

Procédé et système de communications acoustiques

Domaine de l'invention

L'invention concerne de manière générale les communications acoustiques, et en
5 particulier un procédé et un système de communications acoustiques sous-marines discret.

Art antérieur

Les systèmes de communications acoustiques sous-marines discrets émettent
des signaux acoustiques de communication (flux audio) vers des récepteurs ciblés
10 de telle sorte que ces signaux ne soient pas détectés par des tiers ou, s'ils sont
détectés par des tiers, soient considérés par ceux-ci comme une composante
anodine du bruit ambiant.

Plusieurs solutions ont été proposées dans le passé pour cacher de l'information
dans un flux audio, par exemple pour y cacher de courts messages de type SMS
15 (acronyme pour « Short Message Service » signifiant « Service de Messages
courts »). L'information cachée ne peut alors être accédée que par les récepteurs
ciblés qui sont équipés de boîtier de décodage spécifiques.

Plus récemment, les éditeurs ou diffuseurs de musique ont mis au point plusieurs
20 solutions permettant de cacher dans des fichiers audio de type .wav ou .mp3, des
informations de copyright ou des marquages spécifiques destinés à servir de
preuve en cas de piratage ou de diffusion non autorisée du contenu de ces
fichiers. Ces solutions sont par exemple basées sur des techniques d'encodage
telles que l'encodage des bits de poids faibles, l'ajout de signaux auxiliaires faibles
25 en bande étroite ou d'échos. Leur application est principalement limitée à la
transmission via des canaux de transmission peu bruités, sans doppler ni trajets
multiples, et surtout uniquement à des canaux numériques comme décrit dans les
articles suivants :

- N. Cvejic «Algorithms for audio watermarking and steganography, Academic
30 dissertation University of Oulu, 2004»,

- R. Walker, «Audio Watermaking, BBC R&D White Paper, WHP 057, August 2004»,

- K. Gopalan, «Audio steganography using bit modification, Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), Vol. 2, pp. 421-424, April 2003»,

-Gopalan, «Audio Steganography for Covert Data Transmission by Imperceptible Tone Insertion, Proc. the IASTED International Conference on Communication Systems And Applications (CSA 2004), Banff, Canada, July 8-10, 2004».

Les systèmes de communication acoustiques discrets peuvent être basés sur des communications numériques. Selon une première approche, le système émet un signal porteur de l'information à un niveau très faible de manière à ne pas être détecté par un tiers. Le signal de communication présente alors un rapport signal-sur-bruit trop faible pour être détecté par un tiers. Toutes les solutions de ce type se caractérisent par un débit d'information relativement faible (faible efficacité spectrale, typiquement de l'ordre de quelques 10^{-1} bit/sec/Hz).

Plusieurs solutions ont été proposées selon cette première approche, comme par exemple des solutions basées sur des techniques d'étalement de spectre, comme par exemple dans J.G. Proakis, « Digital Communications, Mc Graw Hill, 4th edition, 2001». La connaissance de la séquence ou du code d'étalement utilisé, ainsi qu'un traitement adéquat, permettent alors la détection du signal émis par le destinataire du message seulement. Le destinataire du message peut alors en extraire l'information. Toutefois de telles solutions ne permettent d'atteindre qu'un débit faible. Par ailleurs, un tiers différent du destinataire ciblé pourrait détecter le signal de communication et identifier la séquence d'étalement en analysant des signaux reçus sur une longue durée (G. Burel, Detection of Spread Spectrum Transmission Using Fluctuations of Correlation Estimators, IEEE-ISPACS, Honolulu, Nov. 2000).

On connaît également une technique dérivée des solutions précédentes et basée sur l'utilisation de modulations OFDM (G. Leus and P. van Walree « Multiband OFDM for covert acoustic communications, IEEE Journal on Selected Areas in Communications, Vol. 26, N° 9, December 2008»). Il est possible que cette technique permette théoriquement d'exploiter les propriétés de cyclo-stationnarité des signaux OFDM pour les détecter et les identifier comme portant de l'information. Toutefois, cette détection requière des algorithmes lourds et la disponibilité de signaux longs.

Il existe encore une solution basée sur la première approche qui, au lieu d'utiliser comme séquence d'étalement une même séquence pseudo aléatoire répétée en boucle pendant la transmission, utilise une séquence chaotique, c'est-à-dire un bruit blanc généré par un oscillateur chaotique ou un signal aléatoire non périodique (Stéphane PENAUD, Philippe BOUYSSSE, Jacques GUITTARD et al, Potentialités des séquences d'étalement chaotiques pour l'amélioration du TEEB d'un système DS-CDMA asynchrone, ANN. TELECOMMUN., 58, n ° 3-4. 2003).

Cette absence de périodicité rend impossible la détection du signal de communication selon les précédentes techniques. Néanmoins, elle pose des problèmes de synchronisation émetteur/récepteur qui rendent impossible son application à un système de communication simple et peu coûteux (en raison notamment de la nécessité de re-synchronisations fréquentes et peu discrètes, ou de la nécessité d'utiliser des horloges extrêmement précises, coûteuses et difficilement intégrables dans un "petit" système de communication acoustique).

D'autres solutions ont été proposées, selon une deuxième approche. Ces solutions consistent à émettre des signaux d'apparence anodine, par exemple des signaux pouvant être confondus avec des signaux de mammifères marins, de travaux sous-marins de bâtiments anodins, de bruit de mer (vague, vent, pluie, etc.) sans contraintes quant au niveau émis sous réserve de garder un niveau admissible et peu fort pour que le signal émis apparaisse bien naturel. Par exemple, une technique de ce type consiste à émettre des séquences de clics large bande ressemblant à des clics de dauphins, l'espacement entre les clics portant l'information à transmettre (H.S. Dols et al, « Covert underwater acoustic

communication with marine mammals sounds, Proc. UDT Europe 2008 »). Cependant, avec de telles techniques, il est difficile de générer des signaux qui n'aient pas une allure synthétique (vraies vocalises ou clics de mammifères marins). Elles nécessitent en outre d'émettre des signaux compatibles avec le lieu et le moment de l'émission (par exemple, des signaux ressemblant à une espèce inconnue dans la zone de l'émetteur ne doivent pas être transmis, les craquements d'icebergs en Méditerranée ne doivent pas être simulés, etc.).

Définition générale de l'invention

- 10 L'invention vient améliorer la situation. A cet effet, elle propose un dispositif émetteur, comprenant une antenne d'émission, l'antenne d'émission comprenant au moins un transducteur et une unité de génération de signal pour générer un signal de communication acoustique à émettre vers un dispositif récepteur incluant de l'information cachée. Avantageusement, l'unité de génération de signal est
- 15 configurée pour enregistrer au préalable un signal acoustique d'origine et générer le signal de communication à émettre en ajoutant à un signal initial $x(t)$, dérivé du signal d'origine, un signal auxiliaire préalablement multiplié par au moins un symbole, le symbole ayant une phase et/ou une amplitude portant l'information cachée et le signal auxiliaire étant calculé à partir du signal initial au moyen d'un
- 20 opérateur de transformation choisi qui dépend d'une clé stéganographique.

Selon une caractéristique de l'invention, le signal initial dérivé du signal d'origine est le signal complexe en bande de base obtenu après filtrage du signal d'origine dans une bande de fréquences de largeur choisie, centrée sur une fréquence centrale.

- 25 Selon une autre caractéristique, l'unité de génération de signal est configurée pour diviser au préalable la durée totale du signal d'origine $x(t)$ en un ensemble d'intervalles de temps successifs jointifs de même durée T , l'opérateur de transformation étant appliqué au signal initial sur chacun de ces intervalles pour calculer la valeur du signal auxiliaire correspondante sur l'intervalle.
- 30 En particulier, le signal de communication généré $y(t)$ à un instant t appartenant au n -ième intervalle $[nT, (n+1)T]$ est égal à :

$$y(t) = x(t) + \alpha \cdot a_n \cdot \Psi(x)(t),$$

où α désigne un paramètre de gain et a_n désigne le symbole correspondant au $n^{\text{ième}}$ intervalle.

Dans une première forme de réalisation, l'unité de génération de signal est en outre configurée pour diviser la durée totale du signal initial en un ensemble d'intervalles successifs jointifs de même durée T , et chaque intervalle de durée T en $2M$ sous-intervalles $U_{-M}, \dots, U_{-1}, U_1, \dots, U_M$, séparés par des intervalles de garde, les sous-intervalles ayant des durées croissantes en fonction de la valeur absolue de k , l'opérateur de transformation étant appliqué au signal initial sur chaque sous-intervalle U_k pour calculer la valeur du signal auxiliaire correspondante sur l'intervalle.

Dans cette forme de réalisation, la valeur du signal auxiliaire $\Psi(x)(T/2 + t)$ à un instant $T/2 + t$, avec t appartient à un sous-intervalle U_k , peut être fonction d'un paramètre de phase $\exp j \cdot \beta_k$, avec β_k compris dans l'intervalle $[0, 2\pi]$ et k compris dans l'intervalle $[-M, M]$, de la valeur d'une fonction de pondération d'amplitude $p(t)$ à l'instant t , et de la valeur du signal initial à l'instant $(T/2 - t)$.

En particulier, la valeur du signal auxiliaire $\Psi(x)(T/2 + t)$ à un instant $T/2 + t$, où t appartient à un sous-intervalle U_k , peut être égale à :

$$\Psi(x)(T/2 + t) = \exp j \cdot \beta_k \cdot p(t) \cdot x(T/2 - t).$$

La durée des intervalles de garde entre les sous-intervalles de temps successifs U_k et U_{k+1} peut être choisie de sorte que chacun des sous-intervalles U_k ne recouvre pas ses voisins après dilatation/compression due à un phénomène doppler.

Dans une deuxième forme de réalisation, l'unité de génération de signal peut être en outre configurée pour diviser chaque intervalle de durée T en un ensemble de M sous-intervalles de même durée T/M , la valeur du signal auxiliaire sur un sous-intervalle de temps donné étant obtenue à partir de la valeur du signal initial sur un autre sous-intervalle.

En particulier, dans cette forme de réalisation, la valeur du signal auxiliaire à un instant t appartenant à un sous-intervalle de temps donné peut être obtenue à

partir de la valeur du signal initial à l'instant $-t$ sur un autre sous-intervalle (retournement temporel).

En complément, la valeur du signal auxiliaire à un instant t appartenant à un sous-intervalle de temps donné peut être obtenue à partir de la valeur du signal initial
5 sur un autre sous-intervalle pondérée par la valeur d'une fonction de pondération d'amplitude $p(t)$ à l'instant t .

L'invention propose en outre un dispositif récepteur comprenant une antenne de réception, l'antenne de réception comprenant au moins un hydrophone. Le dispositif récepteur comprend également un détecteur pour détecter un signal de
10 communication émis par un dispositif émetteur selon l'une des caractéristiques précédentes et une unité d'extraction configurée pour reconstituer le signal auxiliaire en appliquant ledit opérateur de transformation au signal de communication détecté à partir de la clé stéganographique, et pour extraire l'information cachée à partir de la phase et/ou de l'amplitude du signal auxiliaire
15 reconstruit.

L'unité d'extraction peut être en outre configurée pour appliquer un filtre au signal reconstitué à partir d'un terme de compensation $e^{-i\widehat{\theta}u}$ propre à compenser le résidu de la porteuse correspondant à l'écart entre la fréquence porteuse avec doppler et la fréquence porteuse nominale, le terme de compensation étant estimé
20 en maximisant, à chaque instant t , le module de la sortie $z(t)$ du filtre pour un ensemble de valeurs possibles de θ . La fonction d'extraction est alors apte à déterminer les symboles et les bits de l'information cachée à partir des phases du signal $z(t)$ calculées à des instants correspondants aux maxima du module du signal $z(t)$.

25 L'invention propose en outre un système de communication comprenant un dispositif émetteur et un dispositif récepteur selon l'une des caractéristiques précédentes.

L'invention propose également un procédé d'émission pour générer un signal de communication acoustique à émettre dans un dispositif émetteur (101),
30 comprenant une antenne d'émission, l'antenne d'émission comprenant au moins

un transducteur, le procédé comprenant les étapes suivantes :

- a. enregistrer un signal acoustique d'origine ;
 - b. ajouter à un signal initial $x(t)$, dérivé du signal d'origine, un signal auxiliaire multiplié par au moins un symbole, le symbole ayant une phase et/ou une amplitude portant l'information cachée et le signal auxiliaire étant calculé à partir du signal initial au moyen d'un opérateur de transformation choisi qui dépend d'une clé stéganographique, ce qui fournit un signal de communication,
 - c. émettre un signal vers un dispositif récepteur à partir du signal de communication obtenu à l'étape b.
- 10 Le signal émis peut ainsi apparaître à un tiers parfaitement naturel à la différence d'un signal synthétique trop régulier. Il est en outre toujours bien adapté à la zone et au moment de l'émission.

Cette solution est applicable à tous types de signaux, avec des performances variables en termes de débits possibles. Elle s'adapte notamment à un environnement fortement bruité.

Description des figures

- 20 D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit et des figures des dessins annexés dans lesquels:
- La figure 1 est un schéma représentant le système de communication acoustiques certains modes de réalisation de l'invention ;
 - La figure 2 est un organigramme représentant le procédé d'émission selon certains modes de réalisation de l'invention ;
 - La figure 3 est une représentation schématique illustrant le découpage de l'intervalle T en 2M sous-intervalles ;
 - La figure 4 est un schéma illustrant la construction du signal auxiliaire au moyen de l'opérateur de transformation selon le premier exemple de réalisation
- 30 - Les figures 5 et 6 sont des schémas représentant respectivement un signal initial et le signal modifié correspondant avec insertion de 16 bits, selon un exemple de réalisation;

- Les figures 7 et 8 sont des schémas représentant respectivement un signal initial et le signal modifié correspondant avec insertion de 50 bits, selon un exemple de réalisation;
- La figure 9 est un organigramme représentant le procédé de réception, selon
5 certains modes de réalisation de l'invention ;
- Les figures 10 et 11 sont des schémas représentant respectivement la réponse d'impulsion dans un canal acoustique en fonction du temps et le profil de retard de puissance en fonction du retard, obtenus pour un signal dans un canal acoustique sous-marin simulé ;
- 10 -Les figures 12 et 13 représentent des exemples de sorties obtenues avec le procédé de réception, pour deux exemples de signaux initiaux différents ;
- La figure 14 représente les symboles détectés pour l'exemple de la figure 12 ;
- La figure 15 représente les symboles détectés pour l'exemple de la figure 13 ;
- La figure 16 est un schéma illustrant la construction du signal auxiliaire au moyen
15 de l'opérateur de transformation selon le deuxième exemple de réalisation ;
- la figure 17 représente un spectrogramme du signal audio original pour un exemple d'enregistrement de clics,
- La figure 18 représente le signal audio modifié porteur de 8 bits d'information correspondant au signal audio original de la figure 17 ; et
- 20 - La figure 19 représente la sortie du récepteur, dans l'exemple de signal de la figure 14, en fonction du temps de la corrélation du signal reçu avec le signal auxiliaire porteur de l'information.

Les dessins pourront non seulement servir à mieux faire comprendre la
25 description, mais aussi contribuer à la définition de l'invention, le cas échéant.

Description détaillée

La figure 1 représente un système de communication 100 sous-marine numérique
30 discret, selon certains modes de réalisation de l'invention, configuré pour émettre un signal comprenant de l'information cachée entre un émetteur et un récepteur cible.

Le système de communication 100 comprend un dispositif d'émission 101 prévu au niveau de l'émetteur pour émettre un signal de communication et un dispositif de réception 102, prévu au niveau du récepteur, pour recevoir le signal émis.

- 5 Le dispositif d'émission 101 est configuré pour émettre un signal acoustique d'origine, préalablement enregistré et modifié de manière à porter de l'information cachée, en ajoutant à un signal initial $x(t)$ dérivé du signal d'origine un signal $q(t)$ qui dépend :
- d'un signal auxiliaire, noté $\Psi(x)(t)$, calculé à partir du signal initial $x(t)$ au moyen
 - 10 d'un opérateur de transformation Ψ (par exemple choisi par l'émetteur); et
 - d'un symbole a_n comprenant une amplitude et ou une phase portant l'information cachée.

Tel qu'utilisé ici, le signal acoustique d'origine désigne un signal acoustique
15 provenant d'une source naturelle. Dans la suite de la description, le signal acoustique d'origine sera également désigné par l'expression « signal d'origine ». Le signal acoustique d'origine peut être un morceau de bruit ambiant d'allure anodine. Ce morceau de bruit ambiant anodin peut être par exemple un bruit de mammifère marin présent sur la zone, un bruit de pluie ou de vague, ou encore le
20 bruit rayonné par un chalutier inoffensif, etc.

Les signaux $x(t)$, $q(t)$ et $\Psi(x)(t)$ varient en fonction du temps t .

L'amplitude du signal ajouté $q(t)$ correspond à l'amplitude du symbole et peut être
25 en particulier faible par rapport à l'amplitude du signal initial de manière à rester imperceptible par des tiers.

Le dispositif de réception 102 est capable de reconstituer le signal auxiliaire de manière approchée, en appliquant le même opérateur de transformation Ψ au
30 signal reçu, en détectant le signal auxiliaire au moyen d'un filtre adapté et en extrayant l'information à partir de la phase et/ou de l'amplitude du symbole.

Plus précisément, le dispositif d'émission 101 comprend une antenne d'émission 1 comprenant un transducteur acoustique ou une pluralité de transducteurs acoustiques 10 si l'émission est directive. La directivité de l'émission permet d'améliorer la discrétion dans le cas où l'émetteur sait, même de manière
5 approximative, où se trouve le récepteur.

Le dispositif d'émission 101 peut comprendre en outre des unités de traitement 11 associées à chaque transducteur 10 comme par exemple des convertisseurs numériques/analogiques, des amplificateurs de puissance, des circuits
10 d'accord/adaptation associés à chacun des transducteurs. Certaines de ces unités de traitement peuvent être directement incluses dans l'antenne d'émission.

Le dispositif d'émission 101 peut comprendre en outre un calculateur 12 équipé d'une unité de génération d'un signal 120 configurée pour générer un signal audio
15 à émettre correspondant au signal initial modifié avec information cachée. Le calculateur 12 peut en outre comprendre des unités de réplication 122 configurées pour générer des répliques du signal à transmettre par chacun des transducteurs d'émission (formation de voies). La formation de voies à l'émission peut permettre d'améliorer la discrétion de manière significative. En effet, la formation des voies
20 peut être utilisée pour émettre préférentiellement dans un secteur angulaire comprenant le récepteur, ce qui réduit la possibilité d'une interception par un tiers situé hors de ce secteur (avec les limitations dues aux lobes secondaires à l'émission).

Spécifiquement, l'unité de génération de signal 120 peut être configurée pour diviser un signal enregistré en blocs temporels successifs et jointifs, de longueur fixe T . Sur chaque bloc, l'unité de génération de signal 120 peut alors calculer à partir du signal initial $x(t)$, pour t appartenant à $[0, T]$, un signal auxiliaire noté $\Psi(x)(t)$ (t appartenant à $[0, T]$), au moyen de l'opérateur de transformation Ψ . Ce
30 signal auxiliaire est multiplié par un symbole a_n qui comprend une phase et/ou une amplitude qui dépend de l'information à transmettre (information cachée). Il peut être aussi multiplié par un gain α choisi pour l'atténuer, dans certains modes de

réalisation (le signal résultant $q(t)$ est alors égal à $q(t) = \alpha \cdot a_n \cdot \Psi(x)(t)$). Le signal résultant $q(t)$ peut alors ajouté au signal initial $x(t)$.

Le dispositif de réception 102 comprend une antenne de réception 2 comprenant
 5 un ou plusieurs hydrophones 13, chaque hydrophone étant associé à des unités de traitement 14 tels que des préamplificateurs et convertisseurs analogiques/numériques. Certaines de ces unités de traitement 14 peuvent être directement incluses dans l'antenne d'émission.

10 Le dispositif de réception 102 peut comprendre en outre un calculateur 15 comprenant une unité de formations de voies 150 pour former des voies dans la ou les directions où est susceptible de se trouver l'émetteur (par exemple dans tout l'horizon en l'absence d'information à priori sur la position de l'émetteur, une voie unique pouvant couvrir tout l'horizon si le système de réception est équipé
 15 d'un seul hydrophone à la réception). Le calculateur 15 peut en outre comprendre un détecteur 151 pour détecter la présence de l'information cachée dans les signaux en sortie de formation de voies et une unité d'extraction 152 pour extraire l'information cachée dans le signal détecté par le détecteur 151.

20 L'unité d'extraction 152 peut être configurée pour générer, à partir du signal reçu $y(t)$ et sur une fenêtre glissante de longueur T , une version approximée du signal auxiliaire en appliquant le même opérateur de transformation, soit $\{\Psi(y)(t), t = 0, T\}$. Il est à noter que l'approximation du signal auxiliaire (encore appelé « signal auxiliaire reconstitué ») peut être d'autant plus précise que le signal auxiliaire a été
 25 atténué par le gain α avant d'être ajouté à l'émission. L'unité d'extraction 152 peut calculer ensuite le produit scalaire entre le signal reçu $y(t)$ et le signal auxiliaire reconstitué, puis déterminer sa phase, ce qui fournit l'information binaire transmise (information cachée), sous forme par exemple d'un bit si une modulation BPSK a été employée à l'émission, ou de deux bits si c'est une modulation QPSK.

30 Dans un canal de transmission idéal (stationnaire et sans trajets multiples), le signal résultant du produit scalaire sur fenêtre glissante de durée T présente des pics séparés d'un intervalle de temps T . La forme de tels pics et leur finesse

peuvent dépendre de la fonction d'auto-corrélation du signal auxiliaire. Dans un canal réel, des pics ont été observés dont la forme correspond au produit de convolution de la fonction d'auto-corrélation de la réponse impulsionnelle $h(t)$ du canal acoustique (soit $C_h(\zeta) = \int h(\zeta-t) h(t) dt$) et de celle du signal auxiliaire.

5

Dans certains modes de réalisation, l'unité de génération de signal 120 peut opérer dans une bande de fréquence limitée, qui peut être choisie en fonction des caractéristiques du signal initial $x(t)$. Par ailleurs, le signal dérivé du signal initial à partir duquel est déterminé le signal auxiliaire $\Psi(x)(t)$ peut être le signal complexe
10 obtenu après démodulation du signal initial autour d'une fréquence centrale ou porteuse nominale et dans une bande de fréquences B donnée. Une fois le signal $q(t)$ ajouté au signal initial (ce qui fournit un signal $y(t)$), le signal à émettre peut alors être obtenu en modulant le signal $y(t)$ par la porteuse nominale puis en prenant la partie réelle du signal ainsi modulé. Dans un tel mode de réalisation, à
15 la réception, avant d'extraire l'information, l'unité d'extraction 152 démodule le signal reçu autour de la fréquence porteuse nominale et dans la bande de fréquences B .

Le système de communication 100 peut en outre comprendre une unité de
20 contrôle 103 associé au calculateur 12 et une unité de contrôle 104 associé au calculateur 15. Chaque unité de contrôle 103 et 104 peut comprendre des Interfaces Homme Machine IHM et des périphériques d'entrée et/ou sortie, comme par exemple un écran et/ou un clavier, pour permettre la saisie ou l'affichage de messages ou d'information à transmettre ou reçus. En variante, une
25 seule unité de contrôle commune couplée à la fois au dispositif émetteur 101 et au dispositif récepteur 102 peut être utilisée. Les unités de contrôle (103, 104) peuvent permettre également de contrôler et de configurer les dispositifs d'émission et de réception 101 et 102.

30 Le système de communication 100 forme ainsi un système acoustique discret permettant d'inclure dans le signal émis de l'information cachée, comme par exemple des messages tactiques courts de quelques dizaines d'octets (SMS, mail, trigrammes prédéfinis, etc.).

L'information peut être cachée dans l'amplitude du symbole a_n et/ou dans sa phase lorsque la quantité d'information est plus importante.

- 5 Ainsi, le système de communication 100 est capable d'émettre des émissions acoustiques qui, si elles sont interceptées par des récepteurs non ciblées, ne permettent pas la détection de l'émetteur.

10 Par exemple, l'émetteur peut être un sous-marin équipé du dispositif émetteur 101 pour transmettre des signaux de communication à des récepteurs de type bâtiments « amis », sans que ces émissions ne permettent la détection du sous-marin par un tiers hostile. Les signaux de communication peuvent être émis par des sonars actifs agencés sur le sous-marin et inclure tout type d'information.

- 15 Le système de communication 100 n'est toutefois pas limité à une utilisation dans un sous-marin et peut être utilisé dans différents types d'applications, comme par exemple dans des systèmes IFF (acronyme pour « Identification Friend or Foe » signifiant reconnaissance ami/ennemi), dans des systèmes de communications sans fil avec des Robots sous-marin autonomes (AUV, acronyme pour « Autonomous Underwater Vehicle »), sur des planeurs, sur des plongeurs ou
20 encore sur des objets équipés de capteurs posés sur le fond marin.

La figure 2 est un organigramme décrivant le procédé d'émission d'un signal audio par l'émetteur, selon certains modes de réalisation.

25

Le signal d'origine correspond à un élément anodin du bruit ambiant enregistré au préalable.

- 30 Dans la première étape 200 du procédé d'émission, la durée totale d'un signal initial $x(t)$, dérivé du signal d'origine par une opération élémentaire (par exemple filtrage passe-bande), est divisée en un ensemble d'intervalles successifs jointifs et sans recouvrement, de même durée T , par exemple de l'ordre de quelques centaines de ms.

A l'étape 202, l'opérateur de transformation Ψ est appliqué au signal initial sur chacun de ces intervalles. L'opérateur de transformation Ψ calcule, à partir du signal initial $x(t)$, un signal auxiliaire de même durée T et d'énergie sensiblement
 5 identique (au moins approximativement), dans la même bande de fréquence.

A l'étape 204, le signal à émettre sur le $n^{\text{ième}}$ intervalle $[nT, (n+1).T]$, noté $y(t)$, est déterminé en fonction du signal initial $x(t)$, du signal auxiliaire $\Psi(x)(t)$ et du symbole a_n . En particulier, le signal $y(t)$ peut être obtenu en ajoutant au signal
 10 initial le signal $q(t)$, ce signal $q(t)$ dépendant du produit entre le signal auxiliaire $\Psi(x)(t)$ et le symbole a_n . Dans un mode de réalisation, le signal à émettre sur le $n^{\text{ième}}$ intervalle $[nT, (n+1).T]$, noté $y(t)$, est choisi égal à :

$$y(t) = x(t) + \alpha \cdot a_n \cdot \Psi(x)(t) \quad (\text{Equation 1})$$

15 Dans l'équation 1 :

- $\alpha \cdot a_n \cdot \Psi(x)(t)$ correspond au signal ajouté $q(t)$,
- a_n désigne un symbole d'information transmis sur l'intervalle (par exemple. $a_n = \pm 1$) si une modulation binaire à deux états de phase BPSK est utilisée, et
- α désigne un gain < 1 , choisi suffisamment faible pour que le signal $y(t)$ soit
 20 proche du signal initial $x(t)$.

Le signal initial $x(t)$ dérivé du signal d'origine peut correspondre au signal complexe en bande de base, obtenu après filtrage du signal initial $x(t)$ dans une bande de fréquence de largeur B centrée sur une fréquence centrale ou porteuse
 25 F_c . L'utilisation d'un tel signal dérivé permet d'utiliser d'autres types de modulations à plus de deux états de phase, avec une meilleure efficacité spectrale que la modulation BPSK, comme par exemple des modulations QPSK, QAM16, QAM64, ce qui augmente le débit atteignable.

30 Selon une autre caractéristique, les symboles a_n peuvent être basés sur un codage différentiel (DPSK), ce qui présente des avantages en termes de robustesse dans un environnement difficile. En variante, il est également possible

de transmettre un ou plusieurs symboles connus afin de pouvoir identifier et compenser la phase du canal acoustique (poursuite et égalisation de phase).

En variante, le signal initial $x(t)$ dérivé du signal d'origine peut correspondre au signal d'origine réel. Dans ce cas, l'équation 1 peut être appliquée en ajoutant l'amplitude du signal initial $x(t)$ à l'amplitude relative du signal auxiliaire préalablement multipliée par le module des symboles a_n portant l'information cachée, et le cas échéant par le gain α . L'utilisation de l'amplitude permet d'augmenter les débits de manière significative en utilisant des constellations de type QAM, par exemple QAM16 ou QAM 64, avec 4 ou 6 bits par symboles.

Pour réduire le taux d'erreur binaire, des méthodes de codages de canal peuvent être appliquées, comme par exemple une technique de code correcteur d'erreur telles que le code Reed-Solomon ou les codes convolutifs, avec entrelacement et/ou brouillage des bits à émettre par application d'un xor avec une séquence pseudo-aléatoire longue et connue pour limiter les problèmes liés à l'émission de longues séquences de 0 ou de 1.

Dans une première forme de réalisation des étapes de division et d'association 200 et 204, chaque intervalle de temps de durée T peut être encore divisé en $2M$ sous-intervalles, notés $U_{-M}, \dots, U_{-1}, U_1, \dots, U_M$, séparés par de courts intervalles de garde (par exemple de l'ordre du 1/10 de la durée des intervalles U_k), avec des durées croissant avec $|k|$, comme illustré sur le schéma de la figure 3.

A l'étape 202, l'opérateur Ψ est alors choisi tel que la valeur du signal auxiliaire $\Psi(x)(t)$ sur chaque sous-intervalle U_k (pour $t \in U_k$) dépend :

- de la valeur du signal initial $x(t)$ sur le sous-intervalle U_{-k} (et réciproquement), après retournement temporel (en remplaçant t par $-t$),
- d'une phase $\exp j\beta_k$, et
- d'une fonction de pondération d'amplitude $p(t)$.

En particulier, la valeur du signal auxiliaire $\Psi(x)(t)$ à un instant $(T/2 + t)$ pour t appartenant à un sous intervalle U_k (pour $t \in U_k$) peut être fonction du produit

entre la valeur du signal initial $x()$ à l'instant $(T/2 - t)$, de la phase $\exp j.\beta_k$, et de la valeur de la fonction de pondération d'amplitude $p()$ à l'instant t . Dans un mode de réalisation, le signal auxiliaire est obtenu selon l'équation 2 ci-dessous :

$$\Psi(x) (T/2 + t) = \exp j.\beta_k . p(t) . x(T/2 - t) , \text{ si } t \in U_k \text{ (Equation 2).}$$

5

Le signal $x(T/2 - t)$ est égal au signal $x(T/2 + t)$ après application d'un retournement temporel autour de l'instant de référence $T/2$.

La pondération d'amplitude $p(t)$ de l'équation 2 peut correspondre par exemple à une pondération de type Tuckey sur une durée de temps égale à la durée du sous-intervalle considéré U_k , avec un front de montée et de descente de durée de l'ordre de 5%. Une telle pondération permet d'éviter l'apparition d'un transitoire large bande à chaque transition entre sous-intervalles ce qui nuirait à la discrétion de la transmission.

15

Dans les modes de réalisation où la fonction de pondération $p(t)$ est une pondération de Tuckey, la pondération peut être définie sur l'intervalle $[0, T]$ par les équations suivantes :

$$\begin{aligned} p(t) &= \sin^2 (\pi. t / (2 r T)) & \text{si } 0 \leq t < rT \\ 20 \quad p(t) &= 1 & \text{si } rT \leq t < (1-r) T \\ p(t) &= \sin^2 (\pi. (T-t) / (2 r T)) & \text{si } (1-r).T \leq t < T \end{aligned}$$

Dans les équations ci-dessus, le paramètre r désigne un paramètre (notamment pris entre 0 et 0.5) qui permet d'ajuster la largeur des fronts de montée et descente de la fonction de pondération. Par exemple, le paramètre r peut être pris égal à 0.05.

25

Les termes de phases « $\exp j.\beta_k$ » de l'équation 2, avec k compris dans l'intervalle $[-M, M]$, et β_k compris dans l'intervalle $[0, 2\pi]$ sont utilisés pour brouiller le signal auxiliaire $\Psi(x)(t)$, rendre sa reconstruction, et sa détection impossible par un tiers qui ne les connaîtrait pas. Ils constituent ainsi la clé stéganographique du système de communication (ici par exemple une clé de longueur $2M$) nécessaire pour retrouver l'information cachée.

30

Dans un exemple de réalisation, le paramètre de phase $\exp j\beta_k$ peut être limité à deux valeurs -1 et/ou +1.

- 5 Il doit être noté que pour $\exp j\beta_k = 1$ (k appartenant à $[-M, M]$), le signal auxiliaire $\Psi(x)(t)$ sur l'intervalle $[nT, n+1T]$ correspond à une copie retournée temporellement du signal initial sur ce même intervalle.

En plus de ses propriétés satisfaisantes en termes de discrétion, cet opérateur de transformation Ψ conduit à un système relativement robuste au doppler, pour des
10 longueurs des sous-intervalles U_k et des intervalles de garde choisis. Par exemple, pour un doppler constant (autrement dit un facteur de dilatation temporel $q = 1 + V/c$, avec V désignant la vitesse radiale de l'émetteur/récepteur, et c désignant la célérité du son), les signaux sont déformés de manière identique sur
15 les sous-intervalles U_k et U_k (le système est donc robuste au doppler). Les intervalles de garde, correspondant aux espaces entre les sous-intervalles U_k et U_{k+1} , peuvent être choisis de sorte que chacun des sous-intervalles U_k , après dilatation et/ou compression due au doppler ne recouvre pas ses voisins. Le système peut alors être rendu robuste au doppler en compensant à la réception la
20 différence entre la valeur de la fréquence porteuse nominale, F_c , et celle de la porteuse affectée par le Doppler, « $q \cdot F_c$ ».

Différents types d'opérateurs de transformation Ψ résultant de permutations quelconques entre les signaux sur les sous-intervalles U_k , avec ou sans
25 retournement temporel sur chaque sous-intervalle peuvent aussi être choisis. Avec de tels opérateurs de transformation Ψ , il peut être utile de compenser le résidu de la fréquence porteuse ainsi que la compression/dilatation résultant du doppler.

30 La figure 4 illustre un exemple de réalisation des étapes 200 et 202, selon la première forme de réalisation. Cette figure montre :

- (a) le signal initial $x(t)$ sur un intervalle de durée T , divisé ici en quatre sous-intervalles U_{-2} , U_{-1} , U_1 , U_2 ,

- (b) le signal après permutation des signaux sur U_{-2} et U_2 , puis U_{-1} et U_1 ,
- (c) le signal après retournement temporel du signal sur l'ensemble des sous-intervalles U_k ,
- (d) le signal résultant après multiplication par les termes de phase qui
5 constituent la clé stéganographique, ici $(1, -1, -1, 1)$,
- (e) le signal après application d'une pondération $p(t)$ pendant les intervalles de garde aux transitions entre sous-intervalles.

Les figures 5 et 6 montrent des exemples de résultats obtenus en appliquant le
10 procédé d'émission de la figure 2, selon la première forme de réalisation, pour des signaux recueillis en mer correspondant à une séquence de 10 secondes de clics de cachalot. Les figures 7 et 8 montrent d'autres exemples de résultats obtenus en appliquant le procédé d'émission de la figure 2, selon la première forme de réalisation, pour des signaux recueillis en mer correspondant à une séquence de
15 25 secondes de bruit de pluie.

Plus particulièrement, les figures 5 et 7 représentent le signal original $x(t)$ dans chacun des cas (clics de cachalot et bruits de pluie) tandis que les figures 6 et 8 représentent respectivement les signaux modifiés correspondants obtenus par
20 addition du signal auxiliaire avec ajout d'information cachée (par multiplication du signal auxiliaire par le symbole a_n). Dans les deux exemples considérés, l'information a été ajoutée dans la bande 1500-3000 Hz, avec un débit égal à 2 bits/sec, avec une période T de 0.5 seconde, une modulation BPSK (acronyme pour « Binary-phase shift Keying » signifiant « par changement de phase
25 binaire »), sans code correcteur d'erreur, et un gain α pris égal à -10 dB.

Il peut être observé que les sonagrammes des signaux initiaux et modifiés sont quasiment indiscernables, ce qui montre le caractère discret de la modulation.

30 La figure 9 est un organigramme décrivant le procédé de réception du signal émis, selon certains modes de réalisation.

Le signal reçu par le récepteur peut être avantageusement exploité, si le signal auxiliaire est ajouté à un faible niveau par rapport au signal initial. Ce faible niveau permet de calculer une approximation efficace du signal auxiliaire, de le détecter et de retrouver l'information cachée par un filtrage adapté.

5

A l'étape 300, une approximation du signal auxiliaire reçu $\Psi(x)(t)$ (encore appelé ci-après « signal auxiliaire reconstruit ») est déterminée en calculant $\Psi(y)(t)$.

10 A l'étape 302, une quantité $z(t)$ est calculée en appliquant un filtre adapté au signal auxiliaire reconstitué $\Psi(x)(t)$, le signal auxiliaire étant échantillonné temporellement à $F_e > 2B$ selon le critère de Nyquist. La quantité $z(t)$ est donnée par l'équation 3 ci-dessous :

$$z(t) \triangleq \int_0^T [\Psi(y)(u)]^* \cdot (u)y(u) \cdot e^{-2i\widehat{\theta}u} du \quad (\text{Equation 3})$$

15

Dans l'équation 3, le terme $e^{-2i\widehat{\theta}u}$ est introduit pour compenser le résidu de porteuse $F_c \cdot V/c$ (correspondant à l'écart entre la fréquence porteuse avec doppler $F_c (1+V/c)$ et la fréquence porteuse nominale F_c). Ce terme $e^{-2i\widehat{\theta}u}$ est estimé en maximisant à chaque instant le module de la quantité $z(t)$ pour un ensemble de 20 2.R+1 de valeurs possibles de θ , notées θ_r , selon l'équation 4 suivante :

$$\theta_r = 2\pi \cdot r \cdot F_c \cdot \Delta V/c \quad \text{pour } -R \leq r \leq R,$$

Dans l'équation 4 :

- ΔV désigne le pas entre vitesses possibles du maillage en vitesse ;
- c désigne la célérité du son.

25

A l'étape 304, des maxima séparés de T sont recherchés dans le module du signal $z(t)$ (le module de $z(t)$ est noté $|z(t)|$), avec une tolérance qui peut être fonction du doppler maximal.

30 A l'étape 305, les phases du signal $z(t)$ sont calculées aux instants correspondant à ces maxima.

A l'étape 306, les symboles et les bits transmis sont déterminés à partir des phases calculées à l'étape 305, ce qui fournit l'information cachée.

5 Le procédé de réception peut en complément comprendre une étape de synchronisation basée sur la recherche et l'extraction de pics de corrélation à une fréquence proche de la fréquence attendue pour les pics, égale à $1/T$ (par exemple avec une tolérance fonction du doppler maximal attendu).

10 Les figures 10 et 11 illustrent les étapes 302 à 306 pour un exemple de réalisation où un signal d'origine a été simulé dans un canal acoustique doublement étalé (en temps et fréquence). Le canal acoustique a été simulé avec les paramètres de simulation suivants :

- Fréquence porteuse: 2250 Hz - Bande : [1500-3000] Hz,
- Distance émetteur/récepteur : 5000 m
- 15 - Hauteur d'eau 100 m (fond plat)
- Immersion émetteur et récepteurs égales à 5 et 60 mètres
- Etalement doppler : 0.5 Hz

20 Un tel canal acoustique simulé correspond à un canal acoustique sous-marin typique en environnement côtier, moyennement difficile pour les communications acoustiques.

Le résultat de l'étape 302 est représenté sur les figures 12 et 13, en module, pour les deux exemples de signaux initiaux considérés sur les figures 5 à 8 (clics de cachalot et bruit de pluie), après propagation dans le canal acoustique et addition
25 d'un bruit additif blanc gaussien blanc, avec un rapport signal-sur bruit égal à 0 dB dans la bande de fréquences 1500-3000Hz où l'information est transmise. Le rapport signal-sur-bruit est égal au rapport des énergies du signal acoustique total et du bruit. Le rapport signal utile-sur-bruit, c'est à dire énergie du signal auxiliaire
30 ajouté, avec le gain $\alpha < 1$, porteur de l'information peut être plus faible. Dans les exemples des figures 12 et 13, un doppler non nul, pour une vitesse radiale égale à 1.7 m/s, a été simulé en ré-échantillonnant le signal émis avant passage dans le canal et ajout du bruit gaussien.

Les figures 14 et 15 illustrent les symboles estimés obtenus à l'étape 306, après synchronisation et compensation du déphasage dû au canal, selon un exemple de réalisation utilisant un symbole connu émis au début de la transmission.

5

Il peut être observé que les symboles sont correctement estimés, le message transmis (de 16 bits pour la figure 14 ou de 50 bits pour la figure 15) étant récupéré sans erreur.

Dans une deuxième forme de réalisation des étapes de division et d'association
10 200 et 204, l'intervalle T est divisé en M sous-intervalles de même durée T/M (étape 200). A partir du signal sur chaque intervalle T , le signal auxiliaire $\Psi(x)(t)$ peut être ensuite déterminé (étape 202) à partir du signal initial $x(t)$ au moyen d'une ou plusieurs permutations quelconques entre les morceaux du signal initial sur les sous-intervalles (i.e. la valeur du signal auxiliaire sur un sous-intervalle de
15 temps donné est obtenue à partir de la valeur du signal initial sur un autre sous-intervalle), retournés temporellement ou non pour chaque sous-intervalle (i.e. la valeur du signal auxiliaire à un instant t appartenant à sur un sous-intervalle de temps donné peut être obtenue à partir de la valeur du signal initial à l'instant $-t$ sur un autre sous-intervalle). Les permutations et les retournements temporels
20 appliqués constituent alors la clé stéganographique du système, qui peut être plus riche ou longue que pour dans la première forme de réalisation de l'étape d'association 202.

L'étape 204 peut ensuite être mise en œuvre comme décrit précédemment en
25 relation avec la figure 2 (ajout du signal auxiliaire multiplié par le symbole dont l'amplitude et/ou la phase porte l'information et le cas échéant par un gain α). Par ailleurs, le procédé de réception, tel que décrit en relation avec la figure 9, peut être appliqué similairement dans cette deuxième forme de réalisation.

30 La figure 16 illustre un exemple de réalisation des étapes 200 et 202, selon la deuxième forme de réalisation. Cette figure montre :

(a) le signal initial $x(t)$ sur un intervalle de durée T , divisé en trois sous-intervalles U_1 , U_2 , U_3 ,

(b) le signal après permutation des signaux sur les sous-intervalles : le signal sur U_1 est permuté avec le tronçon de signal sur U_2 , le signal sur U_2 est permuté avec le tronçon de signal sur U_1 , et le signal sur U_3 est permuté avec le tronçon de signal sur U_3 (la permutation peut alors être notée $(1,2,3) \rightarrow (2,1,3)$)

(c) le signal après retournement temporel sur les sous intervalles 2 et 3, puis produit par les termes de phase $(-1, 1, -1)$.

10 Les opérations successives b et c permettent d'obtenir le signal auxiliaire $\Psi(x)(t)$.

Un exemple d'application de la deuxième forme de réalisation est représenté sur les figures 17 et 18. Dans cet exemple, l'émetteur et le récepteur sont fixes, le canal est idéal, et le signal initial (représenté sur la figure 17) correspond à l'enregistrement de clics de cachalot de 8 secondes. Chaque intervalle de 1 seconde a été divisé en 32 sous-intervalles entre lesquels le signal a été permuté comme expliqué ci-dessus.

Les résultats obtenus apparaissant sur les figures 17 et 18 sont comparables en termes de débit atteignable à ceux obtenus avec la première forme de réalisation des étapes 200 et 202 (figures 5 et 6). Ces résultats peuvent apparaître moins satisfaisants en termes de discrétion, du fait que le signal a été utilisé dans toute la bande 0-4 kHz et sans pondération d'amplitude, les sauts entre sous-intervalles créant un bruit large bande qui apparaît en observant finement les figures 17 et 18. Une pondération en amplitude permet d'améliorer la situation.

Il convient de noter que la ressemblance entre le signal modifié (figure 18) et le signal initial (figure 17) est excellente de sorte qu'il est difficile de détecter que le signal initial a été modifié.

30

La figure 19 illustre la sortie du dispositif de réception obtenue pour le signal modifié de la figure 18. La figure 19 montre un ensemble de pics espacés de 1 seconde et d'amplitudes proches de +1 ou -1, à une constante multiplicative près,

correspondant parfaitement à la séquence de huit bits émise (transmission sans erreur).

La deuxième forme de réalisation des étapes 200 et 202 présente l'avantage de
5 fournir une clé stéganographique très riche. Il peut être utile de la rendre plus robuste au doppler, en compensant le résidu de porteuse comme dans la première forme de réalisation de ces étapes 200 et 202, et /ou en compensant en outre la dilation/compression du signal complexe bande de base autour de la porteuse (enveloppe) avec une précision de l'ordre de l'échantillon temporel.

10

Dans les modes de réalisation où l'antenne de réception comprend plusieurs hydrophones 12, le procédé de réception décrit en relation avec la figure 8 peut être appliqué en parallèle aux signaux correspondant à l'ensemble des voies formées (par exemple, les voies peuvent être formées sur tout l'horizon en
15 l'absence d'information a priori sur la position de l'émetteur).

L'invention permet ainsi de réémettre un signal préalablement enregistré et modifié de manière à porter de l'information grâce à l'ajout d'information au moyen d'un signal auxiliaire calculé à partir du signal initial et de l'information à cacher,
20 selon l'opérateur de transformation qui dépend d'une clé stéganographique, la connaissance de cette clé étant nécessaire pour détecter qu'une information est cachée et retrouver cette information.

Le système de communication 100 peut utiliser des signaux naturels (tels que les
25 bruits biologiques, les travaux sous-marins, le bruit ambiant, etc.) et les modifier de manière imperceptible pour y inclure de l'information (par exemple, courts messages, de type SMS). L'accès à l'information cachée n'est possible qu'en utilisant la clé stéganographique connue seulement de l'émetteur et du récepteur.

Par conséquent, le signal émis apparaît à tout tiers parfaitement naturel et peut être parfaitement adapté à la zone d'émission et au moment de l'émission (par exemple si le signal initial a été recueilli sur la zone quelques minutes ou quelques heures avant sa ré-émission).

30

L'utilisation d'une pondération d'amplitude $p(t)$ en émission et/ou réception permet de limiter les transitoires large bande aux transitions entre sous-intervalles et rendre plus discrète l'insertion d'information.

5

Le système de communication 100 peut s'appliquer à tous types de signaux à large bande, ce qui est le cas de nombreux signaux constitutifs du bruit ambiant sous-marin.

10 Bien qu'il ne soit pas limité à un tel environnement, le système de communication 100 est particulièrement adapté à un environnement fortement bruité et peut être rendu insensible au doppler.

15 L'invention n'est pas limitée aux modes de réalisation décrits ci-avant à titre d'exemple non limitatif. Elle englobe toutes les variantes de réalisation qui pourront être envisagées par l'homme du métier.

Revendications

1. Dispositif émetteur (101), comprenant une antenne d'émission, l'antenne d'émission comprenant au moins un transducteur et une unité de génération de signal (120) pour générer un signal de communication acoustique à émettre vers
 5 un dispositif récepteur incluant de l'information cachée, caractérisé en ce que l'unité de génération de signal est configurée pour enregistrer au préalable un signal acoustique d'origine, ladite unité de génération de signal étant apte à générer ledit signal de communication à émettre en ajoutant à un signal initial $x(t)$, dérivé du signal d'origine, un signal auxiliaire préalablement multiplié par au moins
 10 un symbole, ledit symbole ayant une phase et/ou une amplitude portant l'information cachée et ledit signal auxiliaire étant calculé à partir du signal initial au moyen d'un opérateur de transformation choisi qui dépend d'une clé stéganographique.

2. Dispositif émetteur selon la revendication 1, caractérisé en ce que le signal
 15 initial dérivé du signal d'origine est le signal complexe en bande de base obtenu après filtrage du signal d'origine dans une bande de fréquences de largeur choisie, centrée sur une fréquence centrale.

3. Dispositif émetteur selon l'une des revendications précédentes, caractérisé en ce que l'unité de génération de signal est configurée pour diviser au préalable la
 20 durée totale du signal d'origine $x(t)$ en un ensemble d'intervalles de temps successifs jointifs de même durée T , l'opérateur de transformation étant appliqué au signal initial sur chacun desdits intervalles pour calculer la valeur du signal auxiliaire correspondante sur ledit intervalle.

4. Dispositif émetteur selon la revendication 3, caractérisé en ce que le signal
 25 généré $y(t)$ à un instant t appartenant au n -ième intervalle $[nT, (n+1)T]$ est égal à :

$$y(t) = x(t) + \alpha \cdot a_n \cdot \Psi(x)(t),$$

où α désigne un paramètre de gain et a_n désigne le symbole correspondant au $n^{\text{ième}}$ intervalle.

5. Dispositif émetteur selon l'une des revendications 3 et 4, caractérisé en ce que
 30 l'unité de génération de signal est en outre configurée pour diviser chaque la

durée du signal en un ensemble d'intervalles successifs jointifs de même durée T , et chaque intervalle de durée T en $2M$ sous-intervalles $U_{-M}, \dots, U_{-1}, U_1, \dots, U_M$, séparés par des intervalles de garde, lesdits sous-intervalles ayant des durées croissantes en fonction de la valeur absolue de k , et en ce que l'opérateur de transformation est appliqué au signal initial sur chaque sous-intervalle U_k pour calculer la valeur du signal auxiliaire correspondante sur ledit intervalle.

6. Dispositif émetteur selon la revendication 5, caractérisé en ce que la valeur du signal auxiliaire $\Psi(x)(T/2 + t)$ à un instant $T/2 + t$, avec t appartient à un sous-intervalle U_k , est fonction d'un paramètre de phase $\exp j.\beta_k$, avec β_k compris dans l'intervalle $[0, 2\pi]$ et k compris dans l'intervalle $[-M, M]$, de la valeur d'une fonction de pondération d'amplitude $p(t)$ à l'instant t , et de la valeur du signal initial à l'instant $(T/2 - t)$.

7. Dispositif émetteur selon la revendication 6, caractérisé en ce que la valeur du signal auxiliaire $\Psi(x)(T/2 + t)$ à un instant $T/2 + t$, où t appartient à un sous-intervalle U_k , est égale à :

$$\Psi(x)(T/2 + t) = \exp j.\beta_k . p(t) . x(T/2 - t).$$

8. Dispositif émetteur selon l'une des revendications 5 à 7, caractérisé en ce que la durée des intervalles de garde entre les sous-intervalles de temps successifs U_k et U_{k+1} est choisie de sorte que chacun des sous-intervalles U_k ne recouvre pas ses voisins après dilatation/compression due à un phénomène doppler.

9. Dispositif émetteur selon l'une des revendications 3 et 4, caractérisé en ce que l'unité de génération de signal est en outre configurée pour diviser chaque intervalle de durée T en un ensemble de M sous-intervalles de même durée T/M , et en ce que la valeur du signal auxiliaire sur un sous-intervalle de temps donné est obtenue à partir de la valeur du signal initial sur un autre sous-intervalle.

10. Dispositif émetteur selon la revendication 9, caractérisé en ce que la valeur du signal auxiliaire à un instant t appartenant à sur un sous-intervalle de temps donné est obtenue à partir de la valeur du signal initial à l'instant $-t$ sur un autre sous-intervalle.

11. Dispositif émetteur selon l'une des revendications 9 et 10, caractérisé en ce que la valeur du signal auxiliaire à un instant t appartenant à un sous-intervalle de temps donné est obtenue à partir de la valeur du signal initial sur un autre sous-intervalle pondérée par la valeur d'une fonction de pondération d'amplitude $p(t)$ à l'instant t .

12. Dispositif récepteur (102), comprenant une antenne de réception, l'antenne de réception comprenant au moins un hydrophone, caractérisé en ce qu'il comprend un détecteur (151) pour détecter un signal de communication émis par un dispositif émetteur (101) selon l'une des revendications 1 à 11 et une unité d'extraction (152) configurée pour reconstituer le signal auxiliaire en appliquant ledit opérateur de transformation au signal de communication détecté à partir de la clé stéganographique, et pour extraire l'information cachée à partir de la phase et/ou de l'amplitude du signal auxiliaire reconstruit.

13. Dispositif récepteur selon la revendication 12, caractérisé en ce que l'unité d'extraction est en outre configurée pour appliquer un filtre au signal reconstitué à partir d'un terme de compensation $e^{-i\hat{\theta}u}$ propre à compenser le résidu de la porteuse correspondant à l'écart entre la fréquence porteuse avec doppler et la fréquence porteuse nominale, le terme de compensation étant estimé en maximisant, à chaque instant t , le module de la sortie $z(t)$ du filtre pour un ensemble de valeurs possibles de θ , et en ce que la fonction d'extraction est apte à déterminer les symboles et les bits de l'information cachée à partir des phases du signal $z(t)$ calculées à des instants correspondants aux maxima du module du signal $z(t)$.

14. Système de communication comprenant un dispositif émetteur selon l'une des revendications 1 à 12 et un dispositif récepteur selon l'une des revendications 12 et 13.

15. Procédé d'émission pour générer un signal de communication acoustique dans un dispositif émetteur (101), comprenant une antenne d'émission (1), l'antenne d'émission comprenant au moins un transducteur, le procédé comprenant les étapes suivantes :

- a. enregistrer un signal acoustique d'origine ;
- b. ajouter à un signal initial $x(t)$, dérivé dudit signal d'origine, un signal auxiliaire multiplié par au moins un symbole, ledit symbole ayant une phase et/ou une amplitude portant l'information cachée et ledit signal auxiliaire étant calculé à partir
- 5 du signal initial au moyen d'un opérateur de transformation choisi qui dépend d'une clé stéganographique, ce qui fournit un signal de communication,
- c. émettre un signal vers un dispositif récepteur à partir du signal de communication obtenu à l'étape b.