافية للآداب، وهو ما يعقد من عملية المراقبة المستمرة لهذه الملفات والذي يستلزم الاحتفاظ بالصور أو الملفات الأصلية لدى المحققين لمقارنتها مع تلك المرسلة قصد المطابقة بينها.

9. الخاتمة:

رغم ما عرفته البشرية من طرق مختلفة في تشفير الرسائل والنصوص والذي عرف رواجا كبيرا في الأوساط التجارية والعسكرية والحربية، غير أن ظهور الوسائل التقنية وتكنولوجيات الاتصال أبان عن انتشار واسع لتقنيات الانتحال والسرقات والتقليد عبر الفضاء الرقمي، الأمر الذي مهد لظهور تقنية مشابهة لسابقتها تختلف عنها بعملية إخفاء للمعلومات دون تشفيرها بل تضمينها في حدود النص أو الصورة والصوت المرسل، وهو ما يدعو إلى إمكانية الاستفادة من هذه التقنية في الحفاظ على الملكية الفكرية وحقوق المؤلف والحقوق المجاورة في الفضاء الرقمي، وكذا الاستعانة بها في حماية ممتلكات المكتبات الرقمية من التقليد والاستنساخ غير المرخص.

[8] https://ar.theastrologypage.com/steganography

. قائمة المراجع:

- من مدونة البحث العلمي [على الخط] متاحة على الرابط التالي: https://educad.me/ [شوهد يوم: 20-06-2022]

-الألوسي، زينة رجب.***وسائل تحقيق أمن المعلومات***. **[على الخط] متاح على الرابط:**

https://colaw.uobaghdad.edu.iq. (**شوهد يوم : 22.05.2022**)

– منصور، وفاء و خضرا، ياسر سعيد، 2022. ***إستراتيجية فعالة لتضمين العلامة المائية في الصورة الرقمية أثناء عملية ضغطها بصيغة JPEG***، مجلة جامعة البعث، مج.44، ع.9 ، ص110.

– Empreinte digitale.Wikipédia : l'encyclopédie libre.

https://fr.wikipedia.org/wiki/Empreinte_digitale

- المنظمة العالمية للملكية الفكرية.[على الخط] متاح على الرابط:

https://www.wipo.int/edocs/pubdocs/ar/wipo_pub_450_2020.pdf . (شوهد يوم : 18.09.2022)

–مكتب البراءات السعودي.[على الخط]،متاح على الرابط:

https://www.pnu.edu.sa/ar/Deanship/Research/Documents/.pdf (شوهد يوم: 22.09.2022)

- رحايلي، محمد و بلهوشات الزبير، 2015. حقوق المؤلف والحقوق المجاورة في البيئة الرقمية: الحالة الجزائرية.مجلة جامعة الأمير عبد القادر للعلوم الإسلامية.مج.29، ع.1.ص 504.

- Urbanovich, N., & Plaskovitsky, V. (2011). The use of steganographic techniques for protection of intellectual property rights. *New Electrical and Electronic Technologies and their Industrial Implementation*, 147-148.

- شاكر، سارة علاء، (2010) . استخدام العلامة المائية في اخفاء البيانات.ص26

-Yershov, A., & Rusakov, P. (2010). Universal Stegoconstructor in Context of Intellectual Property Protection. *Computer Science (1407-7493)*, *43*.

- Hamza, R., & Pradana, H. (2022). A Survey of Intellectual Property Rights Protection in Big Data Applications. *Algorithms*, *15*(11), 418.

- https://ar.theastrologypage.com/steganography[1]