Université de Kasdi Merbah Ouargla Faculté des Nouvelles Technologies de l'Information et de la Communication

Un Mémoire Présenté au Département d'Informatique et des Technologies de l'Information pour le Diplôme de Master LMD en Administration et sécurité du réseau

Thème

Tatouage numérique des fichiers audio échangés en télémédecine

Présenté par:

HARRIF Radja

HAMADOU Roumaissa

Encadré par:

KHALDI Amine

Année Universitaire: 2021/2022

Remerciement

*Tout d'abord, nous voudrions remercier le "**Dieu**" Tout-Puissant, qui nous a donné Force, patience et volonté pour faire cet humble travail.*

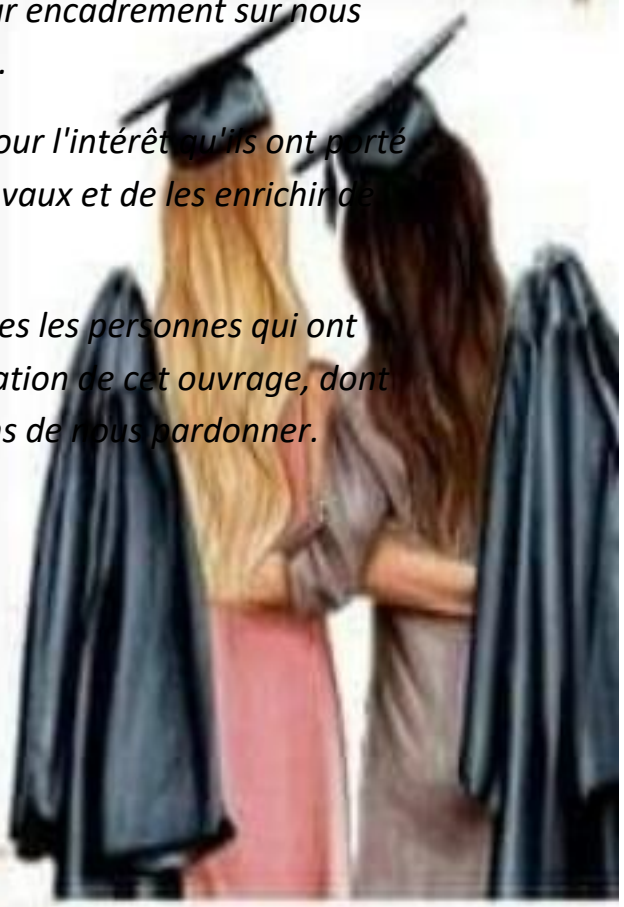
Nous profitons de cette thèse de fin d'étude pour adresser nos remerciements à tous ceux qui ont contribué, tant par leur aide matérielle que morale, à ce que ce travail voie le jour, fruit d'un long cheminement de recherche et de travail.

Nous tenons à remercier nos chers parents pour ces encouragements et cette aide.

*Nous tenons à remercier **Mer. KHALDI Amine**, notre superviseur pour sa disponibilité, ses précieux conseils et ses encouragements, ainsi que toute l'informatique et le service informatique pour leur encadrement sur nous durant toutes ces années.*

Nous remercions également les membres du jury pour l'intérêt qu'ils ont porté à nos recherches en acceptant d'examiner nos travaux et de les enrichir de leurs suggestions.

Enfin, nous exprimons nos remerciements à toutes les personnes qui ont contribué d'une manière ou d'une autre à la réalisation de cet ouvrage, dont les noms ont été omis, et nous leur demandons de nous pardonner.



Dédicace

Je dédie ce mémoire à :

Mon très cher père : Mohemed el Bachir

Merci pour tout ce que tu as fais pour moi pour assurer mon instruction et mon bien être, je veux te dire combien je t'aime, j'espère réaliser ce jour un de tes rêves et être digne de ton nom, ton éducation et ta confiance, que dieu te garde.

Mon adorable mère : Saida

Aucune parole ne peut être dite à ta juste valeur pour exprimer combien je t'aime. Tes prières et tes grands sacrifices m'ont comblé tout au long de mon existence, en ce jour j'espère réaliser un de tes rêves. Que dieu tout puissant, te garde, te procure santé, bonheur et longue vie pour que je puisse te rendre un minimum de ce que je dois.

A mon cher fiancé :Oussama

Merci pour votre soutien moral constant avec motivation et aide dans ce travail.

***A mes jolies sœurs** :kamilia, Zineb, khawla,Latra, Mariem et Asma.*

***A mes chers frères:**Mouhi el Dine et Ilyas.*

Pour leurs encouragements permanents, et leur soutien moral. Merci d'être toujours à mon coté par votre présence et votre amour.

***La femme de me frère:**Djahida.*

Mes très chères amies:

Chaima, Amani, Samah, Salsabil, khadidja, Afaf, Mayson, Inas, Rania, Zineb, Ouisal...

Vraiment Merci pour votre soutien, d'être toujours avec moi, merci pour les bons moments qu'on a passé ensemble, vos sourires étaient un vrai courage pour moi durant toute ma vie.

***Mon binôme:Hamadou Romaissa** merci pour les bons moments qu'on a passé ensemble, tu étais ma sœur et amie, et heureusement je t'ai rencontré.*

A toutes les étudiantes de notre promotion

A tous ceux et celles que je n'ai pas cité mais qui sont présents dans mon cœur.

Merci…

HARRIF Radja!

Dédicace

Je dédie ce mémoire à :

Ma belle maman : Aïcha

Il n'y a pas de mots à dire sur ta vraie valeur pour exprimer à quel point tu m'aimes. Vos grandes prières et sacrifices m'ont accompli toute ma vie, et j'espère qu'en ce jour je réaliserai l'un de vos rêves. Que Dieu Tout-Puissant vous préserve, et vous accorde santé, bonheur et longue vie, afin que je vous rende au minimum ce que vous devez.

Cher papa : Said

Merci pour tout ce que vous avez fait pour moi pour assurer mon éducation et mon bien-être, je veux vous dire combien je vous aime, aujourd'hui je souhaite réaliser un de vos rêves et être digne de votre nom, de votre éducation et de votre confiance que Dieu vous bénisse .

À ma belle sœur :*Nour Al-houda*

A mes chers frères : *Yasser, Abd el-Nour*

Pour leurs encouragements constants et leur soutien moral.

A mon cher fiancé Belkacem *: Je te remercie d'être toujours à mes côtés, pour ton soutien moral et pour ton grand amour.*

Chers amis : *Tante Najat, oum kaltoum, Hanan, Fatima, Rayan, Khadidja, Salsabil,Inas, Shahinaz, Maryam.*

Merci beaucoup pour votre soutien, d'être toujours avec moi, merci pour les bons moments que nous avons passés ensemble, vos sourires ont été un vrai courage pour moi toute ma vie.

Mon partenaire :*Harrif Radja Merci pour les bons moments que nous avons passés ensemble Tu étais ma sœur et ma petite amie et heureusement je t'ai rencontré.*

A ma famille à tous les élèves de notre classe

À tous ceux que je n'ai pas mentionnés mais qui sont dans mon cœur

HAMADOU Roumaissa !

Résumé

L'utilisation de données numériques telle que les images, l'audio et la vidéo augmente de façon exponentielle en raison des progrès technologiques et de la révolution Internet dans de nombreux domaines tels que le commerce et la télémédecine. Avec ces développements vient le problème de la protection de la propriété individuelle et des droits d'auteur pour ces données numériques. Le filigrane audio numérique est utilisé comme méthode de sécurité du signal audio. Afin de sécuriser les données échangées en télémédecine, notre projet vise à proposer des approches robustes et imperceptibles de tatouage numérique. Ces méthodes seront appliquées aux fichiers audio contenant des informations médicales tels que des battements de cœur ou des sons respiratoires. Le filigrane est inséré dans un hôte de signal audio afin que le contenu inséré ne soit pas reconnu (en cachant des informations confidentielles dans le fichier hôte). Dans le même temps, le tatouage inséré doit être suffisamment résistant contre divers sons. Ses travaux sont résumés dans une application qui augmente la sécurité des échanges de données audio sensibles en télémédecine dans le domaine spatial en utilisant la technique LSB (Least SignificantBit)LSB. L'efficacité a été mesurée en calculant les valeurs SNR signal sur bruit (Signal-to-Noise Ratio) et test de capacité(bits).

Mots clés : tatouages numériques, fichiers audio, télémédecine, domaine spatial, LSB,SNR.

الملخص

يتزايد استخدام البيانات الرقمية مثل الصور والصوت والفيديو بشكل كبير بسبب التقدم التكنولوجي وثورة الإنترنت في العديد من المجالات مثل التجارة والتطبيب عن بعد. مع هذه التطورات يأتي مشكل حماية الملكية الفردية وحقوق التأليف والنشر لهذه البيانات الرقمية. يتم استخدام العلامة المائية الرقمية الصوتية كطريقة لأمن الإشارات الصوتية . من أجل تأمين البيانات المتبادلة في الطب عن بعد ، يهدف مشروعنا إلى اقتراح مناهج قوية وغير محسوسة للعلامة المائية الرقمية . سيتم تطبيق هذه الطرق على الملفات الصوتية التي تحتوي على معلومات طبية مثل دقات القلب أو أصوات التنفس. يتم إدراج العلامة المائية في مضيف إشارة صوتية بحيث لا يتم التعرف على المحتوى المدرج (عن طريق إخفاء المعلومات السرية في الملف المضيف). في الوقت نفسه، يجب أن يكون الوشم المدرج قويًا بما يكفي ضد الأصوات المختلفة. تم تلخيص هذا العمل في تطبيق يزيد من أمان تبادل البيانات الصوتية الحساسة في التطبيب عن بعد في المجال المكاني باستخدام تقنية(البت الأقل أهمية LSB)تم قياس الكفاءة عن طريق حساب قيم الإشارة إلى الضوضاء (SNR) واختبار السعة (bit).

الكلمات المفتاحية : العلامات المائية الرقمية ، الملفات الصوتية ، التطبيب عن بعد ، المجال المكاني ، LSB، SNR.

Abstract

The use of digital data such as images, audio and video is increasing exponentially due to technological advancements and the internet revolution in many areas such as commerce and telemedicine. With these developments comes the issue of individual ownership and copyright protection for this digital data. The digital audio watermark is used as a security method by the audio signal. In order to secure the data exchanged in telemedicine, our project aims to propose robust and imperceptible approaches of digital watermarking. These methods will be applied to audio files containing medical information such as heartbeats or breathing sounds. The watermark is inserted into an audio signal host so that the inserted content is not recognized (hiding confidential information in the file host). At the same time, the inserted tattoo should be sufficiently resistant against various sounds. His work is summarized in an application that increases the security of sensitive audio data exchange in telemedicine in the space domain using the Least Significant Bit (LSB) technique. Efficiency was measured by calculait the signal-to-noise (SNR) values (Signal -to-Noise Ratio) and capacity test (bits).

Keywords: digital watermarks, audio files, telemedicine, spatial domain, LSB, SNR.

Table des matières

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des Tableaux

Liste des Abréviations

Abréviations	Designations
AWGN	Additive white Gaussian noise
DCT	DiscreteCosineTransform
DWT	DiscretewaveletTransform
DFT	DiscreteForiuiTransform
SVD	Singular value decomposition
HVS	Human Visual System
HAS	HumanAuditory System
Hz	Hertz
Db	Decibel
Wav	Waveform
MP3	MPEG-1 audio Layer 3
LSB	Least Significant Bit
SNR	Signal to Noise Ratio

Introduction générale

Ces dernières années, la croissance impressionnante de la technologie Internet et l'expansion des appareils informatiques puissants ont non seulement stimulé le commerce électronique multimédia, mais ont également encouragé les artistes, les médecins et les meilleurs encadreurs à partager et à promouvoir leur travail en ligne. Évidemment, cela signifie une présence massive sur le Web pour les données multimédias numériques telles que l'audio, l'image et la vidéo.

Cependant, avec la prolifération et la facilité de l'utilisation d'outils de traitement multimédia performants et personnalisés, ces données représentant différents domaines peuvent être facilement téléchargées, modifiées, saisies illégalement puis redistribuées ou commercialisées en grande partie sur Internet. Ensuite, la protection des droits de propriété intellectuelle des propriétaires est devenue une préoccupation majeure. Ainsi, une solution à ce problème est apportée par le tatouage numérique, qui consiste à inclure un message appelé«watermark» dans les éléments multimédias pouvant être découvert ou extrait ultérieurement sans modifier le contenu original du média numérique.

Le domaine des tatouages numériques a connu un grand développement et de nombreuses méthodes ont été proposées, où la majorité des contributions ont été faites pour des photos et des vidéos avec des tatouages, mais les tatouages audio ont été moins approchés par rapport aux deux autres. En fait, la conception de l'algorithme de tatouage audio est plus difficile par rapport à l'algorithme image et vidéo, en raison de la plus grande sensibilité du système auditif humain (HAS) par rapport au système visuel humain (HVS). Par conséquent, le besoin d'une solution optimale et efficace est devenu nécessaire car les documents audionumériques sont de plus en plus utilisés notamment en télémédecine, qui est notre domaine d'étude maintenant qui réside dans la protection et la dissimulation de données audio telles que : la fréquence cardiaque et les sons respiratoires.

Cependant, pour développer des tableaux de marquage tatouage efficace, deux caractéristiques importantes doivent être prises en compte : (1) Imperceptibilité : pour le système de tatouage invisible, il ne doit pas y avoir de différence évidente entre le contenu original et le contenu en tatouage, (2) la robustesse : celle-ci devrait exister pour que le tatouage en ligne puisse survivre, dans une certaine mesure, avec une manipulation intentionnelle et involontaire du contenu.

Introduction générale

La technologie de tatouage numérique sécurisé comporte deux actions : la procédure d'insertion et la procédure d'extraction. La procédure d'incorporation consiste à insérer un tatouage dans le contenu multimédia hôte (communément appelé la couverture) qui est une signature numérique qui conserve les informations de copyright exclusives au propriétaire. Ensuite, au moyen des clés secrètes spécifiées, la procédure d'extraction permet au propriétaire ou au destinataire autorisé du contenu numérique de récupérer le tatouage à partir du contenu tatoué.

Le tatouage numérique peut se faire soit dans le domaine spatial, soit dans le domaine de la transformation. La technologie du domaine spatial opère directement sur les pixels : le tatouage s'intègre en modifiant directement les valeurs des pixels (comme les bits les moins significatifs (LSB)), tandis que la technologie du domaine de transformation intègre le tatouage en ajustant les paramètres du domaine de transformation. Les transformations courantes qui ont été fréquemment utilisées sont la transformée en cosinus discrète (DCT), la transformation d'onde discrète (DWT), la transformée de Fourier discrète (DFT) et l'analyse de valeur unique (SVD). Plusieurs combinaisons de ces transitions ont également été examinées dans la littérature pour donner de meilleurs résultats. Par rapport aux techniques de domaine spatial, il a été démontré que les techniques de transformation de champ permettent d'obtenir une meilleure force et une meilleure non-perception. De plus, le processus d'extraction peut être aveugle, semi-aveugle ou non aveugle.

Un grand nombre de technologies ont été utilisées récemment pour traiter les tatouages audio, depuis le développement et la création de nombreux systèmes et applications telles qu'une application pour protéger les secrets de l'armée et un système de tatouage pour protéger les données audio... Le but de notre projet nous créera une application qui accroît la sécurité des échanges de données audio sensible en télémédecine, qui consiste à protéger et à masquer les données audio avec une technologie spéciale pour éviter les attaques auxquelles les institutions médicales sont confrontées dans les processus de diagnostic afin de garantir l'intégrité des informations sur chaque patient.

Notre projet est divisé en trois chapitres, le reste du projet est organisé comme suit :

Le chapitre 1 donne un concept général de tatouages numériques et de la télémédecine en termes de cadre du système, et décrire le système de tatouage numérique .

Le deuxième chapitre proposé un concept audio numérique actuel qui contient des caractéristique et formats de tatouage pour le signal audio. Ensuite, le chapitre aborde de le domaine à deux insertions spatial et fréquentielle.

Dans le chapitre 3 nous utilisons l'algorithme LSB pour l'insertion et l'extraction et obtenir l'évaluation à l'aide de SNR et de capacité

Enfin, nous concluons notre projet et soulignons les sujets restants qui peuvent être considérés comme des pistes de recherche plus approfondies sur les tatouages audio.

Chapitre I Généralités sur le tatouage numérique et la télémédecine

Chapitre 1 :Généralités sur le tatouage numérique et la télémédecine

I.1. Introduction :

Les différentes multimédias (image, vidéo et audio) sont devenues des outils très importants dans différentes domaines (imagerie médicales, satellitaire... etc.) ou leur transmission est très facile à travers les réseaux. En effet les documents multimédias peuvent être dupliqués, modifiés et falsifiés. Dans ce contexte il est nécessaire de mettre en ouvre des systèmes adaptés aux nouvelles technologies qui permet de respecter le droit d'auteur et de vérifier l'intégrité et de garantir l'authentification.

Pour répondre à ces besoins il existe plusieurs techniques qui sont utilisées pour plusieurs buts ainsi que la protection de droit d'auteur. Une solution possible consiste à insérer une certaine information invisible dans les fichiers audio où l'information peut être intégrée ou extraite à des fins différentes.

Dans ce chapitre, nous présentons le contexte général du tatouage numérique, y compris l'historique et les propriétés des tatouages, les attaques auxquelles ils sont exposés, ainsi que la définition et les techniques utilisées en télémédecine.

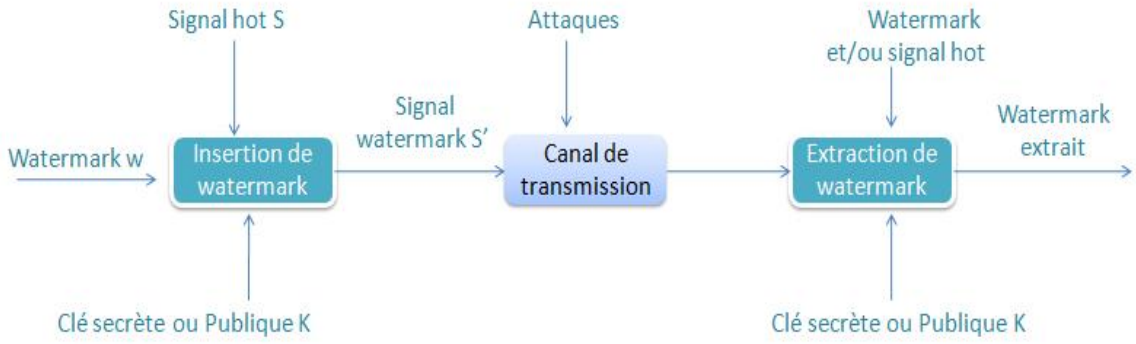


Figure I.1 Système de tatouage audio

I.2. Historique du tatouage numérique :

L'information a toujours eu un rôle primordial au cours de l'histoire. Son contrôle est synonyme de pouvoir et de puissance. Cette entité peut représenter des plans de bataille, des négociations secrètes, les dernières actualités des journaux télévisés, etc. C'est une donnée précieuse et son exploitation peut apporter la richesse. Pour cette raison, sa protection est

nécessaire. Deux grandes tendances visent à protéger l'information : le chiffrement et la stéganographie (qui inclut le tatouage).

Les premiers emplois de la stéganographie sont relatés par l'historien grec **Hérodote** il y a plus de deux mille ans. Les cheveux d'un esclave confiant sont rasés puis le message est tatoué sur son crane chauve, Une fois que les cheveux ont repoussé, l'esclave est envoyé au destinataire qui de son tour lui rase de nouveau la tête afin de lire le message, Une autre approche consiste à graver le message sur une tablette de bois, ensuite la recouvrer de cire afin d'obtenir une tablette d'écriture normale.

En 1586, la police secrète de la couronne britannique a identifié des lettres quicontenaient un message dissimulé contre la reine **Elizabeth**. A cette époque, certains postiers anglais avaient pour tâche d'enlever les formules de politesse des lettres ou encore de reformuler les télégrammes afin de détruire d'éventuels messages cachés. [1]

Cependant, l'art du tatouage a été inventé en Chine depuis plus de mille ans pour tatouer le papier (papemarkirg). Mais, le plus ancien document tatoué dans les archives remonte à 1292 dans la ville de **Fabriano** en Italie qui a joué un rôle important dans l'évolution de l'industrie papetière. [2] Les tatouages se sont ensuite rapidement étendus en Italie et puis en Europe.

I.3. Définition général de La télémédecine :

La télémédecine est désormais considérée comme un acte médical à part entière. Il s'agit plus précisément, d'une forme de pratique médicale à distance en utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé. [3]

Figure I.2 Photo de télémédecine

I.3.1. Techniques de transmission utilisées en télémédecine :

Les techniques suivantes ne s'excluent pas mutuellement : une application ou un service de télémédecine peut en employer une seule ou toute combinaison des trois. [4]

I.3.1.a. Transmission audio :

La transmission audio est une application courante et bien connue, utilisée par exemple pour une consultation médicale entre un patient et son médecin, ou pour un échange d'avis entre deux médecins. L'idée est simple mais efficace, et pourrait être appliquée dans n'importe quelle région un tant soit peu équipée en téléphones.

I.3.1.b. Transmission de données :

La transmission de données permet d'acheminer des données médicales de type statique (dossier médical, matériel de formation...) ou dynamique (fonctions vitales telles que rythme cardiaque, pression sanguine...).

I.3.1.c. Transmission d'images :

La transmission d'images concerne les images fixes (radiographies, etc.) ou animées (vidéo, etc.) qui ont des fins de consultation, d'interprétation diagnostique ou de visioconférence. Les plus couramment échangées dans la pratique actuelle de la télémédecine

sont les images radiologiques, qui comprennent les différents types, l'image produite est analogique mais doit être numérisée pour une transmission efficace. [4]

I.3.2. Avantages et inconvénient de la télémédecine :

I.3.2.a. Avantages :

- Influx sur le développement de la volonté politique, professionnelle et industrielle et Facilite la collaboration et améliore les différents réseaux de soins en incitant la bonne volonté.
- Permet accès à des compétences sortant du cadre de connaissances de son médecin et a voir plusieurs avis en même temps et en temps réel avec formation continue des médecins.
- Évite les déplacements inutiles et élimine la redondance des actes et des examens avec un meilleur control de dépenses.
- La télémédecine trouve une solution pour les pays sous-développés. [5]

I.3.2.b. Inconvénients :

- Hétérogénéité des besoins ; Budget disponible, Spécialisation du médecin, Préférences d'interfaces
- Problèmes d'infrastructure aux niveaux gouvernementaux ; Equiper les villes de réseaux, Subvention d'équipements
- Problèmes habituels des nouvelles technologies, Scepticisme quant à son intérêt et son utilité, Le manque de volonté de
- Changer de médecins, Beaucoup de questions juridiques et éthiques. [5]

I.4. Techniques de protection des données numérique :

I.4.1. Cryptographie, Stéganographie et Tatouage :

La cryptographie, la stéganographie et le Tatouage sont des techniques qui traitent de la protection et de la sécurisation de l'information, mais leurs premiers objectifs sont différents. Ce besoin de sécurisation est motivé par des problèmes de confidentialité et d'intégrité. Bien que la cryptographie et la stéganographie, qui font partie des sciences du secret, ont été utilisées avant le commencement de notre ère à des fins militaires et diplomatique,

le tatouage est un domaine qui a émergé récemment et qui s'apparente beaucoup plus à la stéganographie. L'objectif de cette section est de passer en revue ces différents domaines en précisant les similitudes et complémentarités.

I.4.2. La cryptographie :

Il s'agit d'une technique de conversion de texte brut en texte chiffré. Il est possible de crypter des données hautement sécurisées en appliquant une approche de cryptographie. Cette approche permet de convertir les données de manière à ce qu'elles ne puissent pas être comprises. Seul l'utilisateur autorisé peut décrypter les données cryptées. [6]

I.4.3. La stéganographie :

C'est une technique très ancienne. Elle a pour but de cacher, au sein d'un médium une information secondaire. Ce message invisible doit être uniquement accessible à des personnes propriétaires d'une information secrète, c'est-à-dire des initiés. La nature de l'information dissimulée ne revêt pas d'importance ; il peut s'agir d'un texte en clair ou de sa version chiffrée. L'enjeu est donc d'éviter que des adversaires, appelés aussi attaquants, détectent la présence d'une information camouflée dans un support d'apparence anodine. L'objet de la stéganographie est donc de faire passer inaperçu un message dans un autre, et non de rendre un message uniquement intelligible à qui-de-droit ce qui est le rôle de la cryptographie. [7]

La différence entre la cryptographie et la stéganographie peut se résumer ainsi : l'une est une écriture secrète mais nue, alors -que l'autre est une écriture discrète : elle nécessite une couverture, un contenu. En d'autres termes, avec la cryptographie ancienne, la sécurité repose sur le fait que le message est incompréhensible, pour la stéganographie, la sécurité repose sur la remise en question même de l'existence du message. Mais rien n'interdit de cacher un message préalablement crypté. Les deux disciplines n'ont jamais été concurrentes, mais sont plutôt complémentaires.

La stéganographie a aujourd'hui pris un autre sens. Une définition plus appropriée pourrait consister à assurer la dissimulation d'une information dans un flux de données numériques, tel qu'un fichier numérique image ou son. Ce type de fichiers est habituellement considéré comme inoffensif, incapable de contenir des informations autres que celles normalement prévues.

Figure I.3 system de stéganographie

I.4.4. Le tatouage numérique :

Le tatouage (appelé aussi filigrane en anglais watermark) est une technique qui trouve ces origines dans le marquage des documents papier et des billets. Cette technique a longtemps servi comme preuve d'originalité et d'un mécanisme pour prévenir la contrefaçon. En effet, on peut trouver les premiers filigranes sur des papiers du treizième siècle, dans le but de garantir leur qualité. Sur un billet de banque, les fibres sont marquées au moment de la sortie du bain d'eau, ce qui est à l'origine du terme anglais « *watermark* ».

I.5. Tatouage numérique :

I.5.1. Pourquoi le tatouage numérique est-il nécessaire ?

• Pour la protection des droits d'auteur du contenu original.

• Pour éviter la contrefaçon.

• Pour la sécurité du contenu original.

• Pour revendiquer la propriété.

• Il aide le propriétaire à identifier si ses données multimédias sont volées par d'autres ou pas spécifiquement à partir de sites de médias sociaux.

I.5.2. Types du Tatouage numérique :

I.5.2.a. Tatouage d'image :

Le tatouage d'image numérique est la technique dans laquelle filigrane va être intégré dans une image. Il existe diverses approches pour cette méthode. Il peut être divisé sur la base du domaine ou de la transformation ou sur la base d'ondelettes. [8] Dans la technique du domaine spatial, le travail est directement été fait sur les pixels et le domaine fréquentiel fonctionne sur la base de coefficient de transformation. Utilisation de la propriété du système visuel humain (HVS) et les données d'image sont ajoutées de manière imperceptible.

I.5.2.b. Tatouage de texte :

Dans ce type de technique de tatouage, des données sont ajoutées à tous les documents texte tels que PDF, DOC, etc. Un tatouage peut être ajouté dans une telle façon qu'il porte le message secret afin que le droit d'auteur puisse être facilement reconnu. [9]

I.5.2.c. Tatouage d'audio :

En raison de la popularité de la musique chez les jeunes, il peut y avoir un risque de contrefaçon énorme dans la musique protégée par le droit d'auteur. Pour éviter ce tatouage audio est un problème brûlant pour les chercheurs. Dans cette technique, le tatouage peut être intégré dans le domaine temporel ou fréquentiel de telle manière qu'il n'affectera pas la l'audibilité de l'audio. [9]

I.5.2.d. Tatouage de vidéo :

La diffusion illicite de films est un phénomène typique et énorme risque pour l'industrie cinématographique. Avec l'avènement de l'accès rapide à Internet à large bande, un le duplicata volé d'une vidéo numérique pourrait désormais être transmis efficacement à un rassemblement mondial de personnes.

I.5.3. Définition du tatouage numérique :

Le tatouage numérique (en anglais digital watermark, « tatouage numérique ») est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement

message, un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme désignateur décrivant le signal hôte. Le nom de cette technique provient du masquage des documents papier et des billets. [10]

I.6. Propriétés du tatouage numérique :

I.6.1. L'inaudibilité du tatouage :

L'information tatouée ne doit pas dégrader perceptuellement le signal audio dans lequel elle est insérée ; son insertion doit être transparente. [11]

I.6.2. Le débit et la fiabilité de transmission :

La vocation du système étant de transmettre une information via un signal audio, elle doit permettre au même titre que les chaînes de communication classiques une fiabilité de transmission aussi élevée que possible pour un débit de transmission aussi grand que possible.[11]

I.6.3. Imperceptibilité :

Est indispensable que le tatouage soit invisible pour ne pas dégrader la qualité du document support. Cette contrainte implique notamment que l'énergie du tatouage soit suffisamment faible comparée à l'énergie des données hôtes. La plupart des systèmes de tatouage utilisent un modèle psycho perceptif afin d'accroître l'énergie du tatouage sans en augmenter l'intrusivité. [12]

I.6.4. La robustesse :

Transmettre une information cachée dans le signal audio suppose que le système mis en œuvre soit robuste aux perturbations introduites par l'ensemble des canaux de diffusion au travers desquels le signal audio peut être véhiculé : la fiabilité de transmission doit être maintenue si une dégradation affecte le signal audio tatouée. Contrairement au tatouage de protection, ces perturbations sont exemptes de la notion de pirate. L'information tatouée ayant vocation d'augmenter le contenu à destination de l'utilisateur ou d'une application cible, un pirate n'aurait rien à gagnerà empêcher sa détection. Les perturbations à envisager correspondent donc à l'ensemble des dégradations licites qui peuvent être effectuées sur un

signal audio lors de sa production en studio ou lors de son transfert dans un réseau de diffusion. [13]

I.6.5. La capacité d'insertion :

C'est à dire la quantité maximale d'information pouvant être transmise pour une probabilité d'erreur quasi nulle. Le débit d'insertion exigé par le système de tatouage est fortement dépendant de l'application envisagée, il convient de choisir un système de tatouage permettant une capacité d'insertion la plus grande possible. [11]

I.6.6. Sécurité :

Un tatouage est considéré comme sûr s'il est capable de lutter contre les attaques de sabotage intentionnelles. Va inclure Sécurité exceptionnelle même lorsqu'un attaquant connaît le processus d'inclusion et d'extraction d'un fichier tatouage. La force de la sécurité du tatouage est déterminée en fonction de la clé. Supposer Scénario suivant : Le pirate attaque le tatouage en le supprimant de l'image avec le tatouage Et essayez d'inclure un faux tatouage. Si la clé utilisée est sécurisée, le système est considéré comme sécurisé L'intrus sera refusé. L'aspect sécurité est différent de l'aspect durabilité. Le La durabilité consiste à survivre aux attaques courantes de traitement du signal. Mais la sécurité c'est la survie modification nuisible. Certaines applications veulent être sécurisées tandis que d'autres ne le font pas. [14] Cette propriété est souhaitable dans les applications de sécurité multimédia, d'identification propriétaire, Battements de cœur, télémédecine ou partage de sons médicaux.

I.6.7La détection du tatouage aveugle :

La détection de l'information cachée doit être effectuée directement à partir du signal audio tatoué, sans avoir connaissance du signal audio original. [11]

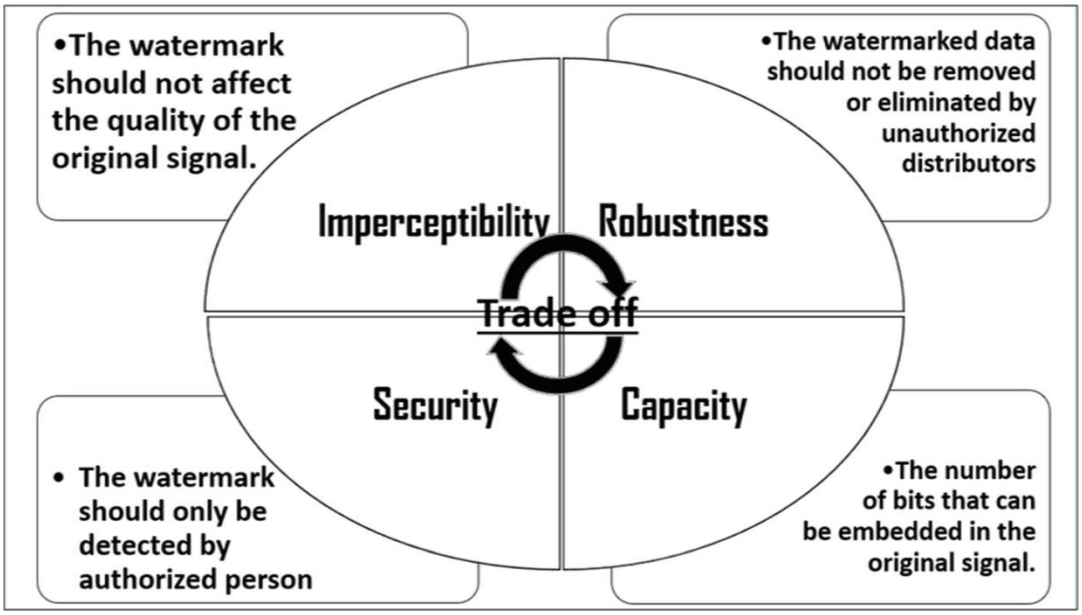


Figure I.4 Propriétés du tatouage numérique

I.7. Différents types d'attaques :

Les nécessités vitales d'un algorithme de tatouage performant sont la robustesse et inaudibilité. Il y a un échange entre ces deux nécessités; en tout cas, par tester l'algorithme de tatouage avec le traitement du signal audio attaque ce trou peut être rendu insignifiant. Chaque application a ses prérequis particuliers et donne une alternative pour choisir le remboursement à haute résistance avec la nature du signal et l'inverse. Sans changements ni assauts, chaque méthode de tatouage fonctionne de manière productive.Probablement les types de procédures les plus largement reconnus les expériences d'un signal audio lorsqu'elles sont transmises via un support sont conformes aux Suivant :

I.7.1. Bruit :

Il est normal de voir la proximité du bruit dans un signal lorsqu'il est transmis. Dorénavant, l'algorithme de tatouage devrait rendre le système solide contre les assauts de commotion. Il est prescrit de vérifier le calcul de ce type de bruit en incluant le signal hôte par un bruit gaussien blanc additif (AWGN) pour vérifier sa robustesse. [15]

I.7.2. Attaque de recadrage :

Le recadrage est une autre technique qui pourrait être utilisée par un ennemi pour modifier la proportion de perspective sans étendre le signal ni remplir les espaces dégagés. Un assaut d'édition peut influencer le tatouage avec peu de changements dans l'audio de la couverture. Cela repose sur la stratégie du filigrane et sa puissance. Le recadrage peut être exécuté sur une partie du signal d'origine. [15]

I.7.3. Dynamique :

Le changement d'amplitude et le changement d'atténuation sont les progressions des assauts. La capacité, l'expansion et la compression sont un type d'applications plus alambiquées qui sont les ajustements non directs. Une partie de ces types d'agressions est une requantification. [16]

I.7.4. Amplifier :

L'audio en tatouage est intensifié à divers taux d'amélioration. A travers cet assaut, les plans de tatouage qui installent le tatouage dans l'adéquation de la des exemples individuels finissent par être impuissants lorsque l'amplitude est ajustée.

I.7.5. Filtrage :

Le filtrage est une pratique courante, qui est utilisée pour amplifier ou atténuer une partie du signal. Les filtres passe-bas et passe-haut de base peuvent être utilisés pour réaliser ces types d'attaques. [16]

I.7.6. Ajout de l'écho :

Des échos avec divers reports sont ajoutés aux audio en tatouage. Cet assaut est fondamentalement le compteur des complots d'ajout d'écho qui incluent le bit de tatouage sous forme d'échos avec divers reports.

I.7.7. Ambiance :

Dans quelques circonstances, le signal audio est différé ou il existe des circonstances dans lesquelles le mouvement d'enregistrement d'un individu à partir d'une source et prétend que la

piste est les leurs. Ces circonstances peuvent être reproduites dans une pièce, ce qui est d'une importance incroyable pour vérifier l'exécution d'un signal audio. [16]

I.7.8. Attaque de retrait :

Les attaques de suppression s'attendent à expulser les informations de tatouage du signal audio tatouage. De telles attaques abusent de la façon dont le tatouage est généralement un signal de bruit additif ajouté introduit dans le signal hôte [16].

I.8. Utilisation du tatouage numérique :

Le tatouage numérique peut être utilisé pour un large éventail d'applications, telles que :

- Protection des droits d'auteur.
- Suivi de la source (différents destinataires reçoivent un contenu tatoué différent).
- Surveillance de la diffusion (les journaux télévisés contiennent souvent des vidéos en tatouage provenant d'agences internationales).
- Authentification vidéo.
- Logiciel paralysant les logiciels de capture d'écran et de montage vidéo, pour encourager les utilisateurs à acheter la version complète pour la supprimer.
- Sécurité de la carte d'identité.
- Détection de fraude et de sabotage.
- Gestion de contenu sur les réseaux sociaux.

I.9. Conclusion :

Les tatouages de télémédecine concernent l'envoi des dossiers médicaux des patients, nous nous intéressons à notre travail de masquage des données dans les fichiers audio ; Connaître le son médical.

Dans ce chapitre, nous avons fourni un aperçu des tatouages et de leur historique, y compris leurs caractéristiques, applications, plate-forme et utilisations. Dans le chapitre suivant, nous fournirons un aperçu détaillé des tatouages numériques pour les fichiers audio.

Chapitre II Tatouage numérique des fichiers audio

Chapitre 2 : Tatouage numérique des fichiers audio

II.1. Introduction :

Le tatouage audio est utilisé pour la sécurité du signal audio comme la protection des droits d'auteur et l'authentification. Dans le tatouage audio, le tatouage est intégré dans un signal audio hôte de manière à ce que le contenu intégré ne soit pas identifié. Dans le même temps, le tatouage intégré doit être suffisamment robuste contre diverses attaques de tatouage audio. Ce chapitre présente les techniques fondamentales de tatouage audio.

II.2. Définition des fichiers audio :

Une boîte ou un conteneur similaire pour contenir et organiser des enregistrements sonores sur l'un des différents supports [17].

II.3. Le son :

Le son est une vibration qui traverse le milieu sous la forme d'ondes longitudinales. Cela signifie que les ondes sonores sont des ondes dans lesquelles les particules du milieu vibrent parallèlement à la direction de propagation des ondes. Les ondes sonores sont appelées ondes mécaniques car elles nécessitent un milieu pour se propager. Le milieu peut être solide, liquide ou gazeux [18].

II.4. Ondes sonores en médecine :

Dans le cas des soins prénatals pour les femmes enceintes, l'imagerie par ultrasons est utilisée pour suivre la croissance du fœtus. L'échographe émet une onde sonore à haute fréquence qui est réfléchie par différents tissus à l'intérieur du corps. La densité du tissu affecte la façon dont l'onde rebondit, et l'échographe a été spécifiquement programmé pour lire ces différences afin de créer une image.

L'échographie est importante pour la médecine car elle peut être utilisée à des fins diagnostiques et thérapeutiques. Des ondes sonores focalisées peuvent être utilisées pour nettoyer vos dents, pour briser un nuage.

Figure II.1. Photo: Source : Bébé en écho, Sam Polara, WikimediaCommons.graphie

II.5. Propriétés du son :

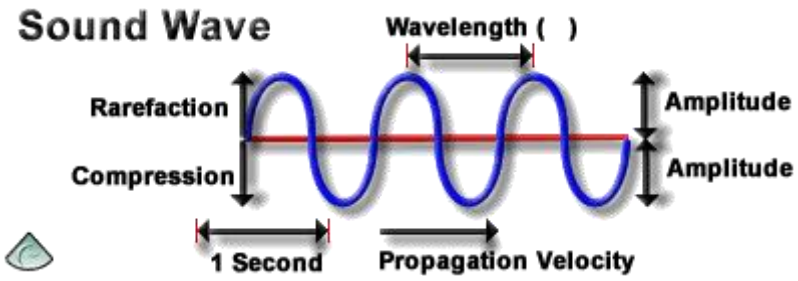


Figure II.2. Propriétés des ondes sonores.

II.5.1. L'amplitude :

Est la hauteur de l'onde sonore et est mesurée en décibels (dB). Au fur et à mesure que l'onde sonore augmente en amplitude, le milieu se dilate (raréfaction). A l'inverse, lorsque l'onde sonore diminue en amplitude.

Un décibel est le logarithme d'un rapport entre la pression acoustique (V) et une valeur de référence (R) multiplié par 20. R est généralement égal à 1 (un).

DB = 20 * log (V / R)

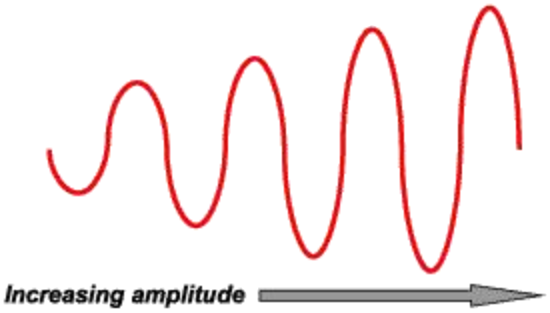


Figure II.3 L'amplitude.

II.5.2. La fréquence :

La fréquence est le nombre périodique de cycles de compression et de vide qui se produisent chaque seconde lorsque l'onde se propage à travers le milieu. Les ondes ultrasonores sont supérieures à 20 000 Hz, Les ultrasons médicaux sont généralement de 1 à 20 mégahertz, ou mégahertz. [19]

f = cycles / sec

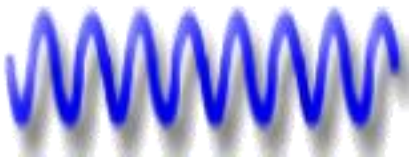


Figure II.4. Basses fréquences.

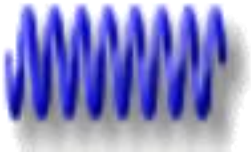


Figure II.5. Haute fréquence.

II.5.3. La longueur d'onde :

Est la longueur d'un cycle d'onde (c'est-à-dire d'un pic à l'autre) qui comprend une raréfaction et une compression et est mesurée en millimètres (mm),Il est généralement représenté par le symbole λ.

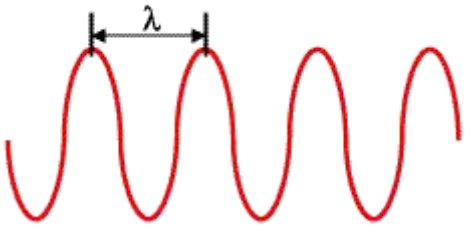


Figure II.6. La longueur d'onde.

II.6. Formats audio numériques :

Il existe une grande variété de formats numériques, cela est principalement dû aux différentes plates-formes de lecture existantes, ci-dessous certains des formats les plus utilisés vont être détaillés.

Figure II.7. Format Audio Numérique.

II.6.1. Format WMA 

Le format WMA (Windows Media Audio) développé par Microsoft. L'une des caractéristiques les plus importantes de ce type de format est que les fichiers portant

l'extension ".wma"ont tendance à être beaucoup plus petits en espace disque que même les mp3. L'inconvénient de ce type de format est la perte de qualité audio, car lorsque le fichier audio est compressé, la qualité sonore est affectée. [20].

II.6.2. Format MP3 

Le format MP3 est l'un des plus populaires car les fichiers avec l'extension .mp3 occupent très peu d'espace sur le disque dur. Par exemple, si vous pouvez stocker 10 fichiers avec l'extension ".wav" sur un CD, les fichiers avec le format ".mp3" peut stocker 100 fichiers sur le même CD. La raison pour laquelle ce type de format est si largement utilisé est qu'il élimine la gamme de fréquences que l'oreille humaine n'entend pas[20].

II.6.3. Format AAC 

Ce type de format est utilisé par **Apple** à travers son logiciel **iTunes**, qui a presque les mêmes caractéristiques que ".mp3", c'est-à-dire qu'il est basé sur l'élimination de la gamme de fréquences que l'oreille humaine n'entend pas, mais avec Ce type de format offre une meilleure qualité audio et moins d'espace disque occupé [20].

II.6.4. Format WAV 

Le format WAV (Wave forme Audio File) a été développé par Microsoft et IBM, c'est l'un des formats audio numériques actuels avec une excellente qualité car il n'a aucun type de compression de données, ce type de fichier est utilisé dans l'exploitation systèmes comme Windows pour les sons de votre propre système, ceux-ci sont entendus lors de la mise sous tension et hors tension des ordinateurs [20].

II.7. Définition du tatouage audionumérique :

Le système de tatouage peut être vu comme une chaîne de communication bruitée. En effet, le tatouage est le signal à transmettre et le signal audio est considéré comme un bruit. Le

tatouage audio (ou audio Watermark en anglais) est l'art de cacher de l'information directement dans des données multimédia de façon robuste et imperceptible. Dans le contexte des signaux audio, le tatouage met à profit les imperfections du système auditif humain pour garantir l'audibilité du message inséré. L'utilisation du tatouage audio comme canal auxiliaire de transmission pour véhiculer des informations supplémentaires. Ces informations peuvent être destinées à l'auditeur [21].

II.8. Classification du tatouage :

La classification du tatouage peut se faire en fonction de diverses caractéristiques tels que le type de données d'entrée, le domaine de traitement et les applications utilisées. Illustration 12 montre la classification du tatouage [22–40].

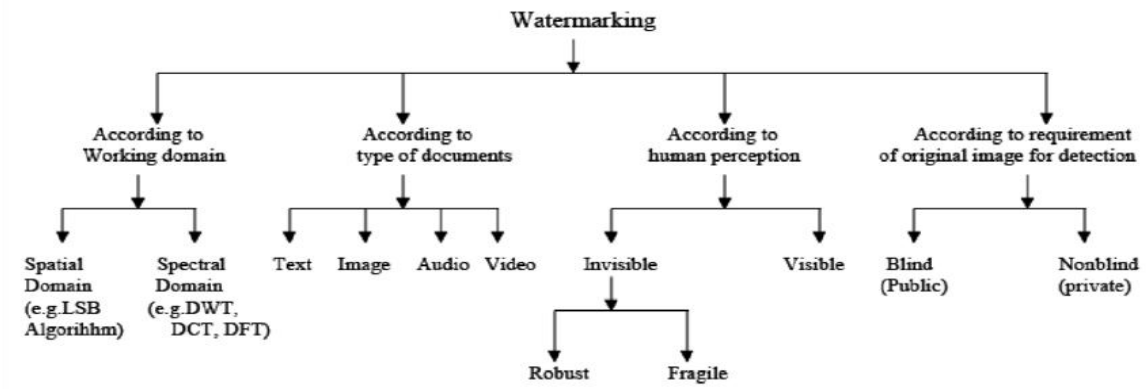


Figure II.8. Classification du tatouage numérique

II.8.1. Tatouage visible et invisible :

II.8.1.a Tatouage invisible :

Dans cette méthode, marque les intégrations dans les informations de l'hôte dans de telle sorte qu'il ne puisse pas être visible ou détecté par l'utilisateur commun.

II.8.1.b Tatouage visible :

Dans cette méthode, marque les intégrations dans les informations de l'hôte dans de manière à ce qu'il puisse être visible ou détecté par l'utilisateur commun.

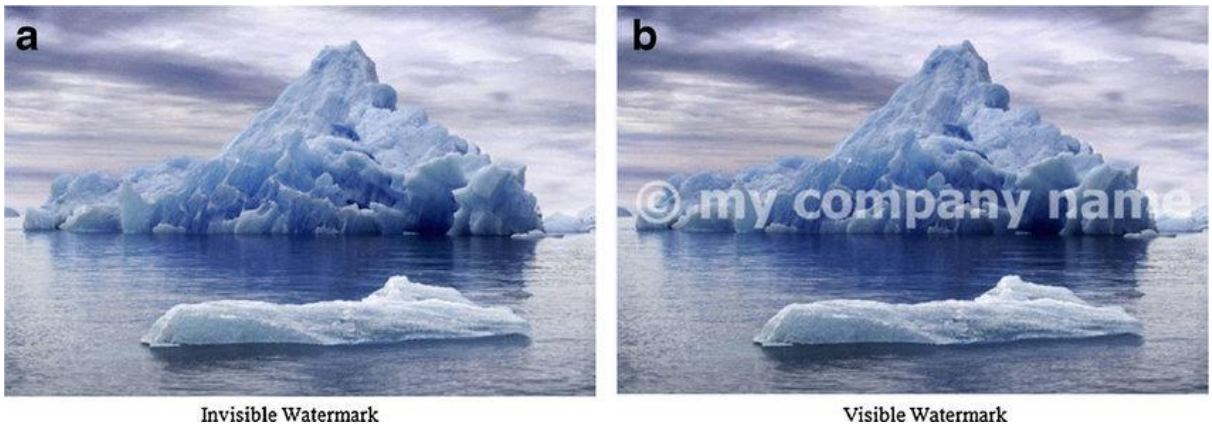


Figure II.9. Image de tatouage visible et invisible

II.8.2. Fragile, Semi-fragile et Robuste :

II.8.2.a. Le tatouage robuste :

Le tatouage robuste est conçu dans le but de protéger des documents. Il doit résister au maximum d'attaques et permettre la compression du signal audio hôte tout en préservant la signature.

II.8.2.b. Le tatouage semi-fragile :

Le tatouage semi-fragile a pour objectif de reconnaître les perturbations mal intentionnées et de rester robuste à certaines classes de dégradations légères de signal audio, comme le ré-quantification et le ré-échantillonnage. Leurs applications sont surtout réservées à l'authentification des signaux audio.

II.8.2.c. Le tatouage fragile :

Le tatouage fragile est conçu pour détecter les changements survenus sur un signal audio. Il ne doit pas résister à une modification du contenu du signal audio hôte. Ce type de tatouage sert à prouver l'authenticité et l'intégrité d'un fichier tatoué.

II.8.3. Tatouage aveugle, Tatouage semi-aveugle, Non aveugle :

II.8.3.a. Filigrane aveugle :

Ce type de système nécessite uniquement les données tatouages pour extraire le tatouage. Pour cette raison, il est le plus difficile à développer [33, 34, 35, 36].

II.8.3.b. Filigrane semi-aveugle :

Il n'utilise pas les données d'origine mais seulement la copie du tatouage et des réponses Qu'il soit présentes ou non [33, 37, 36].

II.8.3.c. Non aveugle :

Un schéma de tatouage non aveugle nécessite la couverture d'origine. Il ne peut être utilisé que dans les applications où les travaux d'origine sont disponibles (Watermark privées applications). Le non-dit ou semi-léger peut être utilisé pour des éléments de preuve devant les tribunaux pour prouver la propriété, le contrôle de la copie ou les empreintes digitales (où le propriétaire devrait encore avoir un Version marquée par l'œuvre) [33, 38, 39]

II.9. Le domaine d'insertion :

II.9.1. Le domaine spatial :

Les techniques de tatouage modifiant directement la valeur des échantillons du signal audio sont naturellement des schémas qui viennent à l'esprit en premier lieu et qui sont faciles mettre en œuvre[40] . Les opérations d'insertion et de détection sont alors peu coûteuses en temps de calcul ; elles peuvent être alors utilisées afin d'effectuer un tatouage en temps réel. Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB (Least Significant Bit) du signal hôte. L'inaudibilité de la marque est obtenue par l'hypothèse que les données contenues dans les bits LSB sont auditivement insignifiantes. [41]

II.9.2. Le domaine fréquentiel :

Des schémas du tatouage peuvent effectuer l'insertion de la marque dans des espaces transformés. Un espace transformé est obtenu après l'emploi d'une transformée telle que : DCT, DST, DFT, DWT, etc. Les schémas qui utilisent le domaine fréquentiel comme domaine d'insertion peuvent être davantage robustes face aux opérations de compression puisqu'ils utilisent le même espace que celui qui sert au codage du signal audio. D'autre part, grâce aux algorithmes de transformations rapides, le calcul de la transformée d'un signal est devenu peu coûteux.[42]

II.10. Application du tatouage numérique :

Il existe un certain nombre de systèmes de tatouage développés sur la base de différentes applications. Ces dernières années, certaines nouvelles applications de tatouage audio ont été découvertes. Par exemple, l'algorithme de filigrane audio a été conçu pour l'audio et évaluation de la qualité de la parole. Dans cette section, nous énumérons six applications principales de tatouage audio : protection des droits d'auteur, protection contre la copie, authentification du contenu, diffusion Surveillance, prise d'empreintes digitales et sténographie.

II.10.1. Protection des droits d'auteur :

L'une des motivations de l'introduction du filigrane audio est la protection du droit d'auteur. L'idée est d'intégrer des informations sur le droit d'auteur ou le(s) propriétaire(s) dans les données pour empêcher d'autres parties de prétendre être le(s) propriétaire(s) légitime(s) des données.

II.10.2. Protection contre la copie :

Cette application est utilisée pour empêcher les copies illégales de CD enregistrables, enregistrables DVD ou toute autre technologie d'enregistrement numérique. Un tatouage est intégré dans le contenu.

II.10.3. Authentification du contenu :

Des tatouages tatouage peuvent être utilisés pour vérifier l'authenticité des données. Une fragilité le tatouage indique si les données ont été modifiées et fournit la localisation des informations sur l'endroit où les données ont été modifiées. Dans l'authentification de contenu, les informations de signature sont intégrées dans la source, et plus tard sont utilisées pour vérifier sille contenu a été altéré ou non.

II.10.4. Surveillance de diffusion :

Dans l'émission audio, sur l'annonceur dans l'émission télévisée pour lequel ils paient. Les propriétaires de logiciels de publication doivent savoir les que linéal. Surveillance de la diffusion de la liste des marques. Dans cette application, programme ou publicité Surveillez-le intégré avec un tatouage avant de diffuser.

II.10.5. Empreintes digitales :

Pour retracer la source des copies illégales, le propriétaire peut utiliser la technologie des empreintes digitales. Dans ce cas, le propriétaire peut inclure différents tatouage s dans les données qui Il est fourni à différents clients.

II.10.6. Applications médicales :

Plus récemment, des algorithmes de tatouage numérique sont utilisés pour sécuriser et authentifier les données médicales lors de leurs déplacements d'une station à l'autre en télémédecine.

II.10.7. Audio Stéganographie :

L'objectif principal de la stéganographie est de communiquer en toute sécurité de manière totalement indétectable[43] et pour éviter tout soupçon à la transmission d'une donnée cachée [44]. Il ne s'agit pas seulement d'empêcher les autres de connaître l'information cachée, mais cela empêche également les autres de penser que le l'information existe même. Si une méthode de sténographie amène quelqu'un à soupçonner qu'il y a une secrète information sur un support, alors la méthode a échoué [45,46].

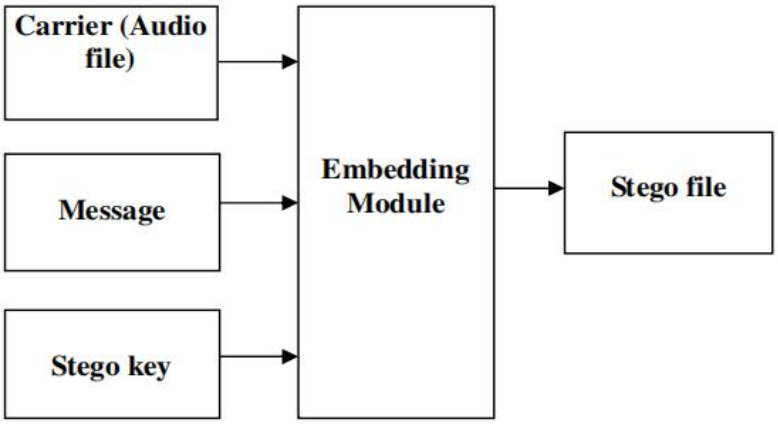


Figure II.10. Modèle audio sténographique de base

Le processus de masquage d'informations consiste à suivre deux étapes :

Identification des bits redondants dans un fichier de couverture. Les bits redondants sont les bits qui peuvent être modifié sans altérer la qualité ni détruire l'intégrité du fichier de couverture.

Pour intégrer les informations secrètes dans le fichier de couverture, les bits redondants dans le fichier de couverture sont remplacés par les bits de l'information secrète.

II.11. Techniques existantes de tatouage audio dans le Domaine spatial :

Il existe de nombreuses techniques pour cacher des informations ou des messages dans l'audio de telle manière que les modifications apportées au fichier audio soient perceptuellement indiscernables. Les approches courantes incluent [47, 48,49].

II.11.1. Codage LSB :

Une méthodologie très populaire est l'algorithme LSB (Least Significant Bit), qui remplace le bit le moins significatif dans certains octets du fichier de couverture pour masquer une séquence d'octets contenant les données cachées. C'est généralement une technique efficace dans les cas où la substitution LSB ne fonctionne pas entraîné une dégradation significative de la qualité.

En informatique, le bit le moins significatif (LSB) est la position du bit dans un entier binaire donnant les unités valeur, c'est-à-dire déterminerai le nombre est pair ou impair. Le LSB est parfois appelé comme le bit le plus à droite, en raison de la convention de notation positionnelle d'écrire le chiffre le moins significatif plus à droite. Il est analogique au chiffre le moins significatif d'un entier décimal, qui est le chiffre dans la position des unités (la plus à droite).

Figure II.11. Représentation binaire du nombre décimal 149

La représentation binaire de la décimale 149, avec le LSB en surbrillance. Le MSB dans un binaire 8 bits nombre représente une valeur de 128 décimal. Le LSB représente une valeur de 1. Par exemple, pour masquera lettre "a" (code ASCII 97, qui est 01100001) à l'intérieur de huit octets d'une couverture, vous pouvez définir le LSB de chaque octet comme ceci :

1001001**0**

0101001**1**

1001101**1**

1101001**0**

1000101**0**

0000001**0**

0111001**0**

0010101**1**

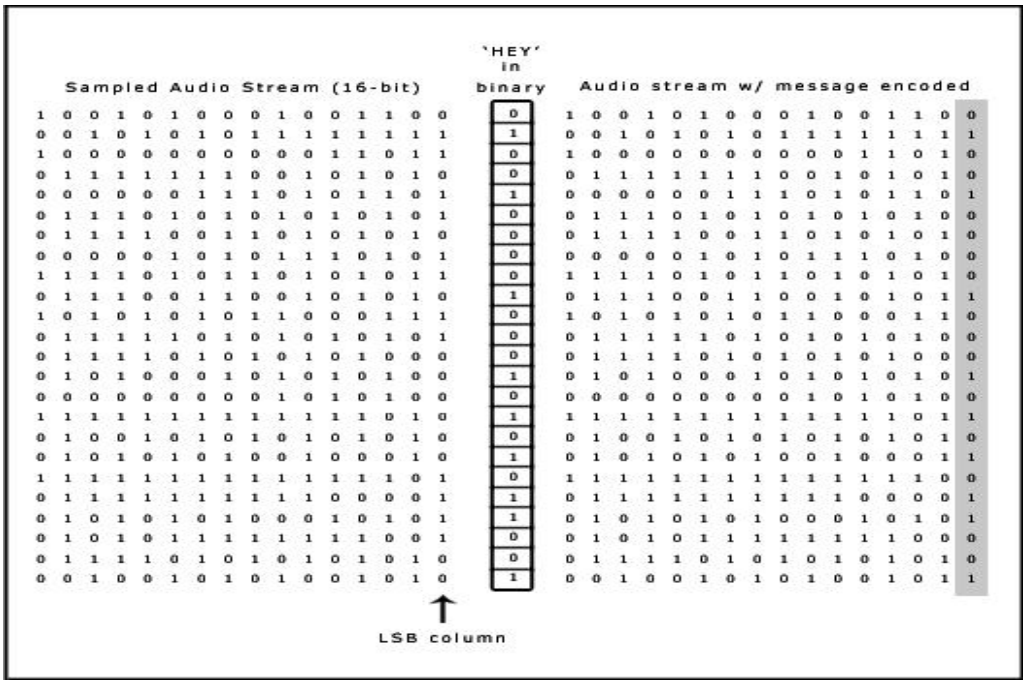


Figure II.12. Exemple de codage LSB

II.11.2. Technique de patchwork :

La technique du patchwork est le modèle statistique de masquage d'informations basé sur le pseudo-aléatoire. Les informations tatouées sont divisées en deux sous-ensembles de manière aléatoire.

II.11.3. Cacher l'écho :

La méthode de masquage d'écho couvre les informations et les insère dans un signal audio unique en présentant un écho dans le domaine temporel avec pour objectif final la simplicité.

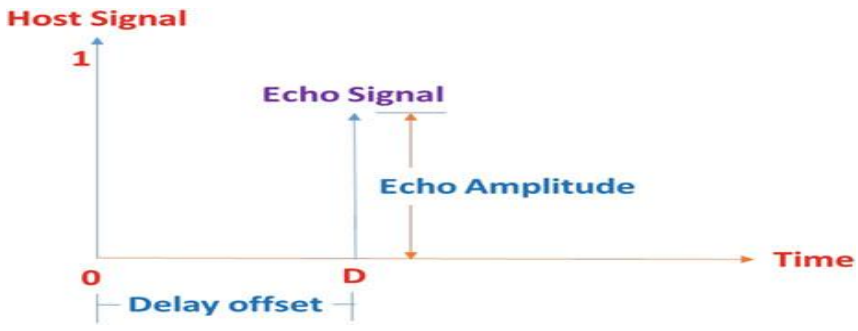


Figure II.13. Schéma Cacher l'écho de tatouage (Katzenbeisser and Petit colas 2000).

II.12. Conclusion :

Dans ce chapitre, nous avons donné un aperçu détaillé des marques d'eau numériques dans les fichiers audio, nous avons également fourni une classification des techniques de filigrane selon différentes normes et bases sonores, où nous avons caché les donnée (LSB). Chaque catégorie de technologies de filigrane a un objectif différent. Cependant, dans ce projet, nous nous concentrerons sur les techniques de l'impact et la puissante marque d'eau pour le son dans le domaine spatial. Ainsi, dans le chapitre suivant, nous fournirons l'interface d'application et la façon dont les opérations d'entrée et de sortie sont effectuées.

Chapitre III Conception et Réalisation

III.1. Introduction :

Les tatouages audio numériques sont la science et l'art d'intégrer un type particulier de données, comme une étiquette ou un message secret, dans le contenu audio numérique. Les informations intégrées sont ensuite extraites à l'extrémité réceptrice à diverses fins liées à la sécurité vocale. [50] Dans ce chapitre, nous présentons la conception et la réalisation, ainsi que les critères de performance pour une évaluation sonore Système de filigrane.

III.2. Environnement :

III.2.1. Langage :

Matlab :

Le logiciel «Matlab» constitue un système interactif et convivial de calcul numérique et de visualisation graphique. Destiné aux ingénieurs, aux techniciens et aux scientifiques, c'est un outil très utilisé, dans les universités comme dans le monde industriel, qui intègre des centaines de fonctions mathématiques et d'analyse numérique calcul matriciel (le MAT de Matlab), traitement de signal, traitement de fichiers audio, visualisations graphiques, etc. [51].

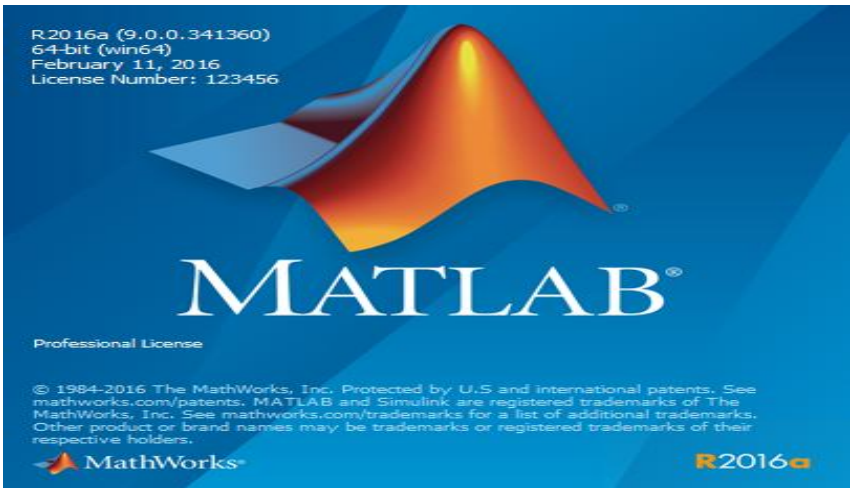


Figure III.1. L'environnement Matlab

III.2.2. Data set :

- Les bruits respiratoires sont des indicateurs importants de la santé respiratoire et des troubles respiratoires.Le son émis lorsqu'une personne respire est directement lié au mouvement de l'air, aux changements dans les tissus pulmonaires et à la position des sécrétions dans les poumons.Un sifflement, par exemple, est un signe courant qu'un patient souffre d'une maladie obstructive des voies respiratoires comme l'asthme ou la maladie pulmonaire obstructive chronique (MPOC).[52]
- Les bruits cardiaques sont les bruits émis par les battements du cœur et la circulation du sang dans celui-ci.Plus précisément, les sons reflètent les perturbations qui surviennent dans les valves cardiaques si elles se ferment soudainement.Le médecin peut généralement utiliser des stéthoscopes pour écouter ces sons uniques et distincts qui fournissent des données auditives importantes liées à l'état du cœur.
- La base de données des sons respiratoires a été créée par deux équipes de recherche au Portugal et en Grèce.Nous avons tiré d'eux 3 enregistrements de durées variables de 10 à 20 secondes.Ces enregistrements ont été effectués sur 3 patients présentant un cycle respiratoire ou une respiration sifflante, une respiration sifflante, une respiration sifflante et une respiration sifflante.Les données comprennent à la fois des sons de respiration propres et des enregistrements bruyants qui simulent des conditions réelles.[52]
- Une base de données de sons internes, tels que les battements cardiaques ou les artères, a été créée à la clinique du Dr **Othmani Ammar** (Touggourt). Nous avons pris 4 enregistrements de durées variables de 5 à 6 secondes, où il a effectué sur nous une expérience pour prendre des sons. de la main (des artères) et le son des battements du cœur (du cou).
- Ces sons peuvent être enregistrés à l'aide de haut-parleurs numériques et d'autres technologies d'enregistrement. Ces données numériques ouvrent la capacité d'utiliser l'apprentissage automatique pour le diagnostic automatique des troubles respiratoires et le rythme cardiaque tels que l'asthme, la pneumonie et la bronchite [52].

III.3.Méthode du tatouage :

III.3.1Création du tatouage :

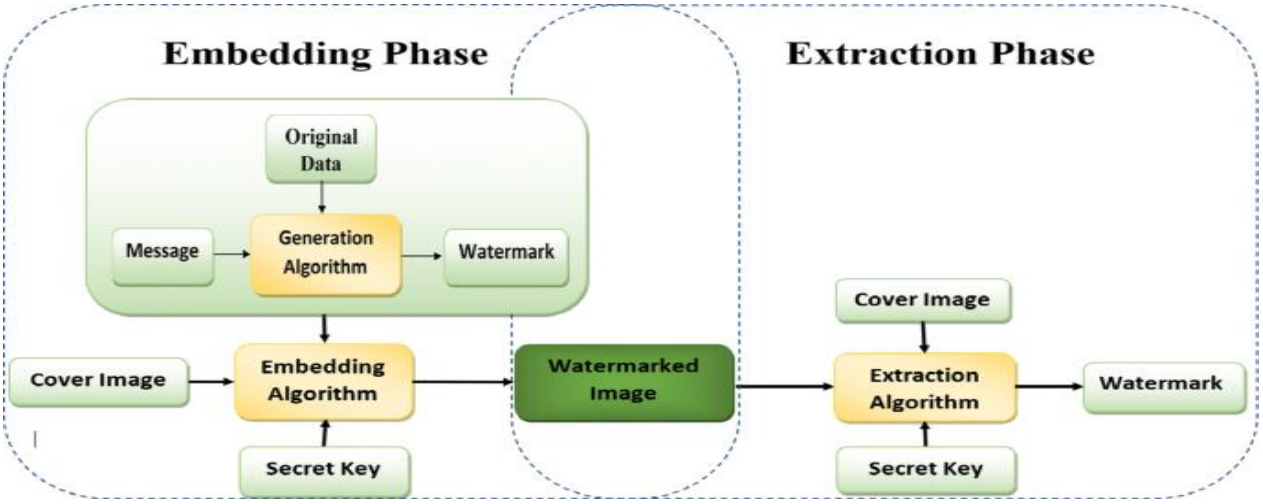


Figure III.2. Processus d'insertion et d'extraction

III.3.1.a Algorithme d'insertion :

Entrées :

Audio : Signal audio de taille n × m.

Texte : Le texte à insérer dans le signal audio.

Clé : Une clé pour crypter le texte du tatouage.

Sortie :

Ts: Signal audio tatouée.

Étapes :

Étape 1 : lire le signal audio, la marque de texte et la clé secrète.

Étape 2 : chiffrer la marque avec une clé secrète.

Étape 3 : Convertir la marque en binaire

Étape 4 : Insérez la marque dans Signal audio (appliquez la méthode LSB) :

Remplacez le bit le moins significatif de audio (i) par le bit de texte_T (i).

Étape 5 : enregistrez le nouveau signal audio avec le texte de la marque (Ts).

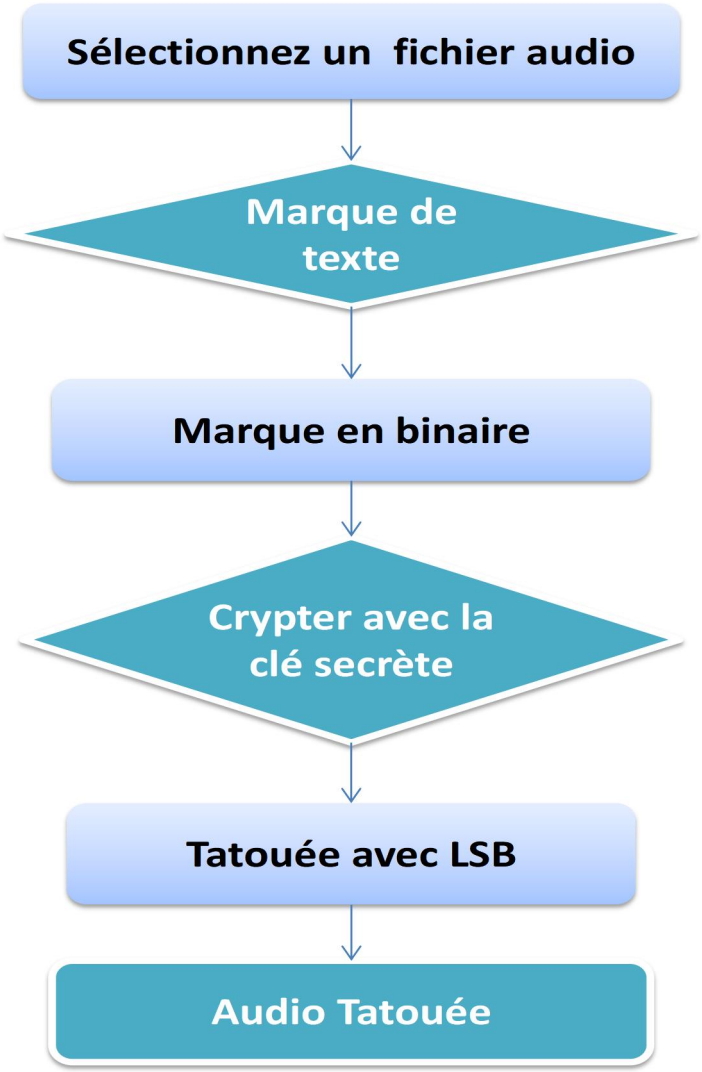


Figure III.3 schéma d'algorithme d'insertion LSB

III.3.1.b Algorithme d'extraction :

Entrées :

Audio : Signal audio de taille n × m.

Clé : Une même clé pour décrypter le texte du tatouage.

Sortie :

Tw : tatouage de texte.

Étapes :

Étape 1 : lire le signal filigrané et la même clé secrète.

Étape 2 : appliquer la méthode LSB inverse pour les données binaires Afin d'extraire le bit le moins significatif pour les données binaires, c'est-à-dire de représenter le bit à la marque de message.

Étape 3 : Convertissez la marque en binaire.

Étape 4 : décryptez le texte de la marque avec la même clé secrète.

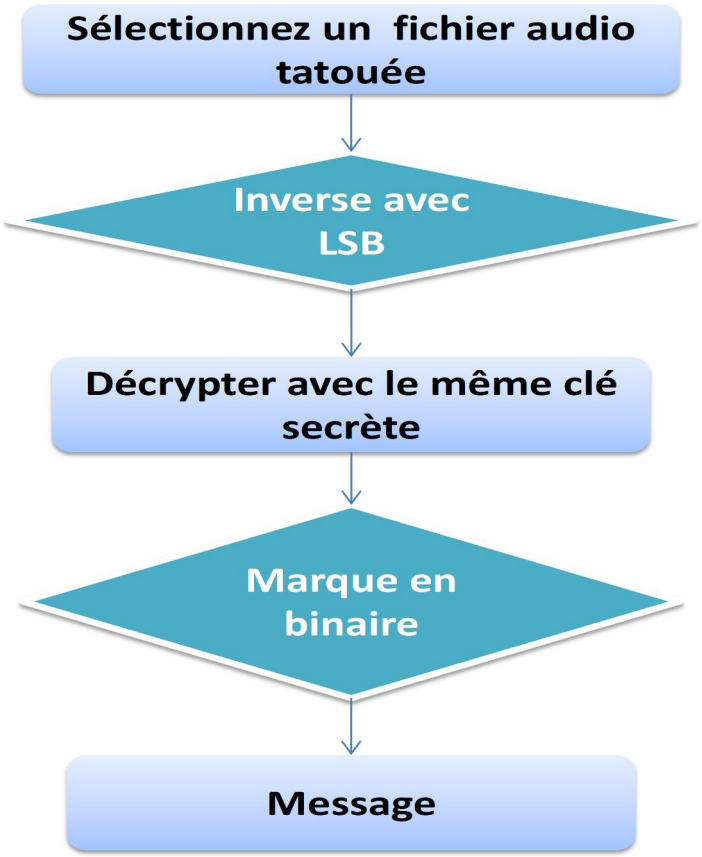


Figure III.4. Schéma d'algorithme d'extraction

III.3.2. Insertion du tatouage :

III.3.2.a. Phase d'insertion :

L'insertion de la marque originale W_o, dans le signal audio original X permet d'obtenir un signal audio tatoué noté $\tilde{X}$. Cependant, dans phase d'insertion, les systèmes de ta- touage utilisent en général une ou plusieurs clés cryptographiques sécrètes afin d'assurer une sécurité contre l'insertion ou l'extraction non-autorisée de la marque. Généralement, cette phase peut être divisée en deux étapes : la génération et l'insertion de la marque.

La génération de la marque : La marque numérique à insérer W générée à partir d'une marque original W_o et d'une clé de générationC_G utilisant une fonction de générationF_G. Dans la plupart des cas, la fonctionF_G, est une fonction cryptographique. La forme de la marque originale est diverse, elle peut être une image binaire ou niveaux de gris, un signal aléatoire, une 'suite de caractères ou simplement une séquence binaire ou bipolaire.

La fonction de génération s'exprime comme suit :

W =F_G.(W_o, C_G)

Probablement, la marque W peut également dépendre du signal original X dans le- quel elle est insérée

W = F_G (W_o ,X,C_G)

L'insertion de la marque : Le signal audio tatoué $\tilde{X}$et obtenu par l'insertion de la marque générée W dans le signal original X par une fonction d'insertion F_I. La fonction d'insertion s'exprime de la façon suivante :

$\tilde{X}$= F_I (T(X), W).

Une clé cryptographique d'insertionC_I, peut aussi être utilisée

$\tilde{X}$= F_I (T(X), W,C_I).

L'espace d'insertion T peut être le domaine temporel ou le résultat d'une transformation réversible fréquentielle ou Spectral. La fonction d'insertion de la marque F_I, peut être une fonction multiplicative ou substitutive. La fonction multiplicative insère la marque dans le signal original en la multipliant ou en l'ajoutant ou en la multipliant à ce dernier, tandis que dans la fonction substitutive, la marque à insérer n'est pas ajoutée mais plutôt substituée à des composantes du signal audio original.

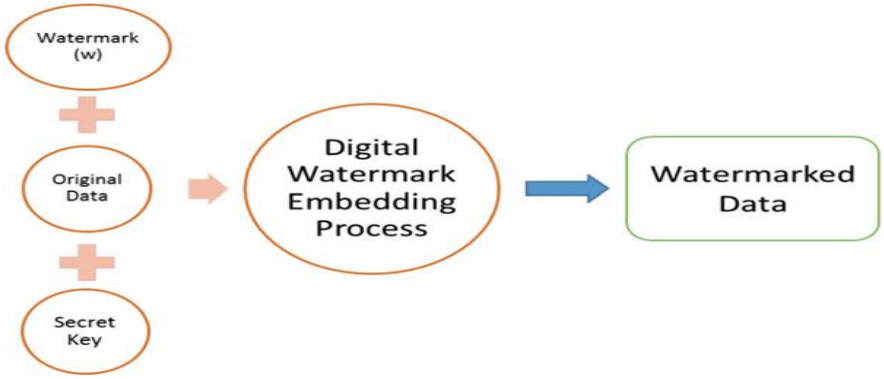


Figure III.5. Processus d'insertion du tatouage numérique.

III.3.3. Extraction du tatouage :

III.3.3.a. Phase d'extraction :

La phase de détection/extraction prend en entrée le signal audio tatoué et éventuelle- ment attaqué $\tilde{X}$et les clé $C_G$et C_I selon l'algorithme d'extraction, le signal audio original peut être ou non nécessaire lors de la détection. Si le signal audio original n'est pas utilisé, la détection est dite aveugle ou non-informée

$$\tilde{W}= F_E(\tilde{X},C_I)$$

Dans le cas contraire, la détection est dite non-aveugle ou informée

$$\tilde{W}= F_E(\tilde{X},X,C_I)$$

La marque originale est finalement récupérée à partir de la marque $\tilde{W}$ et de la clé C_G en utilisant la fonction de génération F_G inversée

$$\tilde{W}_O= {F_G}^{-1}(\tilde{W},C_G)$$

Généralement la robustesse des schémas informés est plus importante que dans les schémas aveugles. Le signal audio original fournit une référence pouvant servir à améliorer le processus de détection.

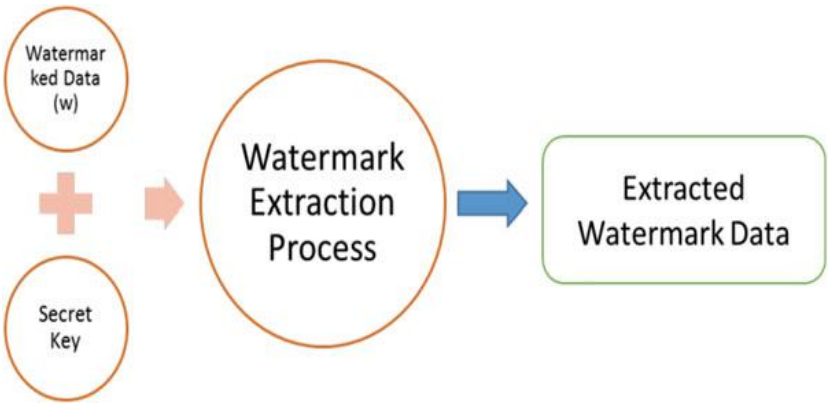


Figure III.6. Processus d'extraction du tatouage numérique.

III.4. Expérimentation et résultat :

III.4.1. Application (présentation) :

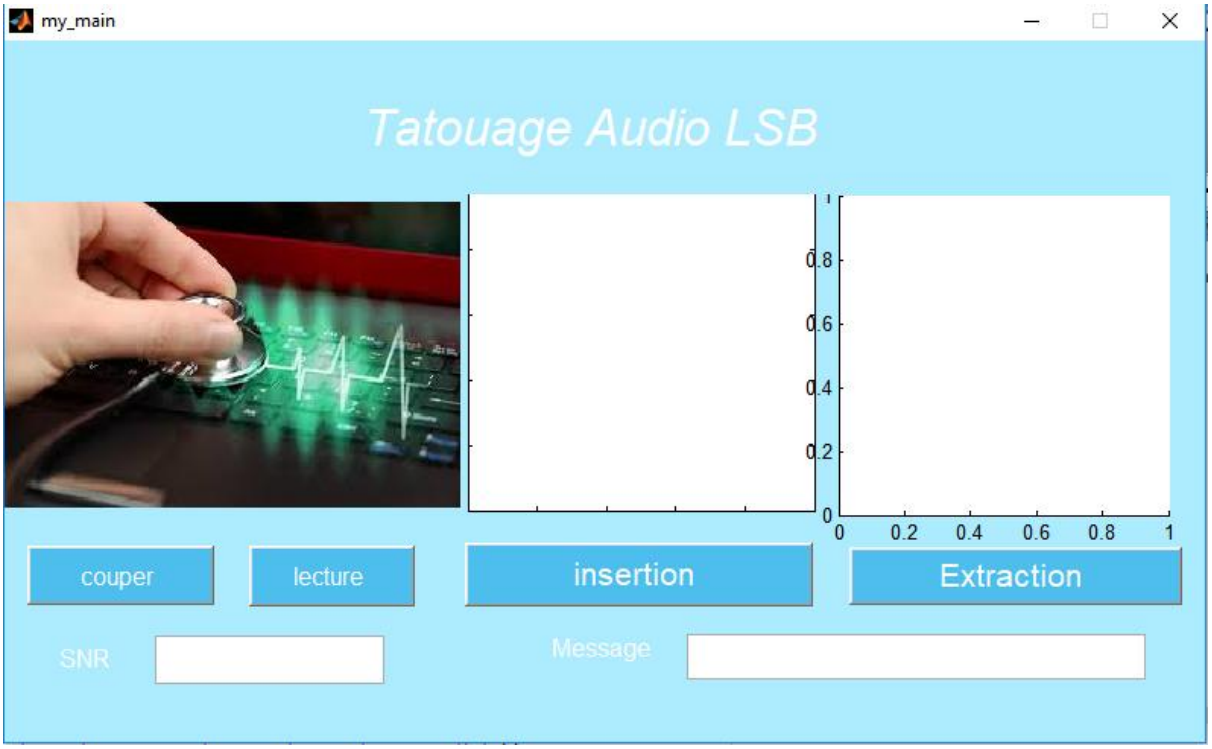


Figure III.7. Interface principal

III.4.1.a. Partie insertion :

Dans cette partie de l'application, nous appuyons sur le bouton « insertion » pour choisir le fichier audio auquel nous voulons appliquer le tatouage, comme indiqué sur **la Figure III.8**.

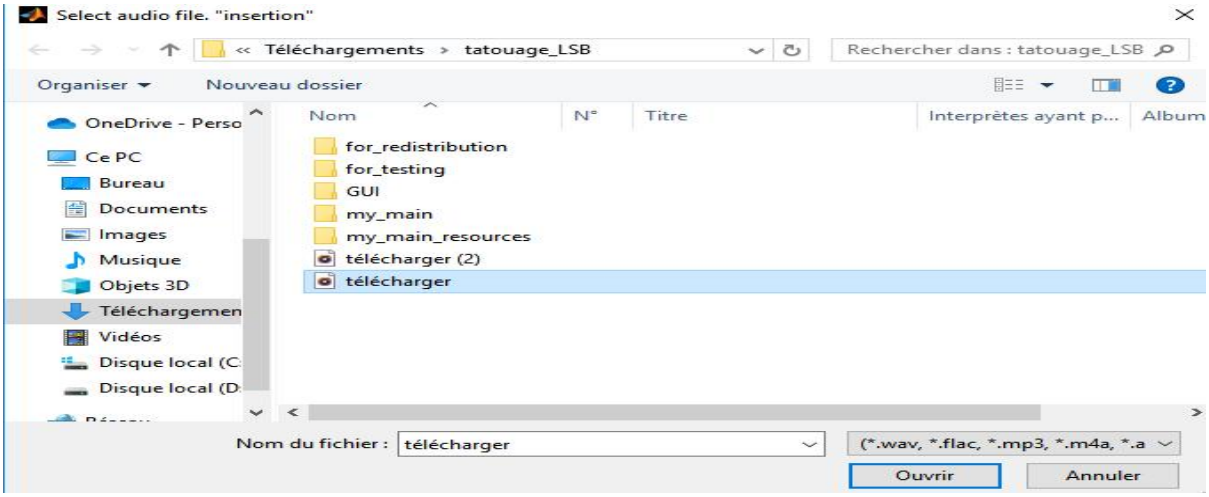


Figure III.8 Sélectionner un fichier audio

Après avoir sélectionné le fichier audio original, nous remarquons l'enregistrement audio après avoir inséré le tatouage par texte selon la méthode LSB, et vous pouvez lire l'audio à partir du bouton« lecteur » ou l'arrêter à partir du bouton « couper » et en même temps nous montrer la valeur de SNR de fichier audio tatouée comme indiqué sur **la Figure III.9**.

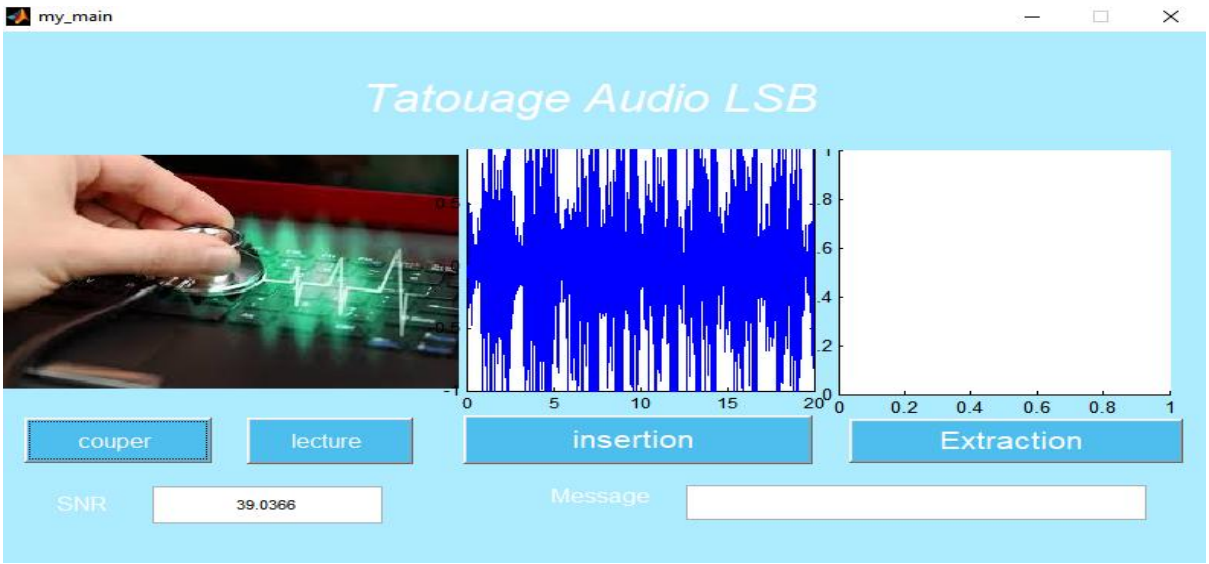


Figure III.9. Insertion de tatouage

III.4.1.b. Partie extraction :

Dans cette partie de l'application, nous appuyons sur le bouton « extraction » pour choisir le fichier audio tatoué avec un nom « …_stego » afin d'extraire le tatouage (texte) comme indiqué sur **la Figure III.10.**

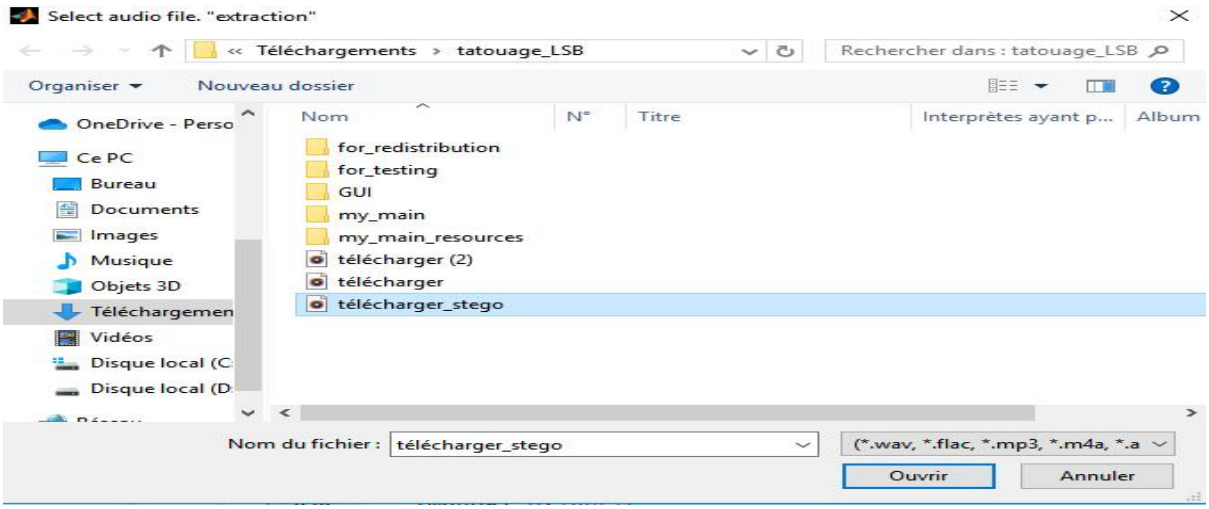


Figure III.10. Sélectionner un fichier audio tatoué

Après avoir sélectionné le fichier audio tatoué, l'enregistrement audio apparait avant d'entrer le tatouage, et le texte que nous avons caché dans son champ apparaît sur la page de l'application comme indiqué sur **la Figure III.11** .

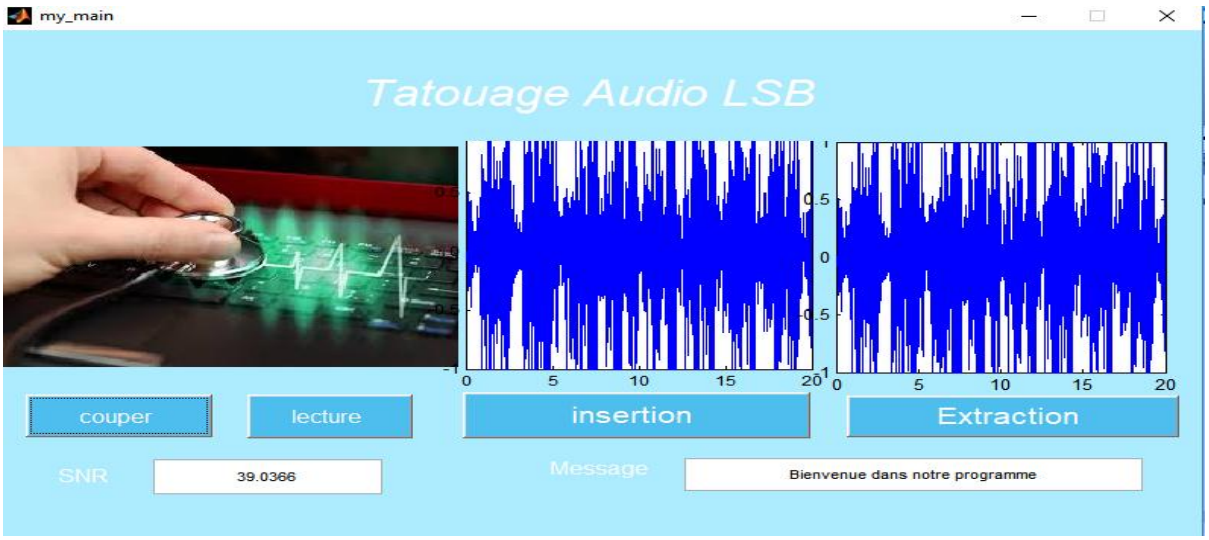


Figure III.11 Extraction de tatouage

III.4.2. Test de capacité (bits) :

La capacité est une propriété importante parce qu'elle a un impact négatif direct sur la robustesse et l'imperceptibilité du système de tatouage. Une capacité d'insertion grande cause une faible robustesse de la marque et une grande distorsion du signal tatoué.

F_S : Nombre d'échantillons bits par seconde .

Longueur (A) : le fichier audio.

$$\text{Cap} = \frac{F_S * \text{longeurs(A)}}{8} \text{(byte)} \qquad (1.1)$$

Puisque tous les fichiers audio sont même type, Fs est constant dans tout le fichier audio, et le résultat est le suivant :

$$\text{Cap} = \frac{\text{longeurs(A)}}{8} \text{(byte)} \qquad (1.2)$$

Tous les fichiers audio ont la même capacité car ils masquent tous le même nombre de bits par seconde.

III.4.3. Test d'imperceptibilité(SNR) :

Pour vérifier la transparence perceptuelle, nous pouvons utiliser le rapport signal-to-noise ratio (SNR).

Signal-to-Noise Ratio :

Le SNR est une métrique de différence statistique qui est utilisée pour mesurer la similitude entre le signal audio d'origine non déformé et l'audio en filigrane déformé signal. Le calcul du SNR est effectué selon l'équation. (1.1) [53], où A correspond au signal d'origine et A0 correspond au signal tatoué. Bien que le SNR soit une mesure simple pour mesurer le bruit introduit par le filigrane intégré et peut donner une idée générale de l'imperceptibilité, il ne prendre en compte les spécificités du système auditif humain [54].

$$\text{SNR (dB)} = 10log10\frac{\sum_n A^2}{\sum_n (A_n - A/_n)^2} \qquad (1.3)$$

Les audio	Signal-to-Noise Ratio(SNR)
Audio1_stego	52.2145
Audio2_stego	52.8226
Audio3_stego	53.0748
Audio4_stego	48.0857
Audio5_stego	40.5953
Audio6_stego	52.6083
Audio7_stego	48.8764
Ensemble de SNR/7	348.2776/7
Moyen	49.7539429

Tableau 1. Les valeurs SNR signal sur bruit.

Le tableau présente les résultats d'imperceptibilité d'une fonction du SNR, qui indique que les signaux portant un filigrane ne sont pas significativement distingués des signaux audio d'origine, et à cela fournit la méthode de valeurs de SNR allant de 40-52dB avec (une moyenne 49.75), ce qui indique clairement d'imperceptibilité excellent. Parce que le SNR est généralement jugé par les valeurs suivantes :

10-15 dB : le minimum acceptable pour créer une connexion.

16-24 dB: qualifié comme "faible".

25-40 dB : il est considéré comme "bon".

Le rapport ≥ 41 dB : il est considéré comme "excellent".

Nous avons écouté les signaux aquatiques avec un tatouage, et nous avons eu du mal à les distinguer avec les signaux audio originaux. Même si nous expliquons cela avec un schéma spectral, nous ne trouvons pas de différence visuelle entre eux. Cela indique la bonne transparence de notre application.

III.5. Conclusion :

Dans ce chapitre, nous avons fourni la conception et la Réalisation de l'application, Environnement, Méthode du tatouage, car nous avons fourni une explication détaillée sur la manière d'entrer, de guider et de calculer le test d'imperceptibilité (SNR), le test de capacité (bit).

Conclusion générale

L'échelle élargie de données avancées accessibles pour les téléchargements en double sur les ordinateurs et la transmission prudente sur le Web met l'accent sur les exigences assurance droits d'auteur. Cette affaire a touché des innovateurs titulaires d'une licence. Le filigrane numérique offre une défense contre de tels problèmes. Notre sujet portait sur le tatouage numérique pour augmenter la sécurité des échanges de données vocales sensibles en télémédecine dans un contexte spécifique de transmission de données cachées.

Cette classe d'application permet notamment d'augmenter le contenu d'un signal audio. L'insert de tatouage doit être transparent, la meilleure fiabilité de transfert. Il est possible de masquer des informations dans les fichiers audio «.wav», d'un simple mot comme "bonjour", au texte intégral avec des chiffres et des symboles. Les informations cachées dans le fichier audio peuvent nuire à la qualité audio, car, plus il y a d'informations cachées dans le fichier, plus il subira de modifications en raison du remplacement des derniers bits par ceux du message à envoyer.

Dans différents scénarios de test, on peut conclure que les fichiers qui étaient sur l'ordinateur et mis dans le lecteur de musique, sont ceux qui ont le moins changé et ne peuvent pas être détectés par les personnes interrogées. Les fichiers compressés et envoyés sur Internet souffrent d'une légère modification de leur qualité sonore, car en masquant les informations, en modifiant et en compressant les bits les moins significatifs à envoyer sur Internet, ils sont affectés deux fois et la qualité sonore peut subir quelques changements.

La principale caractéristique qui a été déterminée pour réaliser la mise en œuvre de la stéganographie dans les fichiers audio est que les fichiers doivent avoir l'extension «.wav », car leur qualité sonore est supérieure aux autres formats et est la norme pour fonctionner sur la plate-forme «Matlab». Lors du démarrage de la mise en œuvre de la stéganographie, il convient de garder à l'esprit que l'en-tête du fichier audio ne peut subir aucune modification, car l'en-tête contient des informations spécifiques aux fichiers «.wav».

Les facteurs d'échelle ont été analysés pour établir la robustesse, la non-perception et la capacité. Des idées distinctives ont été déduites, y compris SNR pour remettre en question la qualité audio filigranée et la prise de décision. Dans la plupart des cas, on doit maintenir une

qualité SNR élevée. Notre objectif de recherche et la principale contribution de cette étude sont concentrés sur la conception d'une application qui protège les données audio médicales sensibles sous les contraintes auxquelles sont confrontées les institutions médicales.

Le domaine de la recherche est jusqu'à présent ouvert à des travaux approfondis au fur et à mesure que la technologie progresse avec le temps.

Référence

[1] **PatrickBas.**Méthodes de tatouage d'images fondées sur le continue. PhDthesis, (2000).

[2] **Loukhaoukha, Khaled.** "Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective." (2010).

[3] **Anne-Sophie MAZEIRAT Juriste SHAM ,**Article La télémédecine est désormais considérée comme un acte médical à part entière.(7/04/2011).

[4] **Wright, D &Androuchko, L.** (1996). Telemedicine and developing countries. *Journal of Telemedicine and Telecare*, *2*(2), 63-70.

[5] **Philippe Lefebvre et Michel Aka .**Applications : Commerce électronique et Télémédecine, La Telemedecine 4 décembre 2000.

[6] **VaddeSeethaRama Rao ,L.V.R Chaitanya Prasad .**MATLAB Implementation of Audio Steganography for Secure Data Transmission . International Journal of Scientific Engineering and Technology Research Volume.06, IssueNo.31, October-2017, Pages: 6069-6079.

[7] **Cayre, F.** (2008). Cryptographie, stéganographie et tatouage: des secrets partagés. *Interstices*.

[8] **Usha C, Kumar SR** (2016) Digital image watermarking techniques and applications: a survey. IntJAdv Res ComputSciSoftwEng 6:3

[9] **Tiwari, N.** Sharmila (2017) Digital watermarking applications, parameter measures and techniques. *Int J ComputSciNetwSecur*, *17*(3), 184.

[10] https://fr.m.wikipedia.org/wiki/Tatouage_num%C3%A9rique

[11] **CléoBaras, Nicolas Moreau, Alejandro Lobo Guerrero et Patrick Bas .**Procédés d'insertion

audiobas´es sur le tatouage. Dans Rapport d'avancement du projet ARTUS,octobre, 2003.

[12] **Nguyen, Philippe, and Séverine Baudry.** "Le tatouage de données audiovisuelles." *Les Cahiers du numérique* 4.3 (2003): 135-165.

[13] **Philips .**Contenidentification.http://www.research.philips.com/initiatives/contentid/index.html.

[14] **Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R**. (2014). Watermarking techniques used in medical images: a survey. *Journal of digital imaging*, *27*(6), 714-729.

[15] **Steinebach, M., Petitcolas, F. A., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., ... &Ferri, L. C**. (2001, April). StirMark benchmark: audio watermarking attacks. In *Proceedings international conference on information technology: coding and computing* (pp. 49-54). IEEE.

[16] **Tewari, T. K., Saxena, V., & Gupta, J. P**. (2011). Audio watermarking: Current state of art and future objectives. *International Journal of Digital Content Technology and its Applications*, *5*(7).

[17] https://www.lexico.com/en/definition/audio_file (12 mai 2022).

Référence

[18] https://byjus.com/jee/properties-of-sound/(08 mai 2022).

[19] https://e-echocardiography.com/page/page.php?UID=1429454151(08-12 mai 2022).

[20] **CRodríguezQuito,**Ecuador: Universidad de las Fuerzas Armadas ESPE, 2016.

[21] **BENHACICENEWafa ,MADDEHI Meriem,Mr.MOUDACHE Saïd:** université AKLI Mohand Oulhadj-Bouira**,** «Tatouage audio utilisant le masquage perceptuel »(26/09/2017).de **CT GOMES, L., MBOUP, M., BONNET, M., & MOREAU, N**. (2001). Tatouage audio exploitant des propriétés de cyclostationnarité. *Traitement du Signal*, *19*(1), 1.

[22] **Kim, K. H., & Ro, Y. M**. (2003, October). Enhancement methods of image quality in screen mark attack. In *International Workshop on Digital Watermarking* (pp. 474-482). Springer, Berlin, Heidelberg.

[23] **Hartung, F., &Kutter, M.** (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, *87*(7), 1079-1107.

[24] **Bender, W., Gruhl, D., Morimoto, N., & Lu, A**. (1996). Techniques for data hiding. *IBM systems journal*, *35*(3.4), 313-336.

[25] **Langelaar, G. C., Setyawan, I., &Lagendijk, R. L**. (2000). Watermarking digital image and video data. A state-of-the-art overview. *IEEE Signal processing magazine*, *17*(5), 20-46.

[26] **Cox, I. J., Kilian, J., Leighton, F. T., &Shamoon, T**. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, *6*(12), 1673-1687.

[27] **Wolfgang, R. B., Podilchuk, C. I., &Delp, E. J**. (1999). Perceptual watermarks for digital images and video. *Proceedings of the IEEE.*

[28] **Thanki R, Kothari A.** (2016) Digital watermarking – technical art of hiding a message. In:

Intelligent analysis of multimedia information, pp 426–460, IGI Global, USA.

[29] **H. J. Kim.** "Audio Watermarking Techniques". Department of Control and Instrumentation Engineering, Kangwon National University, Korea, 2004.

[30] **N.Cvejic,** "Algorithms for Audio Watermarking and Steganography". Department of Electrical and Information Engineering, University of Oulu, 2004. Bibliographie 103.

[31] **G. C. Rodriguez, M.N. Miyatake, H.M.P. Meana,** "Analysis of audio watermarking schemes". IEEE 2 nd International Conference on Electrical and Electronics Engineering, pp. 17-20. 2005.

[32] **N.Cvejic,** T. Seppanen, "Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks". IGI Global, Hershey, Pennsylvania. USA, 2007.

[33]**S. Katzenbeisser, F. Petitcolas,** “Information Hiding Techniques for Steganography and

Référence

Digital Watermarking,“Artech House, 2000.

[34] **W. Kong, B. Yang, D. Wu, X. Wu D., Niu X.,** “Svd based blind video watermarking algorithm”, in proceedings of International Conference on Innovative Computing, Information and Control (ICICIC’06) , Vol. 1, pp. 265-268, Beijing, China, 30 Augst-1 September 2006.

[35] **N. I. Yassin, N. M. Salem, M. I. El Adawy,** “Qim blind video watermarking scheme based on wavelet transform and principal component analysis,” Alexandria Engineering Journal, vol. 53, no. 4 , pp. 833-842,2014.

[36] **G. J. Durieu, “Survey of watermarking techniques,**" Theses and Dissertations. 708,2001.

[37] **D. K. Thind, S. Jindal,** “A semi blind dwt-svd video watermarking,” Procedia Computer Science, vol. 46, no. Supplement C, pp. 1661- 1667, 2015.

[38] **O. S. Faragallah,** “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain,” AEU-International Journal of Electronics and Communications, vol. 67, no. 3, pp.189-196, 2013.

[39] **Cox I. Cox, M. Miller, J. Bloom, J. Fridrich, T.,** “The First 50 Years of Electronic Watermarking,” EURASIP Journal on Applied Signal Processing, Vol. 2002, No. 2, pp.126–132, 2002.

[40] **P.Bassia , I. Pitas , N. Nikolaidis** , " Robust Audio Watermarking in the Time Domain " . IEEE Transactions on Multimedia ,vol 3 , No. 2 , 2001 .

[41] **M.Arnold,S. Wolthusen, M. Schmucker**, "Techniques and applications of digital watermarking and content protection ". Artech House Publishers, July 2003.

[42] **I. Cox, M. Miller,J. Bloom**, "Digital watermarking". Morgan Kaufmann Publishers, San Francisco, USA, 2002.

[43] **NedeljkoCvejic ,** TapioSeppben " Increasing the capacity of LSB - based audio steganography " FIN 90014 University of Oulu , Finland , 2002.

[44] **SajadShirali - Shahreza M.T. Manzuri - Shalmani ,**" High capacity error free wavelet domain speech steganography " ICASSP 2008.

[45]**NeilF.Johnson , Z.Duric and S.Jajodia ,** " Information Hiding Steganography and Watermarking - Attacks and Countermeasures " . Kluwer Academic Publishers , 2001.

[46] **Min Wu . Bede Liu ,** " Multimedia Data Hiding " , Springer - Verlag New York . 2003 .

Référence

[47] **M.Pooyan , A. Delforouzi ,** " LSB - based Audio Steganography Method Based on Lifting Wavelet Transform " , in Proc . 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT07) . December 2007 , Egypt .

[48] **Potdar VM, Han S, Chang E** (2005) A survey of digital image watermarking techniques, 0-7803-

9094-6/05/$20.00 ©2005 IEEE.

[49] **Rathee N, Kumar S** ,(2014) A survey on audio watermarking techniques. Int J EngApplManagSci

Paradigm 16(1).

[50] **Boney L, Tewfik A, Hamdy K** (1996) Digital watermarks for audio signals. In: The Third IEEE

international conference on multimedia computing and systems, pp 473–480.

[51] Premiers pas en Matlab **Florent Kr**¸zaka la Laboratoire P.C.T., UMR CNRS 7083, ESPCI,

10 rue vauquelin, 75005, Paris, France.

[52] Respiratory Sound Database | Kaggle.

[53] **Darabkh KA** (2014) Imperceptible and robust DWT-SVD-based digital audio watermarking algorithm. J SoftwEngAppl 7:859–871. https://doi.org/10.4236/jsea.2014.710077.

[54] **Beerends JG, Stemerdink JA** (1992) A perceptual audio quality measurement based on a psychoacoustic sound representation. J Audio Eng Soc 40:963–972.

Référence