République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. MIRA - Bejaïa

Faculté des sciences exactes
Département informatique
Système LMD

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme d'un Master professionnel

Option : Génie Logiciel

Thème

Conception et réalisation d'un système de messagerie à base de la stéganographie

Réalisé et Présenté par :

- M me DIB Thiziri
- Mme BOUDJEMA Tinhinane

Sous la direction de :

Mme YESSAD Nawal

Devant le jury composé de :

- **Présidente :** Dr S. LAHLAH MCB Université A/Mira
- **Examinatrice :** Dr N. BOUADEM MCB Université A/Mira
- **Encadrante :** Dr N. YESSAD MCB Université A/Mira

Année universitaire : 2022/ 2023

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

LSB	Least Significant Bit.
RSA	Rivest-Shamir-Adleman.
UML	Unified Modeling Language.
XP	Extreme Programming.
OTP	One-Time Password.
DCT	Discrete Cosine Transform.
IDE	Integrated Development Environment.
SDK	Software Development Kit.
VS code	Visual Studio Code.
mac OS	Macintosh Operating System.
MTPoto	Mobile Transport Protocol
WAV	Waveform Audio File
RAD	Rapid Application Development
IOS	iPhone Operating System

Remerciments

Nous tenons avant tout à exprimer notre gratitude à Allah Tout-Puissant. Grâce à Dieu, nous avons pu atteindre nos objectifs et réaliser ce travail.

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de Mme.YESSAD Nawal , nous la remercions pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant notre préparation de ce mémoire.

Nous remercions les membres du jury d'avoir pris la peine de lire et de juger ce travail.

Nos remerciements s'adressent également à tous nos professeurs de la spécialité pour leur aide.

Nos profonds remerciements vont également à toutes les personnes qui nous ont aidé et soutenu de près ou de loin .

Dédicaces

Je souhaite dédier ce travail à toutes les personnes qui ont joué un rôle important dans ma vie et m'ont soutenu tout au long de ce parcours. Tout d'abord, je voudrais exprimer ma profonde gratitude envers Dieu le tout-puissant pour sa guidance et son soutien constants.

Je suis reconnaissante envers mes chers parents, mon père ALI et ma mère HASSIBA, pour leurs encouragement et leurs amour inconditionnel, qui ont été essentiels à mes réalisations.

À mon petit frère MOHAMED, qui a toujours été là pour moi, je suis reconnaissante pour son soutien et son inspiration.

À mon mari ARIS et à ma belle-famille, je vous remercie d'avoir été une source constante de soutien et de motivation. Votre présence dans ma vie est une bénédiction.

Je tiens également à remercier mes grands-parents, mes grands-mères et mes grands-pères, pour leurs amours, leurs conseils et leurs sagesses précieuse.

À tous mes oncles, mes tantes, mes cousins et mes cousines, en particulier MERIEM, SARAH, TINHINENE, DYHIA, KENZA, SONIA, KATIA, FOUZIA, YOUBA et RAFIK, je vous suis reconnaissante pour vos encouragements et votre soutien indéfectible.

Je n'oublie pas nos petits anges de la famille : NARIMANE, GHILAS et SELYAN, qui apportent tant de joie à nos vies.

À mes amies proches : YASMINE, SONIA, YASMINE, FATIMA, NASSIMA et SABRINA, je vous remercie pour votre amitié précieuse et votre soutien constant.

Je tiens à exprimer ma reconnaissance envers Madame T. KAHINA pour son soutien et ses précieux conseils.

Toute la famille DIB, TARIKT, MOURI, AMEZIANE .

Et enfin, je voudrais exprimer ma gratitude envers ma binôme TINHINANE et sa famille pour leurs soutiens et leurs collaborations tout au long de ce travail.

Je vous suis reconnaissante à tous et je ne pourrais jamais assez-vous remercier pour votre soutien et votre affection sincère.

DIB Thiziri

Dédicaces

Rien n'est aussi beau à offrir que le fruit d'un labeur que je dédie du fond du cœur à ceux que j'aime.

À mes très chers parents AISSA et SAIDA qui ont toujours été là pour moi , qui ont sacrifié leur vie pour ma réussite et m'ont éclairé le chemin par leurs conseils judicieux. j'espère qu'un jour, je pourrai leur rendre un peu de ce qu'ils ont fait pour moi. Que dieu leur prête bonheur et longue vie.

À mes soeurs THANINA ,DIHIA, KATIA, LILYA mes compagnes de vie, mes confidentes qui ont toujours été là quand j'en avais le plus besoin.

À mes grands parents qui sont une source de réconfort et de soutien inébranlable dans ma vie,Je suis profondément reconnaissante pour les précieux moments passés à leurs côtés, Que dieu leur prête de bonheur, de santé et de joie, et sachez que vous êtes aimés et appréciés au-delà des mots.

Je tiens également à remercier mon oncle MOKRANE et sa femme KAHINA pour leur soutien indéfectible, leurs encouragements. Je suis reconnaissante de votre sens de l'humour et de votre générosité, sans oublier Mes chers AMEL, KHALED et LINA ces rayons de soleil qui illuminent ma vie.

Je tiens à remercier mes chers oncles NACER, ILYES et mes tantes pour leurs encouragements je suis tellement fière d'être votre nièce je vous aime.

À mes chers cousins et cousines Vous êtes des modèles de force, d'intégrité et de persévérance. Vos réalisations et vos réussites sont une source d'inspiration pour moi je vous remercie du fond du cœur pour votre soutien.

À mes chers amis YANIS, B. YASMINE, SONIA, FATIMA, NASSIMA, SABRINA, A .YASMINE, MIRA, SAMIRA, Anissa et KATIA ces personnes exceptionnelles qui sont devenues une partie essentielle de ma vie. Votre amitié sincère, Votre soutien inconditionnel et votre présence constante sont des trésors inestimables pour moi.

Je tiens à exprimer ma reconnaissance envers Madame T. KAHINA pour son soutien et ses précieux conseils.

Toute la famille BOUDJEMA,ADJIR et LOUNIS.

Et enfin, je voudrais exprimer ma gratitude envers ma binôme THIZIRI et sa famille pour leurs soutiens et leurs collaborations tout au long de ce travail.

Je vous suis reconnaissante à tous et je ne pourrais jamais assez-vous remercier pour votre soutien et votre affection sincère.

BOUDJEMA Tinhinane

Introduction générale

La communication sécurisée et confidentielle est devenue un enjeu majeur dans notre société numérique avec l'expansion des technologies de l'information et de la communication, il devient primordial de mettre en place des mécanismes efficaces pour protéger nos échanges de données sensibles, dans ce contexte la stéganographie émerge comme une solution prometteuse pour assurer la confidentialité des messages échangés.

La stéganographie est l'art de dissimuler des informations secrètes au sein d'autres fichiers anodins contrairement au chiffrement classique qui rend les messages inintelligibles, la stéganographie permet de cacher la présence même des informations confidentielles ainsi elle offre un niveau supplémentaire de sécurité en rendant les messages indétectables par des tiers.

Dans ce mémoire, nous nous intéressons à la conception et à la réalisation d'une application de messagerie basé sur la stéganographie, l'objectif est de développer un outil qui permettra aux utilisateurs d'échanger des messages d'une manière sécurisée, en dissimulant le contenu des messages au sein de fichiers multimédias tels que des images, des audios ou des vidéos.

Pour mener à bien ce projet, nous avons établi un plan détaillé couvrant toutes les parties du travail, depuis la partie théorique jusqu'aux aspects de programmation et de mise en œuvre. Notre travail est divisé en quatre chapitres organisés de la manière suivante :

— **Le premier chapitre intitulé « Concepts de base de la stéganographie»** présente une vue d'ensemble de la stéganographie. Il aborde les concepts fondamentaux et les principes de base de cette discipline.

— **Le deuxième chapitre intitulé « Etude préliminaire »** offre un premier aperçu des différentes fonctionnalités qui seront présentes dans notre application nommée "MysterMessage" . Cette section permet de définir les besoins et les objectifs du projet, en identifiant les principales caractéristiques et fonctionnalités attendues.

— **Le troisième chapitre intitulé « Analyse et conception »** approfondit les détails des fonctionnalités clés de notre application "MysterMessage". C'est dans cette section que nous détaillons les spécifications techniques et les diagrammes de conception.

— **Le quatrième et le dernier chapitre intitulé « Implémentation »** se concentre sur la partie pratique de notre projet. Il décrit en détail les étapes de réalisation de notre application, en mettant l'accent sur les aspects de programmation.

Chapitre 1

Concepts de base de la stéganographie

1.1 Introduction

Dans ce chapitre, nous présentons tout d'abord quelques définitions de la stéganographie, afin de bien comprendre les concepts clés de la discipline, ainsi qu'un bref aperçu historique des techniques utilisées,cela nous permet de mieux appréhender la philosophie et les principes fondamentaux du domaine ensuite, nous explorons les bases de la stéganographie moderne et mettons en évidence les caractéristiques essentielles des schémas stéganographiques.

1.2 Définition de la stéganographie

La stéganographie vient du mot grec « steganos » qui veut dire cacher et le mot « graphein » qui veut dire écriture elle s'agit de cacher un message dans un fichiers inoffensif afin qu'ils ne puissent pas être détectés [**20**].

1.3 Historique de la stéganographie

La stéganographie est l'art de dissimuler des informations, ce dernier existe depuis longtemps bien avant l'invention de l'ordinateur, le premier exemple apparu vers les années 400 avant J.C. quelques-uns des plus anciens témoignages à propos de la dissimulation de l'écriture nous ramènent à Hérodote qui raconte dans sa chronique que les grecs pour se communiquer secrètement rasaient les cheveux d'un esclave lui tatoua le message sur le crâne une fois les cheveux sont repoussé l'esclave pouvait traverser le territoire ennemi sans éveiller les soupçons il suffisait alors de raser à nouveau l'esclave pour lire le message.

Hérodote raconte aussi que Damarto un roi grec exilé de la cité Perse de Susa a réussi de découvrir les préparative de Xerxès pour attaquer la Grèce il a voulu avertir Sparte il a donc retiré la cire des tables en bois et a écrit le message et les recouvert à nouveau avec de la cire. Dans les 2000 ans qui se sont écoulés depuis Hérodote, différentes formes de messages cachés ont été utilisées par le monde. Par exemple on écrit au milieu des texte déjà écrit à l'encre à l'aide de jus de citron, de lait au de certain produit chimique il est invisible à l'œil mais une simple flamme ou un bain dans un réactif chimique révèle le message comme la Figure 1.1 le représente [**8**].

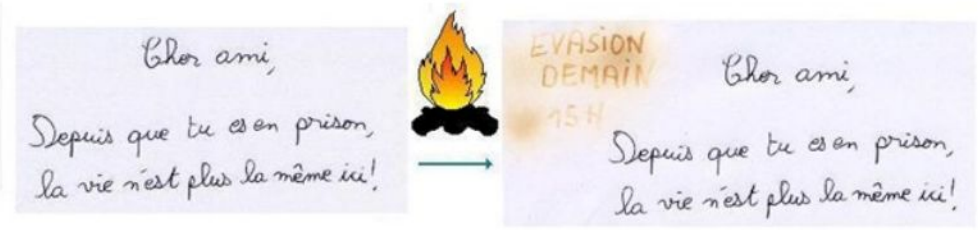

FIGURE 1.1 – Stéganographie d'encres sympathiques
[6]

La stéganographie a pris l'importance après l'apparition des réseaux informatiques et des canaux numériques Le domaine de la cryptographie a beaucoup avancé après la deuxième guerre.

1.4 Le principe de la stéganographie

La stéganographie consiste à cacher un message secret de grande taille à l'intérieur d'une image, d'un fichier audio ou vidéo existant, appelé média original, le résultat obtenu est appelé média stéganographique, qui ne semble pas différent du média original pour l'œil humain, en conséquence, la présence du message secret dans le média stéganographique est quasiment impossible à détecter,le message secret peut être sous forme de texte brut, de texte chiffré ou d'image [**7**]. La Figure 1.2 représente le principe de la steganographie.

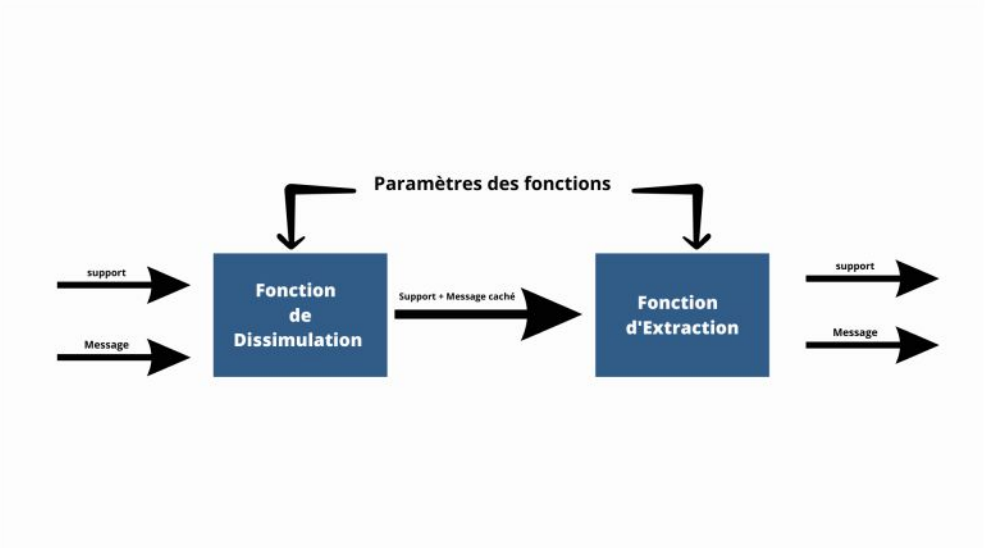

FIGURE 1.2 – Principe de la stéganographie.

1.5 Les types de la stéganographie

Il existe deux types de stéganographie :

— **Stéganographie linguistique :** toute forme de stéganographie qui emploie la langue dans le processus de dissimulation. Elle Consiste à modifier les propriétés linguistiques d'un texte pour cacher l'information, elle est la plus faible par rapport à d'autres médias, probablement parce qu'il est plus facile de modifier le média non linguistique dans lequel le message secret

ne peut pas être découvert par l'observateur [**20**].

— **Stéganographie technique :** ce type de stéganographie suscite un intérêt particulier des professionnels de l'informatique, il est défini comme l'art et la science de dissimuler une information privée ou secrète au sein d'un support numérique en apparence anodin, la particularité essentielle de cette méthode est que le support utilisé ne doit révéler aucune indication de la présence d'informations sensibles, il ne doit pas contenir de traces apparentes telles qu'une altération visible de l'image ou du fichier [**20**].

1.5.1 Les types de support

La stéganographie utilise divers types de supports pour atteindre l'objectif de la dissimulation l'un des plus courants est l'image mais ce dernier utilise également les vidéos et les audios.

— **Image :** La stéganographie image est très populaire de nos jours pour plusieurs raisons, tout d'abord, les images sont largement utilisées et partagées sur Internet, les réseaux sociaux et les plateformes de communication, ce qui les rend accessibles à un large public. Ensuite, la stéganographie image exploite les capacités limitées de notre perception visuelle. Les modifications imperceptibles apportées aux pixels d'une image permettent de dissimuler des données de manière difficilement détectable par un observateur.
Enfin, les images numériques offrent une grande capacité de stockage, ce qui permet de dissimuler des informations volumineuses, comme du texte, des documents ou d'autres images,de plus la stéganographie image peut être utilisée pour cacher pratiquement n'importe quel type de données en les encodant en binaire [**5**].

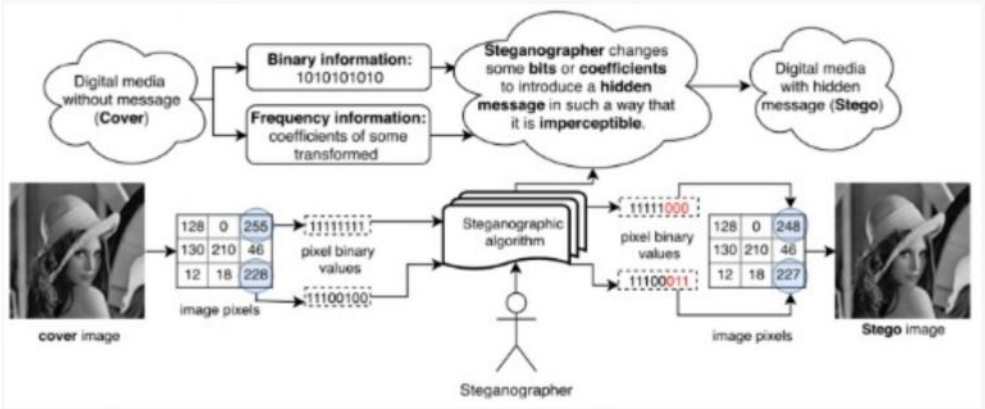

FIGURE 1.3 – Exemple d'encodage de données dans le bit de poids faible (LSB) [**3**]

— **Audio :** La stéganographie audio repose sur les limitations de l'oreille humaine en termes de plage de fréquences et de sensibilité aux variations d'amplitude du signal, malgré son utilisation moins répandue par rapport à d'autres supports, telle que l'image, l'audio offre des possibilités de dissimulation d'informations confidentielles dans des contextes de communication, tels que les appels téléphoniques ou les enregistrements vocaux, l'oreille humaine est

moins sensible aux variations subtiles des signaux audio, rendant plus difficile la détection d'informations dissimulées. Cependant, la stéganographie audio présente des limitations en termes de capacité de stockage et de logiciels spécifiquement dédiés.
En conclusion la stéganographie audio, bien que moins répandue, peut être utilisée dans des contextes spécifiques de communication pour dissimuler des informations, en exploitant les caractéristiques de l'oreille humaine [**9**].

La Figure 1.4 illustre une système de stéganographie audio

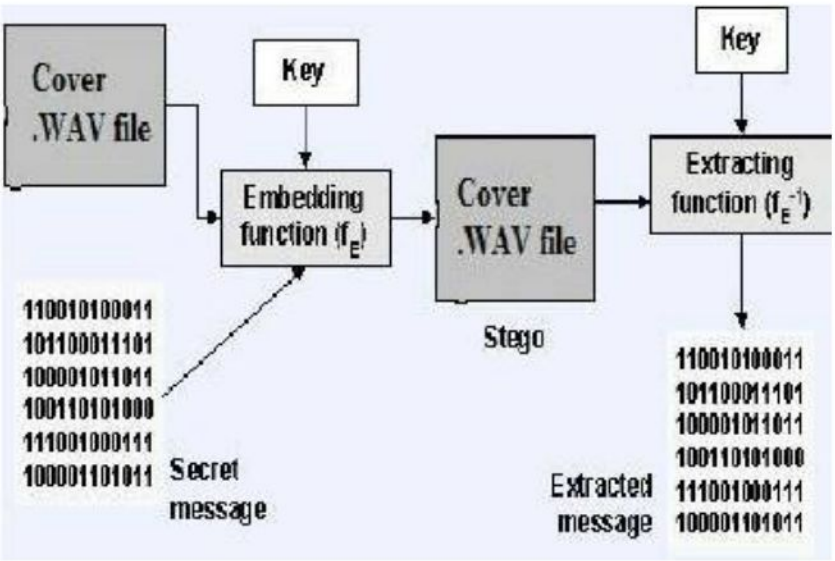

FIGURE 1.4 – Système de stéganographie audio
[**1**]

— **Vidéo :**
La dissimulation d'informations dans un support vidéo repose sur l'utilisation de la transformée en cosinus discret (DCT) pour encoder les données secrètes dans les coefficients de hautes fréquences, la DCT divise l'image en blocs de pixels et effectue une transformation mathématique pour obtenir une représentation en domaine fréquentiel, les coefficients de hautes fréquences, moins perceptibles pour les spectateurs, sont utilisés pour dissimuler les informations. Les techniques de stéganographie vidéo modifient de manière imperceptible les coefficients de hautes fréquences afin d'encoder les données secrètes. Cela permet de dissimuler les informations sans affecter de manière significative la qualité visuelle de la vidéo, cependant, la capacité d'insertion d'informations dans une vidéo est limitée en raison de contraintes telles que la quantité de coefficients disponibles et les limitations de qualité visuelle.
En conclusion, la dissimulation d'informations dans un support vidéo repose sur l'utilisation de la DCT pour encoder les données secrètes dans les coefficients de hautes fréquences, cette approche exploite la sensibilité de l'œil humain aux différentes fréquences présentes dans la vidéo, permettant ainsi de dissimuler les informations de manière imperceptible pour les

spectateurs [4]. La Figure 1.5 montre un diagramme de stéganographie védio

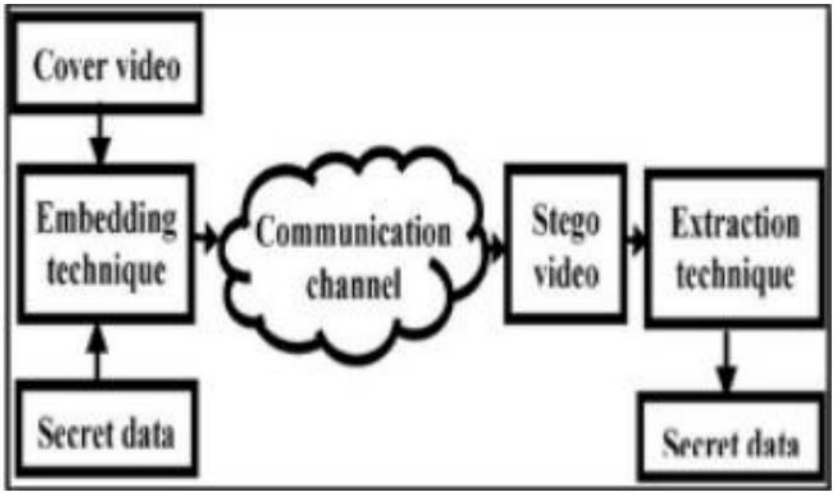

FIGURE 1.5 – Diagramme de stéganographie vidéo
[4]

1.6 Les méthodes de la stéganographie

La stéganographie utilise diverses méthodes pour dissimuler des informations secrètes dans un support numérique,ces méthodes sont conçues pour garantir la sécurité et la confidentialité des données cachées, tout en préservant l'apparence et la fonctionnalité du support utilisé, voici quelques-unes des méthodes les plus couramment utilisées en stéganographie :

1.6.1 Insertion dans le domaine spatial

La stéganographie par insertion dans le domaine spatial est une technique de stéganographie qui dissimule des informations secrètes dans l'espace entre les pixels d'une image,cette technique est souvent utilisée pour dissimuler des informations dans des images bitmap, où chaque pixel est défini par des informations de couleur,dans cette technique, les informations secrètes sont dissimulées en modifiant légèrement la couleur des pixels d'une image, les modifications apportées à l'image sont généralement très subtiles et ne sont pas visibles à l'œil nu, mais elles permettent de coder les informations secrètes.
La stéganographie par insertion dans le domaine spatial peut également être utilisée pour dissimuler des informations secrètes dans des fichiers audio et vidéo, dans le cas de la stéganographie audio, les informations secrètes peuvent être dissimulées en modifiant très légèrement les niveaux de volume des échantillons audio,dans le cas de la stéganographie vidéo, les informations secrètes peuvent être dissimulées en modifiant très légèrement les couleurs ou les niveaux de luminosité des pixels vidéo,la stéganographie par insertion dans le domaine spatial est souvent considérée comme une technique fiable de stéganographie, car les modifications apportées à l'image, audio ou la vidéo sont très subtiles et difficiles à détecter,cependant, elle peut également être affectée par des opérations telles que la compression, la rotation ou le redimensionnement, ce qui peut entraîner une perte de qualité ou une révélation accidentelle des informations secrètes [11]. Il existe deux types de technique de

steganographie insertion dans le domaine spatial :

— **Stéganographie par substitution de LSB (LSB Replacement)**

Le principe de cette technique consiste à substituer les bits de poids faibles (les LSB) des pixels par les bits de message à insérer, càd pour un message inséré m= (m1, . . ., mn) le bit de poids faible bi,de chaque pixel est remplacé par un bit du message à dissimuler le sens de parcours des pixels est choisi par un parcours pseudo-aléatoire, l'émetteur et le récepteur doivent échanger une clé utilisée comme un générateur de nombre de pseudoaléatoire. Pour les fichiers audio et vidéo, la substitution de LSB consiste à remplacer les bits les moins significatifs de chaque (échantillon audio) et (séquence vidéo) par un bit du message secret [**11**].

— **Stéganographie par correspondance de LSB (LSB Matching)**

La stéganographie par correspondance de LSB (LSB Matching) est une technique de stéganographie basée sur les bits similaire à la stéganographie par substitution de LSB, elle consiste à dissimuler des informations secrètes en comparant les bits les plus faibles d'un fichier à ceux d'un autre fichier, et en utilisant les différences pour coder les informations secrètes,dans cette technique, les bits les plus faibles d'un premier fichier (appelé "fichier porteur") sont comparés à ceux d'un deuxième fichier (appelé "fichier secret"), et les différences sont utilisées pour coder les informations secrètes, les bits modifiés du fichier porteur peuvent alors être utilisés pour dissimuler les informations secrètes. Bien que la stéganographie par correspondance de LSB soit plus difficile à détecter que la stéganographie par substitution de LSB, elle peut également être affectée par des opérations telles que la compression, la rotation ou le redimensionnement, ce qui peut entraîner une perte de qualité ou une révélation accidentelle des informations secrètes.
Il est donc important de choisir une technique de stéganographie qui convienne à vos besoins en matière de confidentialité et de sécurité [**11**]

1.6.2 Insertion dans le domaine transformé

L'insertion de données dans le domaine transformé est une méthode de stéganographie qui utilise une transformation mathématique pour cacher des informations à l'intérieur d'une image ou d'un signal audio. Par exemple, si nous avons une image, nous pouvons la transformer en utilisant une transformée de fourier qui décompose l'image en ses 5 composants fréquentiels. Nous pouvons ensuite cacher des informations en modifiant légèrement les composants fréquentiels. Lorsque nous avons terminé, nous pouvons utiliser la transformée inverse pour retransformer l'image. L'image aura toujours l'air normale pour quelqu'un qui ne sait pas que les informations sont cachées, mais si nous connaissons la méthode que nous avons utilisée pour cacher les informations, nous pouvons les récupérer [**11**].

1.7 Classification des schémas de la stéganographie

Cette section vise à présenter une variété de schémas utilisés en stéganographie. Elle explore les différentes approches et techniques utilisées pour dissimuler des informations secrètes dans divers sup-

ports. En examinant ces schémas, nous pourrons mieux comprendre les méthodes spécifiques utilisées pour masquer les données et les rendre invisibles

1.7.1 Stéganographie pure

La stéganographie pure est une méthode de stéganographie qui consiste à cacher des données dans un message de couverture sans aucun chiffrement ni algorithme de sécurité supplémentaire. Cette technique repose sur le fait que la présence de données cachées est difficile à détecter sans connaître la méthode utilisée pour les cacher [**5**].

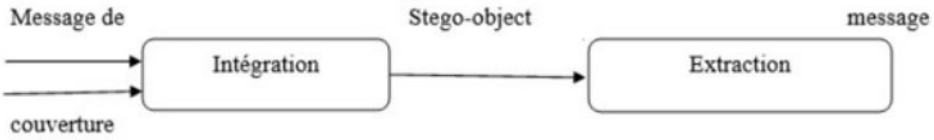

FIGURE 1.6 – Stéganographie pure
[**5**].

— **Encodage le message :** le message est encodé pour être inséré soit dans l'image, audio ou vidéo L'encodage permet de cacher le message d'une manière imperceptible pour l'œil humain ou l'oreille.

— **Intégration :** Le message encodé est inséré dans le message de couverture, généralement en modifiant certains bits ou pixels du fichier de couverture.

— **Envoi du message :** Le message avec les données cachées est envoyé au destinataire.

— **Extraction de message caché :** Le destinataire reçoit le message, extrait les données cachées en utilisant la même méthode d'encodage que celle utilisée pour les cacher.

Ce type de stéganographie ne peut pas fournir la meilleure sécurité parce qu'il est facile pour extraire le message si la personne non autorisée connaît la méthode d'incorporation. Il a un avantage à réduire la difficulté de partage des clés.

1.7.2 Stéganographie à clé secrète

La stéganographie à clé secrète est une méthode de stéganographie qui ajoute une couche de sécurité en utilisant un algorithme de chiffrement pour masquer les données cachées dans un message clair. Cette technique utilise une clé secrète partagée uniquement entre l'émetteur et le récepteur et les données cachées ne peuvent être récupérées qu'à l'aide de cette clé [**5**]..

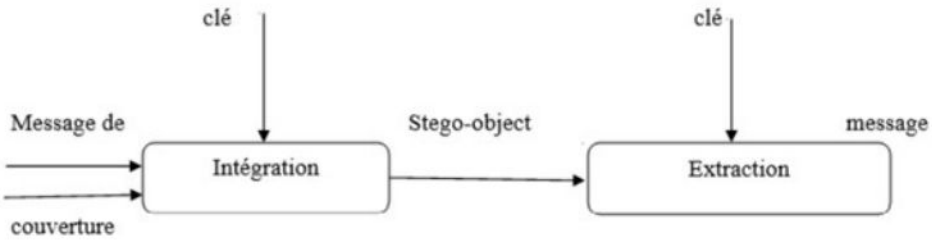

FIGURE 1.7 – Stéganographie à clé secrète
[5].

— **Chiffrement de message :** Le Message est chiffré à l'aide d'un algorithme de chiffrement symétrique, en utilisant une clé secrète partagée entre l'émetteur et le récepteur.

— **Encodage de message :** Le message chiffré est encodé pour être inséré dans le message de couverture, tel qu'un fichier image, audio ou vidéo. L'encodage permet de cacher le message d'une manière imperceptible pour l'œil humain ou l'oreille.

— **Intégration :** Le Message caché encodé est inséré dans le message de couverture, généralement en modifiant certains bits ou pixels du fichier de couverture.

— **Envoi du message :** Le message avec les données cachées est envoyé au destinataire.

— **Extraction le message caché :** Le récepteur reçoit le message de couverture, extrait les données cachées et déchiffre les données à l'aide de la clé secrète partagée.

Ce type de stéganographie offre une meilleure sécurité par rapport à la stéganographie pure. Le problème principal de l'utilisation de ce type de système stéganographie est le partage de la clé secrète. Si l'attaquant connaît la clé, il sera plus facile de déchiffrer et d'accéder à l'information originale[**5**].

1.7.3 Stéganographie à clé publique

La stéganographie à clé publique est une méthode de stéganographie qui utilise un système de chiffrement asymétrique, tel que RSA, pour ajouter une couche de sécurité aux données cachées dans un message de couverture. Contrairement à la stéganographie à clé secrète qui utilise une clé partagée entre l'émetteur et le récepteur, la stéganographie à clé publique utilise une paire de clés mathématiquement liées : une clé publique pour chiffrer les données cachées et une clé privée pour les déchiffrer [**5**]. Ce processus est illustré dans la Figure 1.8

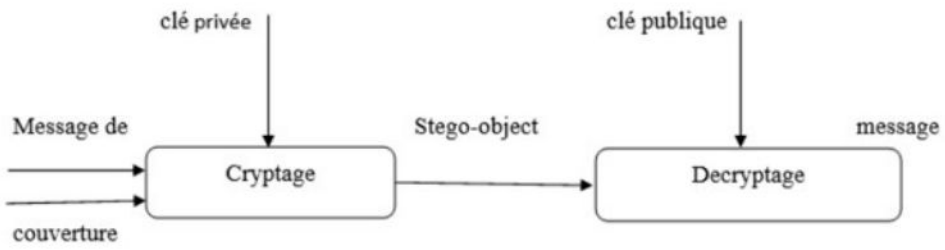

FIGURE 1.8 – Stéganographie à clé publique
[5].

— **Chiffrement de message :** Le message est chiffré avec la clé publique du récepteur l'aide d'un algorithme de chiffrement asymétrique, tel que RSA.

— **Encodage du message chiffré :** Le message chiffré est encodé pour être inséré dans le message de couverture, tel qu'un fichier image, audio ou vidéo. L'encodage permet de cacher le message de manière imperceptible pour l'œil humain ou l'oreille.

— **Intégration :** Le message caché encodé est inséré dans le message de couverture, généralement en modifiant certains bits ou pixels du fichier de couverture.

— **Envoi du message :** Le message de couverture avec le message caché est envoyé

— **Extraction le message caché :** Le récepteur reçoit le message, extrait les données cachées et déchiffre les données à l'aide de sa clé privée.

La stéganographie à clé publique est plus sécurisée que la stéganographie à clé secrète, car elle utilise un système de chiffrement asymétrique pour protéger les données cachées. Cependant, elle est également plus lente que la stéganographie à clé secrète car elle nécessite une opération de chiffrement asymétrique pour chaque message caché [5].

1.8 Domaines d'application de la stéganographie

— **Communications sécurisées :** Les utilisateurs peuvent dissimuler des messages secrets dans des images, des fichiers audio ou vidéo pour transmettre des informations confidentielles de manière sécurisée.
— **Sécurité de l'information :** La stéganographie est utilisée pour cacher des informations sensibles, telles que des codes d'accès, des numéros de carte de crédit ou d'autres informations personnelles importantes, afin d'éviter qu'elles ne soient détectées ou compromises.
— **Protection des droits d'auteur :** La stéganographie peut être utilisée pour ajouter des informations sur les droits d'auteur à des images, des vidéos, etc. pour protéger les créateurs de contenu et leurs œuvres.
— **Échange de données confidentielles :** Les entreprises, les organisations gouvernementales,

etc. peuvent utiliser la stéganographie pour dissimuler des informations sensibles dans des images, des fichiers audio ou vidéo pour les transmettre de manière sécurisée entre les parties autorisées.

— **Médias sociaux :** La stéganographie peut être utilisée pour communiquer de manière secrète ou pour contourner la censure sur les réseaux sociaux.

— **Médecine :** La stéganographie peut être utilisée pour dissimuler des informations médicales confidentielles dans des images, afin de protéger la vie privée des patients.

— **Watermarking :** la stéganographie peut être utilisée pour ajouter des marques numériques ou des codes d'identification uniques aux fichiers numériques pour identifier leur propriétaire et protéger contre le plagiat.

— **Sécurité des données :** La stéganographie peut être utilisée pour masquer des informations sensibles dans des fichiers de données apparemment ordinaires, tels que des images ou des documents, pour éviter leur détection ou leur interception.

1.9 Efficacité de système stéganographie

Dans cette section, nous évaluons l'efficacité d'un système stéganographique .

— **La capacité à dissimuler le message secret :** Un bon système de stéganographie doit être capable de dissimuler le message secret[**10**].

— **La robustesse contre la détection :** Un système de stéganographie efficace doit être capable de résister à une analyse systématique visant à détecter la présence d'un message caché[**10**].

— **La capacité à préserver la qualité du message original :** Le système de stéganographie ne doit pas altérer la qualité du message original de manière significative[**10**].

— **La facilité d'utilisation :** un système de stéganographie efficace doit être facile à utiliser et accessible aux utilisateurs qui n'ont pas de connaissances en cryptographie[**10**].

1.10 Conclusion

Ce chapitre introductif nous a permis d'acquérir une compréhension approfondie des concepts fondamentaux de la stéganographie. Nous avons pu saisir l'objectif principal de cette discipline, qui est de dissimuler des informations confidentielles au sein de supports en apparence innocents.

Chapitre 2

Étude préliminaire

2.1 Introduction

Dans ce chapitre, nous allons décrire en détail les différentes parties de notre projet. Nous expliquerons l'objectif du projet, c'est-à-dire ce que nous souhaitons accomplir à travers celui-ci. Nous allons également établir une démarche à suivre pour identifier et exprimer les besoins spécifiques du projet. En résumé, ce chapitre va présenter une vue d'ensemble du projet, en détaillant ses parties, son objectif et la méthodologie utilisée pour exprimer les besoins.

2.2 Contexte et Objectifs du projet

À l'ère actuelle, où les réseaux sociaux et les communications en ligne sont omniprésents, la protection des informations personnelles et la sécurisation des échanges deviennent des préoccupations majeures. Dans ce contexte, ce projet vise à concevoir un système novateur de messagerie sécurisée en introduisant le concept de la stéganographie. La stéganographie est une technique de sécurité bien établie, offre la possibilité de dissimuler le contenu des messages échangés entre les utilisateurs, en les intégrant d'une manière imperceptible à des fichiers multimédias tels que des images, des vidéos ou des fichiers audios. Grâce à cette approche, seuls les émetteurs et les destinataires autorisés seront en mesure d'accéder au contenu des messages dissimulés, garantissant ainsi une confidentialité accrue des communications. Le système de messagerie proposé offrira aux utilisateurs la liberté de choisir la méthode de dissimulation qui leur convient le mieux, leur permettant d'utiliser des images, des vidéos ou des fichiers audios comme supports pour leurs échanges sécurisés. De plus, les utilisateurs pourront continuer à communiquer de manière conventionnelle en envoyant des messages non dissimulés.

Afin de préserver l'intégrité du système et d'assurer la sécurité des communications, une authentification préalable de l'identité des émetteurs et des destinataires sera mise en place. Les utilisateurs devront s'authentifier en utilisant des identifiants sécurisés, tels que des mots de passe, afin de garantir leur légitimité avant de leur permettre d'échanger des messages sécurisés. Ce projet offre une solution innovante et complète pour préserver la confidentialité des échanges sur les réseaux sociaux, tout en maintenant une facilité d'utilisation et une flexibilité pour les utilisateurs.

2.3 Étude de l'existant

L'étude de l'existant est une étape importante dans le développement de projet, y compris dans les applications de messagerie basées sur la stéganographie. Elle consiste à collecter des informations sur les applications existantes pour comprendre leurs fonctionnalités, leurs forces et leurs faiblesses, et les retours d'expérience des utilisateurs. Cette analyse permet de concevoir une application encore plus fiable et sécurisée, ainsi que de découvrir de nouvelles fonctionnalités innovantes. Nous présentons à présent quelques applications existantes dans la littérature utilisant la stéganographie.

2.3.1 Signal

2.3.1.1 Présentation

Signal est une application de messagerie sécurisée qui assure une communication entièrement chiffrée grâce à l'utilisation du cryptage de bout en bout. L'application utilise son propre protocole, qui a été adopté par d'autres services de messagerie tels que WhatsApp et Skype. En tant qu'application open source, la sécurité de Signal est vérifiée par des experts en cybersécurité. Cette approche transparente permet une évaluation indépendante de la sécurité de l'application et contribue à renforcer la confiance des utilisateurs dans la protection de leurs données [**24**]. La Figure 2.1 représentel'interface graphique de l'application signal.

FIGURE 2.1 – Interface graphique de Signal
[**14**]

2.3.1.2 Fonctionnalités

Signal offre plusieurs fonctionnalités qui garantissent la confidentialité et la sécurité des communications parmis ces dernières nous çitons[**14**] :

— **Chiffrement de bout en bout :**Signal chiffre tous les messages et appels de bout en bout, ce qui signifie que seuls l'expéditeur et le destinataire peuvent les lire. Les messages sont sécurisés contre les écoutes indésirables .

— **Appels vocaux et vidéo sécurisés :** Signal permet des appels vocaux et vidéo de haute qualité, tout en maintenant le chiffrement de bout en bout cela garantit que les conversations restent confidentielles et ne peuvent pas être interceptées.
— **Messages autodestructeurs :** Les utilisateurs de Signal peuvent activer les messages autodestructeurs pour définir une durée de vie limitée aux messages. Une fois que le temps écoulé, les messages sont automatiquement supprimés des appareils des participants.
— **Vérification des identités :** Signal propose une fonctionnalité de vérification des identités visuelles pour assurer l'authenticité des correspondants. Les utilisateurs peuvent comparer les empreintes de sécurité pour ct qu'ils communiquent avec la bonne personne.
— **Protection des métadonnées :** Signal utilise une technique appelée "remplissage" pour masquer les métadonnées lors de l'envoi de messages. Cette technique consiste à ajouter un certain nombre de bits de données aléatoires à la fin du message, qui sont ensuite supprimés par le destinataire lorsqu'il reçoit le message.
— **Transfert de fichiers :** Les utilisateurs peuvent partager en toute sécurité des fichiers, tels que des images, des vidéos, des documents, etc., via Signal.
— **Groupes sécurisés :** Signal prend en charge les conversations de groupe chiffrées de bout en bout. Les membres d'un groupe peuvent communiquer en toute confidentialité et partager des médias en groupe.
— **Code source ouvert :** Signal est une application open source, ce qui signifie que le code source est disponible pour examen par la communauté cela permet de renforcer la confiance et de favoriser l'amélioration continue de la sécurité de l'application.

2.3.1.3 Limites

— **Gestion des contacts :** Signal ne propose pas de fonctionnalités avancées de gestion des contacts, telles que la possibilité de créer des listes de contacts personnalisées ou de synchroniser des contacts à partir d'autres sources.
— **Absence de sauvegarde cloud intégrée :** Signal ne propose pas de sauvegarde cloud intégrée pour les messages cela signifie que si vous changez d'appareil ou réinitialisez votre téléphone, vous pouvez perdre l'historique de vos conversations.

2.3.2 Telegram

2.3.2.1 Présentation

Telegram est une application de messagerie instantanée populaire qui offre diverses fonctionnalités ce dernier se concentre plutôt sur la sécurité et la confidentialité des communications, en utilisant son propre protocole de chiffrement appelé MTProto pour protéger les messages échangés entre les utilisateurs [**12**]. La Figure 2.2 représente les interfaces graphiques de l'application Telegram.

FIGURE 2.2 – Interface graphique de Telegram
[**21**]

2.3.2.2 Fonctionnalités

Telegram offre plusieurs fonctionnalités qui garantissent la confidentialité et la sécurité des communications parmi ces dernières nous çiton [**14**] :

- **Chiffrement de bout en bout :** Telegram utilise le chiffrement de bout en bout pour les appels vocaux, les appels vidéo, les échanges secrets et les discussions de groupe secrètes. Cela signifie que seuls les expéditeurs et les destinataires peuvent accéder au contenu des messages, et même Telegram ne peut pas le lire.
- **Échange secret :** La fonctionnalité "échange secret" de Telegram permet d'envoyer des messages qui sont automatiquement supprimés après un certain laps de temps défini. Cela garantit une plus grande confidentialité en assurant que les messages ne restent pas sur les appareils des utilisateurs ou sur les serveurs de Telegram.
- **Confidentialité des données :** Telegram offre la possibilité de masquer son numéro de téléphone aux autres utilisateurs et de contrôler les informations personnelles visibles sur le profil. Les utilisateurs peuvent également choisir qui peut les ajouter à des groupes et peuvent bloquer ou signaler des utilisateurs indésirables.
- **Messagerie instantanée :** Les utilisateurs peuvent envoyer des messages texte, des photos, des vidéos, des fichiers et des messages vocaux à leurs contacts.
- **Groupes de discussion :** Telegram permet de créer des groupes de discussion pouvant accueillir un grand nombre de membres. Les utilisateurs peuvent échanger des messages, des médias et participer à des discussions de groupe.

2.3.2.3 Limites

- **Pas de sauvegarde dans le cloud :**Les messages et les médias sur Telegram ne sont pas sauvegardés automatiquement dans le cloud, ce qui signifie que si vous changez de périphérique ou si vous désinstallez l'application, vous risquez de perdre vos données.

2.3.3 Dust

2.3.3.1 Présentation

Dust, anciennement connu sous le nom de Cyber Dust, est une application de messagerie privée qui garantit la confidentialité des communications grâce à un chiffrement de bout en bout [**14**]. La Figure 2.3 représente les interfaces graphiques de l'application Dust

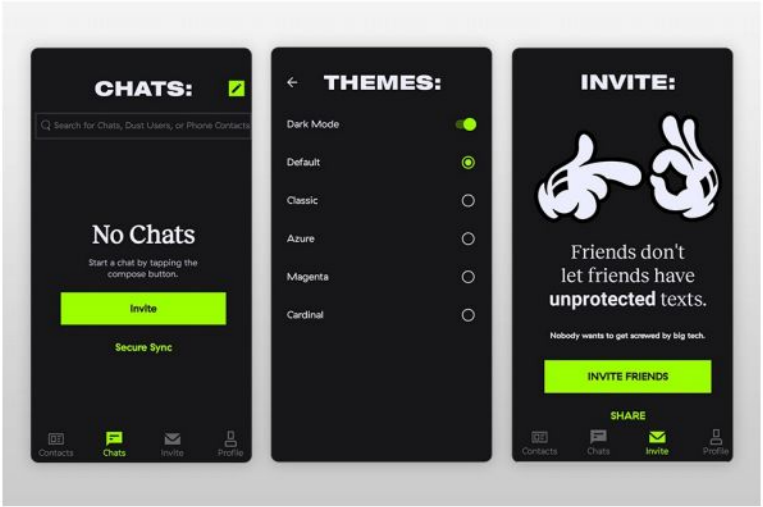

FIGURE 2.3 – Les interfaces graphiques de Dust
[**19**]

2.3.3.2 Fonctionnalités

— **Messages éphémères :** Vous pouvez envoyer des messages privés appelés "Dusts" qui sont configurés pour s'autodétruire après un certain délai, généralement dans les 24 heures ou juste après leur lecture. Cela garantit que les messages ne restent pas indéfiniment sur les appareils des destinataires.

— **Fonctionnalités de surveillance de la vie privée :** Dust propose des fonctionnalités pour surveiller votre vie privée, notamment en vous informant sur les applications qui accèdent à votre carnet d'adresses et en vous permettant de révoquer l'accès si nécessaire.

— **Avertissement de capture d'écran :** Dust vous avertit lorsque quelqu'un fait une capture d'écran de vos messages. Cela permet de détecter les tentatives de capture d'informations sensibles.

2.3.3.3 Limites

— **Imitations des fonctionnalités :**
Par rapport à d'autres applications de messagerie, Dust présente des fonctionnalités plus limitées. Par exemple, il n'offre pas des fonctionnalités avancées telles que les appels vocaux ou vidéo, les fonctionnalités de partage de fichiers, ou une intégration étendue avec d'autres applications et services.

2.3.4 WhatsApp

2.3.4.1 Présentation

WhatsApp est une application de messagerie instantanée qui permet aux utilisateurs de communiquer via des messages textuels, des appels vocaux et vidéo, ainsi que de partager des fichiers et des médias tels que des photos et des vidéos [**14**]. La Figure 2.4 représente les interfaces graphiques de l'application WhatsApp.

FIGURE 2.4 – Les interfaces graphiques de WhatsApp
[**19**]

2.3.4.2 Fonctionnalités

Voici un aperçu des fonctionnalités, de la sécurité et des limites de WhatsApp [**14**].

- **Messages et appels :** WhatsApp permet d'envoyer des messages texte, des photos, des vidéos, des enregistrements audio et des documents. Vous pouvez également passer des appels vocaux et vidéo de haute qualité avec vos contacts WhatsApp.
- **Groupes :** WhatsApp permet de créer des groupes de discussion pour communiquer avec plusieurs contacts simultanément.
- **Statuts :** WhatsApp propose une fonctionnalité de statuts éphémères où vous pouvez partager des photos, des vidéos et des textes qui disparaissent après 24 heures.
- **Partage de localisation :** WhatsApp offre une possibilité de partager la localisation en temps réel avec, ce qui est utile pour les rencontres ou pour indiquer la position.
- **Chiffrement de bout en bout :** WhatsApp utilise un chiffrement de bout en bout pour tous les messages, les appels vocaux, les appels vidéo et les transferts de fichiers. Cela signifie que seuls l'expéditeur et le destinataire peuvent lire le contenu, et personne d'autre, y compris WhatsApp, n'a accès aux données.

2.3.4.3 Limites

— **Stockage dans le cloud :** Lorsque l'on choisit de sauvegarder les conversations WhatsApp sur Google Drive, les données sont stockées de manière chiffrée sur le service cloud de Google. Cependant, il est important de noter que le chiffrement utilisé diffère du chiffrement de bout en bout appliqué aux messages normaux sur WhatsApp. Google Drive a la capacité d'accéder aux données sauvegardées, ce qui signifie que, en cas de violation de la sécurité de Google Drive ou d'une demande légale, les messages sauvegardés pourraient être accessibles.

2.3.5 Analyse Concurrentiel

Notre application "MysterMessage" se distingue des autres applications existantes en offrant une méthode de communication sécurisée utilisant la stéganographie. L'utilisateur peut choisir de dissimuler ses messages dans des fichiers personnels tels que des textes, des images, des vidéos ou des fichiers audio. Contrairement aux autres qui utilise le chiffrement de bout en bout comme une méthode pour garantir la sécurité et la confidentialité. De plus, la fonctionnalité unique d'utilisation de la stéganographie pour une communication sécurisée,"MysterMessage" offre également un processus de vérification de la qualité des fichiers.
Notre application "MysteMessage" garantit que seul le destinataire prévu peut extraire le message en utilisant un code envoyé à son numéro de téléphone personnel. Cela permet à l'utilisateur de sélectionner les fichiers les plus adaptés pour servir de support à ses messages cachés. En vérifiant la qualité et la validité des fichiers, notre application garantit une expérience de communication fluide et fiable.

2.4 Charte graphique

La charte est un guide qui permet d'être à la fois créatifs, surprenants et rassurants, et cohérents dans la durée.

2.4.1 Intitulé de l'application

"MysterMessage" combine les mots "mystère" et "message" pour exprimer le concept fondamental de l'application. La stéganographie est l'art de cacher un message secret au sein d'un support apparentement anodin, comme une image, un fichier audio ou vidéo. Le nom "MysterMessage" reflète donc l'idée de dissimuler des messages mystérieux au sein de communications apparemment ordinaires. L'ajout du mot "mystère" dans le nom met l'accent sur le caractère secret et énigmatique des messages échangés.

Il peut susciter l'intérêt des utilisateurs en les incitant à découvrir cette méthode de communication alternative et intrigante.

En choisissant le nom "MysterMessage" comme le nom de notre application il est possible de créer une association forte avec les concepts de mystère, de confidentialité et de dissimulation, ce qui peut captiver l'attention des utilisateurs intéressés par des méthodes de communication sécurisées et originales.

2.4.2 Logo

La Figure 2.5 illustre le Logo conçu pour notre application "MysterMessage", qui présente sa thématique principale.

FIGURE 2.5 – Logo dédié pour notre application

2.4.2.1 Signification du logo

Le choix d'une bulle de discussion comme logo pour l'application "MysterMessage" peut être expliqué de plusieurs manières :

— **Symbole de la messagerie :** Les bulles de discussion sont couramment utilisées pour représenter les conversations et les échanges de messages. Elles sont instantanément reconnaissables en tant que symboles de la messagerie et peuvent aider à créer une identité visuelle forte pour l'application.

— **Les bulles de discussion :** sont souvent représentées de manière simple et épurée, ce qui permet de créer un logo facilement reconnaissable et mémorable. La clarté visuelle facilite également l'association de l'image avec le domaine de la messagerie.

En choisissant une bulle de discours comme logo pour l'application "MysterMessage", l'objectif est de créer une représentation visuelle qui évoque la communication, la confidentialité et la simplicité, tout en étant facilement identifiable et mémorable pour les utilisateurs.

L'ajout de l'icône de cadenas dans le logo de "MysterMessage" peut être expliqué de la manière suivante :

— **Symbole de sécurité :** Le cadenas est généralement associé à la sécurité et à la protection des informations. Son inclusion dans le logo transmet un message clair selon lequel les messages échangés via l'application sont sécurisés et protégés.

— **Réassurance visuelle :** L'icône du cadenas peut agir comme un élément visuel rassurant pour les utilisateurs, en les incitant à choisir l'application pour leurs communications sécurisées. Cela peut renforcer leur sentiment de contrôle sur la confidentialité de leurs messages.

— **Différenciation :** L'ajout de l'icône de cadenas dans le logo peut aider à distinguer "MysterMessage" des autres applications de messagerie, en soulignant son engagement envers la sécurité des messages. Cela peut attirer l'attention des utilisateurs qui recherchent des solutions de communication sécurisées.

L'icône du cadenas dans le logo sert principalement à communiquer l'idée de sécurité et de confidentialité des messages échangés.

2.4.3 Couleurs

— Bleu marine [#0F4A74] : Une couleur a pour but d'inspirer la confiance et crédibilité. La Figure 2.6 représente la couleur bleu marine.

FIGURE 2.6 – Couleur bleu marine

— Bleu Cobalt [#065E98] : Une couleur a pour but d'attirer l'attention (renforcer l'identité visuelle). La Figure 2.7 représente la couleur bleu cobalt.

FIGURE 2.7 – Couleur bleu Cobalt

— Bleu Lavande [#7C80B7] : Une couleur a pour but de créer une ambiance calme et relaxante cela pour aider à réduire la fatigue visuelle. La Figure 2.8 représente la couleur bleu lavande.

FIGURE 2.8 – Couleur bleu lavande.

— Bleu ciel [#8FBEDC] : Une couleur a pour but de renforcer la connexion de communication fluide et d'interaction sociale. La Figure 2.9 représente la couleur bleu ciel.

FIGURE 2.9 – Couleur bleu ciel.

— Bleu Gris [#DFE6EC] : Une couleur a pour but de mettre en valeur les éléments spécifiques d'une interface il peut être utiliser comme une couleur d'accentuation pour attirer l'attention sur les boutons et les icônes importantes créant un contraste visuel et efficace. La Figure 2.10 représente la couleur bleu Gris.

FIGURE 2.10 – Couleur bleu gris.

2.5 Méthode de développement

Nous avons adopté une méthode agile pour le développement de notre projet. Cette approche de gestion de projets implique la division du projet en plusieurs itérations autonomes qui, ensemble, constituent le projet final. Les méthodes agiles accordent une importance primordiale aux besoins du client et favorisent la communication entre toutes les parties prenantes du projet. Plusieurs méthodes agiles existent, notamment XP, SCRUM, CRYSTAL et RAD, dont nous avons opté pour la méthode XP [**23**]

2.5.1 Extrême programming

Extrême Programming est une méthode de développement agile, orientée projet informatique dont les ressources sont régulièrement actualisées. Destinée à accélérer la réalisation des projets du type flexible, c'est-à-dire se concentrer sur les besoins du client, mettre en place un développement itératif et l'intégration continue [**23**].

2.5.2 Cycle de vie de la méthode XP

La méthode XP est organisée en fonction du temps et divisé en six phases successives. La Figure 2.11 représente le cycle de vie de la méthode XP.

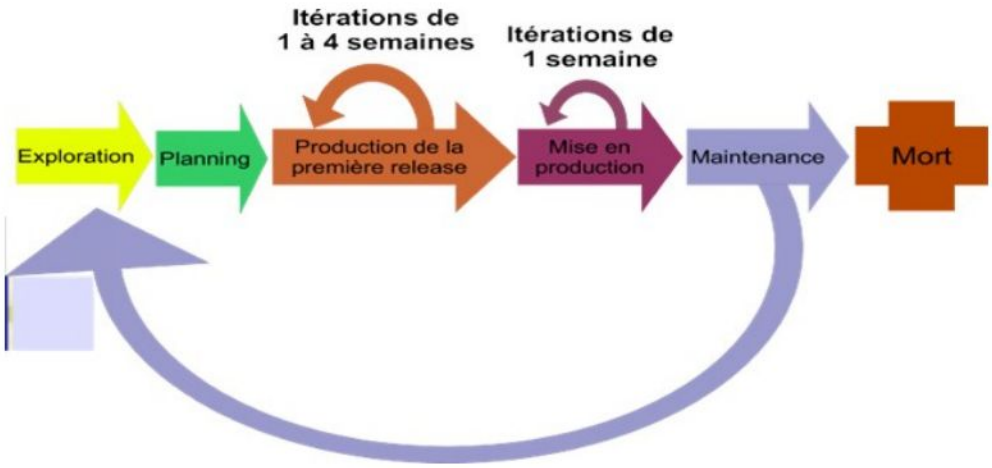

FIGURE 2.11 – Cycle de vie de XP
[**23**]

— **Exploitation :** Dans cette phase les développeurs essayent de se familiariser avec le projet en rencontrant le client qui va exprimer ses besoins sous forme d'user stories que les développeurs doivent estimer en termes de temps de développement [**23**].

— **Planning :** Les développeurs sont chargés d'établir le planning de la première release, qui consistera à choisir les fonctionnalités essentielles pour cette version. Ils prévoient d'enrichir la release ultérieurement en y ajoutant des fonctionnalités supplémentaires. Le planning lui-même devrait être établi en seulement 1 à 2 jours. La première version de cette release devrait être prête dans un délai de 2 à 6 mois [**23**].

— **Production de la première release :** Cette phase consiste à produire la première version d'une application en plusieurs itérations d'une durée d'une à quatre semaines. Chaque itération vise à développer un sous- ensemble de fonctionnalités principales qui sera soumis à des tests fonctionnels avant d'être intégré dans la version finale de l'application. L'utilisation d'itérations courtes permet de détecter rapidement les écarts par rapport au planning, tandis que les réunions quotidiennes impliquant toute l'équipe permettent de suivre l'avancement du projet [**23**].

— **Mise en production :**Cette étape est mise à disposition des utilisateurs finaux. Cette version doit offrir toutes les fonctionnalités essentielles et être parfaitement fonctionnelle. Pour y parvenir, Les itérations sont très courtes et les tests sont effectués en parallèle du développement afin de garantir la qualité du logiciel. Ensuite, les développeurs peuvent procéder à des réglages affinés pour améliorer les performances et optimiser le logiciel en fonction des retours des utilisateurs. Cette étape est cruciale pour assurer la satisfaction des clients et la réussite du projet [**23**].

— **Maintenance :** La maintenance a pour objectif d'assurer le bon fonctionnement continu d'un système ou d'un logiciel, tout en prenant en compte les besoins en évolution des utilisateurs. Cette étape peut également inclure l'ajout de nouvelles fonctionnalités, pour lesquelles une évaluation minutieuse est généralement réalisée pour déterminer leur faisabilité et leur

valeur ajoutée. Si ces fonctionnalités sont considérées comme bénéfiques, elles peuvent être implémentées dans de nouvelles versions du logiciel pour maintenir sa compétitivité sur le marché. En somme, la maintenance est une étape essentielle pour garantir la qualité et la fiabilité d'un système sur le long terme [**23**].

— **Mort :** Lorsque le client ne peut plus spécifier de nouveaux besoins pour un projet, cela peut indiquer que tous les besoins possibles ont été satisfaits ou que le système ne peut pas supporter de nouvelles modifications sans coûter trop cher ou affecter la rentabilité du projet. Dans les deux cas, le projet est considéré comme étant "mort". Cela peut également signifier que le projet a atteint son objectif et peut être considéré comme terminé [**23**].

2.5.3 Pourquoi choisir la méthode XP

Notre choix s'est porté sur la méthode XP pour les principales raisons :
— La capacité d'apporter constamment des améliorations.
— Un logiciel stable grâce à un développement itératif contenu.
— Préconise surtout le travail en binôme des développeurs.
— Facilite la production d'un code simple lisible et maintenable.
— Programmation bout par bout permet de gagner du temps sur la résolution des bugs

2.6 Langage de modélisation

Un langage de modélisation est un langage informatique spécialement conçu pour représenter des modèles, c'est-à-dire des abstractions de systèmes réels ou virtuels. Il existe de nombreux types de langages de modélisation, chacun avec ses propres caractéristiques et fonctionnalités nous avons opté pour le langage **UML** qu'est un langage visuel normalisé utilisé pour modéliser et concevoir des systèmes logiciels. Il fournit une notation graphique pour représenter les composants logiciels et leurs relations ce qui facilite la compréhension et la communication des idées entre les membres de l'équipe de développement [**2**].

2.7 Conclusion

Dans ce chapitre, nous avons commencé à présenter notre projet, en expliquant la méthode de développement XP (extrême programming), qui est une méthode agile pour la gestion de projets logiciels. Nous avons également introduit le langage de modélisation UML (Unified Modeling Language), qui est utilisé pour représenter graphiquement les différents aspects d'un système logiciel, tels que ses fonctionnalités, ses composants, ses interactions, etc.
Nous avons expliqué comment UML nous a permis de traduire nos besoins fonctionnels en une série de cas d'utilisation, qui seront détaillés dans le prochain chapitre. En somme, ce chapitre a jeté les bases de notre approche de développement logiciel et a posé les fondements de notre compréhension du système que nous allons construire.

Chapitre 3

Analyse et conception

3.1 Introduction

Dans ce chapitre, nous allons aborder deux phases cruciales du processus de développement de notre projet : l'analyse des exigences et la conception, L'analyse des exigences consiste à comprendre les besoins et les attentes des utilisateurs finaux du système en identifiant les différents acteurs impliqués dans le processus et les interactions entre eux. Nous allons aussi établir les cas d'utilisation pour décrire les fonctionnalités principales de notre système, La phase de conception consiste à traduire les exigences fonctionnelles et non-fonctionnelles du système en une architecture technique et une conception détaillée.

En somme, ces deux phases sont cruciales pour le développement d'un système efficace et fiable. L'analyse des exigences et la conception permettent de définir clairement les objectifs du système, de structurer les différentes parties du système et de s'assurer que les différentes fonctionnalités sont cohérentes et interagissent correctement entre elles.

3.2 Analyse des besoins

Dans cette section nous allons présenter les besoins fonctionnels et non-fonctionnels.

3.2.1 Besoins fonctionnels

— Créer un système d'authentification.
— Gérer les profils.
— Envoyer et recevoir des messages dissimulés via plusieurs médias.
— Envoyer et recevoir des messages non dissimulés.
— Gérer les contacts.
— Notifier les utilisateurs lorsqu'ils reçoivent de nouveaux messages.
— Gérer les conversations.
— Gérer les invitations.

3.2.2 Besoins non-fonctionnels

Les besoins non fonctionnels pour une application de messagerie basée sur la stéganographie peuvent inclure les éléments suivants :

- **Disponibilité :** L'application doit être disponible en tout temps pour les utilisateurs, sans interruption ou erreur.
- **Scalabilité :** L'application doit pouvoir gérer une augmentation du nombre d'utilisateurs.
- **Utilisabilité :** L'interface utilisateur doit être intuitive et facile à utiliser pour les utilisateurs, sans nécessiter une formation supplémentaire.
- **Performance :** L'application doit fonctionner rapidement et efficacement, sans temps d'attente ou de ralentissement pour les utilisateurs.
- **Conformité :** L'application doit respecter les réglementations en matière de protection des données personnelles et de confidentialité.
- **Maintenabilité :** L'application doit être facile à entretenir et à mettre à jour, avec un coût minimum pour les opérations et le support.
- **Ergonomie :** L'interface utilisateur doit être claire et intuitive, avec une utilisation cohérente

3.3 Identification des acteurs

Un acteur est une entité externe qui interagit avec le système, l'utilisateur peut être un utilisateur humain, une organisation, une machine ou un autre système externe . Un acteur peut avoir le comportement suivant :

- Donner des informations au système[**2**].
- Recevoir des informations du système[**2**].
- Donner et recevoir des informations[**2**].

3.4 Définition de diagramme de cas d'utilisation

Le diagramme de cas d'utilisation est un diagramme UML (Unified Modeling Language) utilisé pour une représentation des besoins des utilisateurs par rapport au système. Cas d'utilisation correspond à un certain nombre d'actions que le système devra exécuter en réponse à un besoin d'utilisateur [**2**].

3.4.1 Identifications des cas d'utilisation

L'acteur effectue un certain nombre de tâches ces derniers sont résumées dans le tableau 3.1 ci-dessus :

Acteur	Tâches
USER	T1 : S'inscrire T2 : Se connecter T3 : Ecrire un message T4 : Dissimuler un message dans une image T5 : Dissimuler un message dans une vidéo T6 : Dissimuler un message dans un audio T7 : Envoyer un message T8 : Recevoir un message T9 : Accéder à la liste des contacts T10 : Supprimer les conversations T11 : Synchroniser les contactes T12 : Accéder à son profil T13 : Modifier son profil T14 : Consulter les notifications T15 : Envoyer une invitation T16 : Accepter une invitation T17 : Refuser une invitation T18 : supprimer une invitation T19 : Se déconnecter T20 : Supprimer son compte

TABLE 3.1 – Tâches de l'utilisateur.

3.4.2 Diagramme de cas d'utilisation

La Figure 3.1 représente le diagramme de cas d'utilisation de notre système.

FIGURE 3.1 – Diagramme de cas d'utilisation

3.5 Description textuelle des cas d'utilisation

Dans cette section nous présentons quelques descriptions textuelles associés aux diagrammes de cas d'utilisation :

3.5.1 Description du cas « S'inscrire »

Le tableau 3.2 représente la description textuelle du cas "S'inscrire" :

Nom du cas d'utilisation	**S'inscrire**
But	Permet de créer un compte utilisateur pour accéder au système
Acteur	User
Préconditions	L'utilisateur doit être connecté à un serveur.
Enchaînement nominal	1. L'utilisateur lance l'application 2. Le système affiche le formulaire à remplir 3. L'utilisateur remplit et valide le formulaire 4. Le système envoie un code OTP pour l'utilisateur 5. L'utilisateur saisie le code 6. Le système ajoute les informations à la base de données 7. L'utilisateur accède à l'application
Enchaînements alternatifs	**A2 : champs non conformes aux types** : L'enchaînement démarre au point 3 de la séquence nominale : **1.** Le système indique que les informations entrées sont incorrectes. La séquence nominale reprend au point 2. **A3 : Le formulaire est vide** L'enchaînement démarre après le point 3 de la séquence nominale : **1-** Le système indique que les champs sont obligatoires. **2-** La séquence nominale reprend au point 2. **A4 : le code OTP est incorrect** L'enchaînement démarre après le point 4 de la séquence nominale : **1-** Le système indique que le code est incorrect, La séquence nominale reprend au point 3
Post-condition	L'utilisateur accède à l'application et sera ajouté à la base de données

TABLE 3.2 – Description textuelle du cas d'utilisation « S'inscrire »

3.5.2 Description du cas « Se connecter »

Le tableau 3.3 représente la description textuelle du cas "Se connecter" :

Nom du cas d'utilisation	Se connecter
But	S'assurer que l'utilisateur est bien celui qui prêtant être.
Acteur	User
Préconditions	L'utilisateur doit être inscrit
Enchaînement nominal	1. Le système affiche le formulaire 2. L'utilisateur remplit le formulaire avec l'ensemble des informations nécessaires 3. Le système vérifie les informations saisies par l'utilisateur, et il envoie un code OTP 4. L'utilisateur saisie le code 5. L'utilisateur accède à l'application
Enchaînements alternatifs	**A1 : Erreur Authentification :** L'information saisie est non valide L'enchaînement démarre au point 4 de la séquence nominale : **1-**Incorrectes en envoyant un message d'erreur. **2**- Le système invite l'utilisateur à ressaisir ses identifiants à nouveau, la séquence nominale reprend au point 2. **A2 : Champs obligatoires vides :** L'enchaînement démarre après le point 2 de la séquence nominale : **1**- Le système indique que les champs sont obligatoires. **2**- Le système invite l'utilisateur à saisir ses identifiants à nouveau, la séquence nominale reprend au point 2.
Post-conditions	L'utilisateur est connecté au système et rédigé vers la section qui lui convient.

TABLE 3.3 – Description textuelle de cas d'utilisation « Se connecter »

3.5.3 Description du cas « Gérer les invitation »

Le tableau 3.4 représente la description textuelle du cas " Gérer les invitations" :

Nom du cas d'utilisation	Gérer les invitations
But	Permettant à un utilisateur de gérer ses propres invitations envoyées et reçues
Acteur	User
Préconditions	L'utilisateur doit être connecté
Enchaînement nominal	**Cas 1- l'utilisateur envoie une invitation** **1.**L'utilisateur lance l'application. **2.**L'utilisateur clique sur la barre de recherche. **3.**L'utilisateur saisit le nom de la personne pour lui envoyer l'invitation. **4.**L'utilisateur sélectionne le profil de cette personne. **5.**L'utilisateur clique sur le bouton envoyer. **Cas 2- l'utilisateur accepte une invitation** **1.**L'utilisateur lance l'application. **2.**L'utilisateur clique sur l'onglet notification. **3.**L'utilisateur choisit l'invitation à accepter ce dernier clique sur le bouton accepter. **Cas 3- l'utilisateur supprime une invitation** **1.**L'utilisateur lance l'application et accède à son compte. **2.**L'utilisateur clique sur l'onglet notification. **3.**L'utilisateur consulte la liste des invitations et il la supprime.
Enchaînements alternatifs	**Cas 1- l'utilisateur envoie une invitation** **A1** : l'utilisateur n 'existe pas. L'enchaînement démarre au point 3 de la séquence nominale. **4-** Le système indique que le nom saisi n'existe pas La séquence nominale reprend au point 2.
Post-conditions	La liste d'amis de l'utilisateur sera mise à jour.

TABLE 3.4 – Description textuelle du cas d'utilisation « Gérer les invitation » .

3.5.4 Description du cas « Gérer son compte »

Les tableau 3.5 et 3.6 représentent la description textuelle de " Gérer son compte", à savoir "Modifier un compte" et "Supprimer son compte.

Le tableau ci-dessus représente la description textuelle de cas d'utilisation "Modifier son compte" :

Nom du cas d'utilisation	Gérer son compte
But	L'utilisateur peut gérer les informations de son compte et les modifier.
Acteur	User.
Préconditions	L'utilisateur doit être connecté.
Enchaînement nominal	**Cas1 : modifier le compte** **1**. L'utilisateur accède au paramètre du compte **2**. L'utilisateur choisit quelles sont les informations à modifier **3**. L'utilisateur saisit ses nouvelles informations. **4**. L'utilisateur valide ses modifications. **5**. Le système met à jour les informations dans la base de données. **6**. Le système actualise le profil de l'utilisateur et l'affiche
Enchaînements alternatifs	**A1 : champs non conformes aux types.** L'enchaînement démarre au point 3 de la séquence nominale : 4- Le système indique que les informations saisies sont invalides en envoyant un message d'erreur. Le système invite l'utilisateur à saisir ses identifiants à nouveau, la séquence nominale reprend au point 3 La séquence nominale reprend au point 3. **A2 : Modification avec des champs vides.** L'enchaînement démarre après le point 3 de la séquence nominale : **4-** Le système indique que les champs sont obligatoires. La séquence nominale reprend au point 3.
Post-condition	L'utilisateur peut modifier ses informations .

TABLE 3.5 – Description textuelle du cas d'utilisation«Modifier le compte».

Le tableau ci-dessus représente la description textuelle de cas d'utilisation "Supprimer le compte" :

Nom du cas d'utilisation	Gérer son compte
But	L'utilisateur peut supprimer son compte
Acteur	User
Préconditions	L'utilisateur doit être connecté
Enchaînement nominal	**Cas 2 : supprimer un compte :** **1**. L'utilisateur accède aux paramètres du compte. **2**.l'utilisateur choisit "supprimer mon compte" **5**.Le système vérifie l'authenticité de l'utilisateur. **6**.Le système met à jour les comptes dans la base de données.
Enchaînements alternatif	**A1 :la suppression ne peut pas être effectuée"problème technique " ou interruptions,** L'enchaînement démarre au point 1 de la séquence nominale.
Post-condition	L'utilisateur peut supprimer son compte

TABLE 3.6 – Description textuelle du cas d'utilisation « Supprimer un compte »

3.5.5 Description du cas « Chatter avec contacts »

Les tableaux ci-dessus représentent la description textuelle des cas relatifs à " Chatter avec contacts", à savoir "Envoyer un message non-dissimulé ","Envoyer un message dissimulé "," Recevoir un message non-dissimulé","Recevoir un message dissimulé" .

Le tableau 3.7 représente la description textuelle de cas d'utilisation "Envoyer un message non-dissimulé " :

Nom du cas d'utilisation	Envoyer un message non-dissimulé
But	Envoyer des messages non-dissimulé
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 1 : Envoyer un message non-dissimulé** **1**.L'utilisateur lance l'application **2**.L'utilisateur consulte la liste de ses contacts **3**.L'utilisateur sélectionne un contact avec lequel il souhaite chatter **4**.L'utilisateur écrit le message dans la zone de saisie, ou choisir l'image à envoyer . **5**. L'utilisateur clique sur le bouton envoyer
Enchaînements alternatif	**A1 : Connexion internet restauré** . **1-** Le message n'a pas été envoyer l'enchainement démarre au point 4 de la séquence nominale : **5-** Le système détecte que le message n'a pas été envoyé la séquence nominale reprend au point 4
Post-condition	L'utilisateur peut envoyer des messages non-dissimulé

TABLE 3.7 – Description textuelle du cas d'utilisation «Envoyer un message non-dissimulé»

Le tableau 3.8 représente la description textuelle de cas d'utilisation " Envoyer un message dissimulé dans une image " :

Nom du cas d'utilisation	Envoyer un message dissimulé dans une image
But	Envoyer des messages dissimulé dans une image
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 2 : Envoyer un message dissimulé dans une image :** **1**. L'utilisateur lance l'application et consulte sa liste d'amis **2**. L'utilisateur sélectionne le contact avec lequel il souhaite chatter et il clique sur l'icone envloppe. **3**.Le système affiche une interface de stéganographie et l'utilisateur choisit la méthode de dissimulation **4**.L'utilisateur choisit de dissimuler le message dans une image et choisit l'image qui servira de support pour dissimuler le message **5**.Le système va convertir le message en binaire **6**.Le système modifie les pixels de l'image pour cacher les bit de données de message binaire **7**.L'utilisateur enregistre l'image modifié **8**.L'utilisateur envoie l'image modifiée à la personne qui devra extraire le message caché.
Enchaînements alternatif	**A1 : la taille de l'image est insuffisante**. L'enchaînement démarre au point 4 de la séquence nominale : **9-**Le système détecte que la taille de l'image est insuffisante la séquence nominale reprend au point 4 **A2 : la qualité de l'image** L'enchaînement démarre au point 6 de la séquence nominale : **7-**Le système indique que l'image n'a pas une bonne qualité La séquence nominale reprend au point 4.
Post-condition	L'utilisateur peut envoyer des messages dissimulé dans une image

TABLE 3.8 – Description textuelle du cas d'utilisation≪Envoyer un message dissimulé dans une image≫

Le tableau 3.9 représente la description textuelle de cas d'utilisation "Envoyer un message dissimulé dans un audio" :

Nom du cas d'utilisation	Envoyer un message dissimulé dans un audio
But	L'utilisateur peut envoyer des messages dissimulé dans un audio
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 3 : Envoyer un message dissimulé dans un audio :** **1**. L'utilisateur lance l'application et consulte sa liste d'amis. **2**. L'utilisateur sélectionne le contact avec lequel il souhaite chatter et clique sur le bouton l'icone envloppe . **3**. Le système affiche une interface de stéganographie et l'utilisateur choisit la méthode de dissimulation. **4**. L'utilisateur choisit de dissimuler le message dans un audio. **5**. L'utilisateur sélectionne et choisit un audio qui servira comme support pour dissimuler le message. **6**. Le système convertit le message que l'utilisateur veut envoyer en un format binaire et le système modifie les échantillons audios. **7**. Le système utilise l'audio modifié pour cacher les bites de données du message binaire et demande à l'utilisateur d'enregistrer l'audio modifié. **8**. l'utilisateur transmet l'audio modifié à la personne qui devra extraire le message caché.
Enchaînements alternatif	**A1 : connexion échouée** L'enchaînement démarre au point 8 de la séquence nominale **9-** Le système indique que le message n'a pas été envoyé Séquence nominale reprend au point 8
Post-condition	L'utilisateur peut envoyer un message dissimulé .

TABLE 3.9 – Description textuelle du cas d'utilisation «Envoyer un message dissimulé dans un audio»

Le tableau 3.10 représente la description textuelle de cas d'utilisation "Envoyer un message dissimulé dans une vidéo" :

Nom du cas d'utilisation	Envoyer un message dissimulé dans une vidéo
But	L'utilisateur peut envoyer un message dissimulé dans une vidéo
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 4 : Envoyer un message dissimulé dans une vidéo** **1**. L'utilisateur lance l'application. **2**. L'utilisateur consulte sa liste d'amis et sélectionne le contact avec lequel il souhaite chatter et clique sur le bouton l'icone envloppe. **3**. Le système affiche une interface de stéganographie et l'utilisateur choisit la méthode de dissimulation. **4**. L'utilisateur choisit de dissimuler le message dans une vidéo et choisit une vidéo qui servira de support pour dissimuler le message. **5**. Le système convertit le message en binaire et modifie les frames. de la vidéo pour cacher les bit de données de message binaire. **6**. L'utilisateur enregistre la vidéo modifié. **7**. Envoie la vidéo modifiée à la personne qui devra extraire le message caché
Enchaînements alternatif	**A1 : connexion échouée** L'enchaînement démarre au point 7 de la séquence nominale **9-**Le système indique que le message n'a pas été envoyé Séquence nominale reprend au point 7
Post condition	L'utilisateur peut envoyer des messages dissimulé vidéo

TABLE 3.10 – Description textuelle du cas d'utilisation≪Envoyer un message dissimulé dans une vidéo.≫

Le tableau 3.11 représente la description textuelle de cas d'utilisation "Recevoir un message non-dissimulé" :

Nom du cas d'utilisation	Recevoir un message non dissimulé
But	Recevoir un message non dissimulé
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 5 : Recevoir un message non dissimulé** **1**. L'utilisateur lance l'application **2**. L'utilisateur consulte sa messgerie. **3.**L'utilisateur clique sur un contact et affiche la discussion . **4.**L'utilisateur consulte ses messages
Post condition	L'utilisateur peut envoyer des messages dissimulé vidéo.

TABLE 3.11 – Description textuelle du cas d'utilisation « Recevoir un message non-dissimulé »

Le tableau 3.12 représente la description textuelle de cas d'utilisation"Recevoir un message dissimulé" :

Nom du cas d'utilisation	Recevoir un message dissimulé
But	Recevoir un message dissimulé
Acteur	User
Préconditions	L'utilisateur doit être authentifié.
Enchaînement nominal	**Cas 6 : Recevoir un message dissimulé** **Cas 6.1 : Dans une image** **1**. L'utilisateur lance l'application et consulte ses messages. **2**. Le système détecte l'image dissimulée et envoie un code d'accès à l'utilisateur. **3**. Le système démodule les pixels de l'image modifier et convertit les bits binaire de message lisible **4**. Le récepteur extraire le message dissimulé **Cas 6.2 : Dans un audio** **1**. L'utilisateur lance l'application et consulte ses messages reçus . **2**. L'utilisateur ouvre une conversation en cliquant sur le nom de l'émetteur. **3**. le système détecte l'audio dissimulé et envoie un code d'accès à l'utilisateur . **4** : Le récepteur récupére le message dissimulé. **Cas 6 .3 : dans une vidéo** **1**. L'utilisateur lance l'application. **2**. L'utilisateur consulte ses messages reçus. **3**. le système détecte la vidéo dissimulée et envoie un code d'accès à l'utilisateur. **4**. Le récepteur récupére le message dissimulé .
Post condition	L'utilisateur peut recevoir des message dissimulé.

TABLE 3.12 – Description textulle du cas d'utilisation« Recevoir un message dissimulé »

3.5.6 Description du cas « Se déconnecter »

Le tableau ci-dessus représente la description textuelle de cas d'utilisation Se déconnecter :

Nom du cas d'utilisation	Se déconnecter
But	Permet de terminer la session actuelle de l'utilisateur et de protéger la confidentialité et la sécurité des informations
Acteur	User
Préconditions	L'utilisateur doit être authentifié
Enchaînement nominal	**1**.L'utilisateur clique sur le bouton "Déconnecter" depuis l'interface paramètre. **2**.Le système affiche alertdialogue pour demander la confirmation **3**.L'utilisateur confirme son choix **4**.Le système se déconnecte.
Enchaînement alternatif	**A1 :Problème de connexion** L'encaînement démarre au point 1 de la séquance nominal : 4- Le système indique que l'utilisateur n'a pas une bonne connexion, la séquance nominal reprend au point 1
Post condition	L'utilisateur quitte le système

TABLE 3.13 – Description textuelle du cas d'utilisation «Se déconnecter»

3.6 Définition d'un diagramme de séquence

Un diagramme de séquence est un diagramme UML qui représente en détaille la façon dans les opérations sont exécutées en mettent l'accent sur la chronologie de ses derniers en interaction avec objets [**2**].

3.6.1 Diagramme de séquence « S'inscrire »

La Figure 3.2 représente le diagramme de séquence de cas d'utilisation "S'inscrire" :

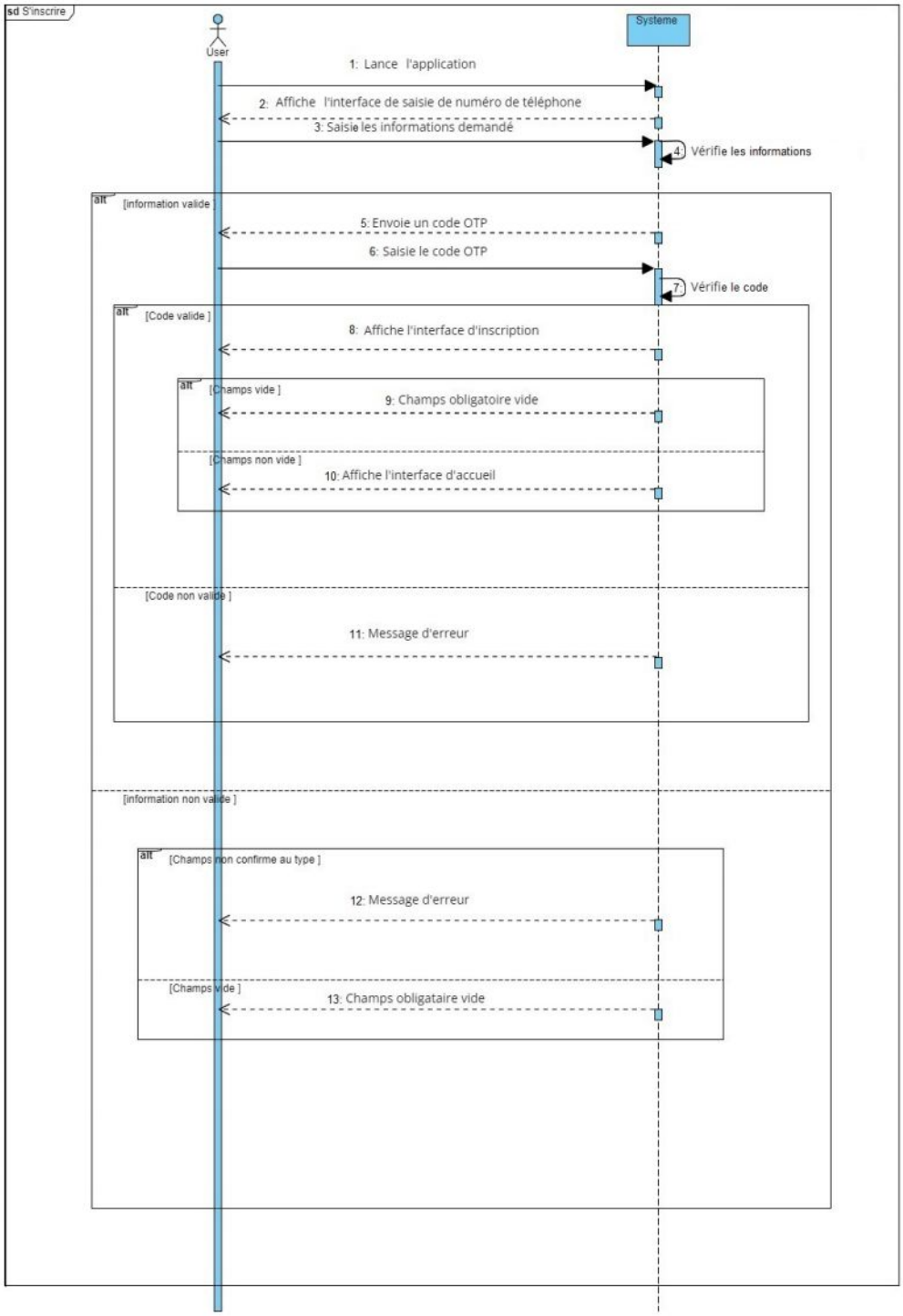

FIGURE 3.2 – Diagramme de séquence de cas d'utilisation « S'inscrire »

3.6.2 Diagramme de séquence « Se connecter »

La figure 3.3 représente le diagramme de séquence de cas d'utilisation" Se connecter" :

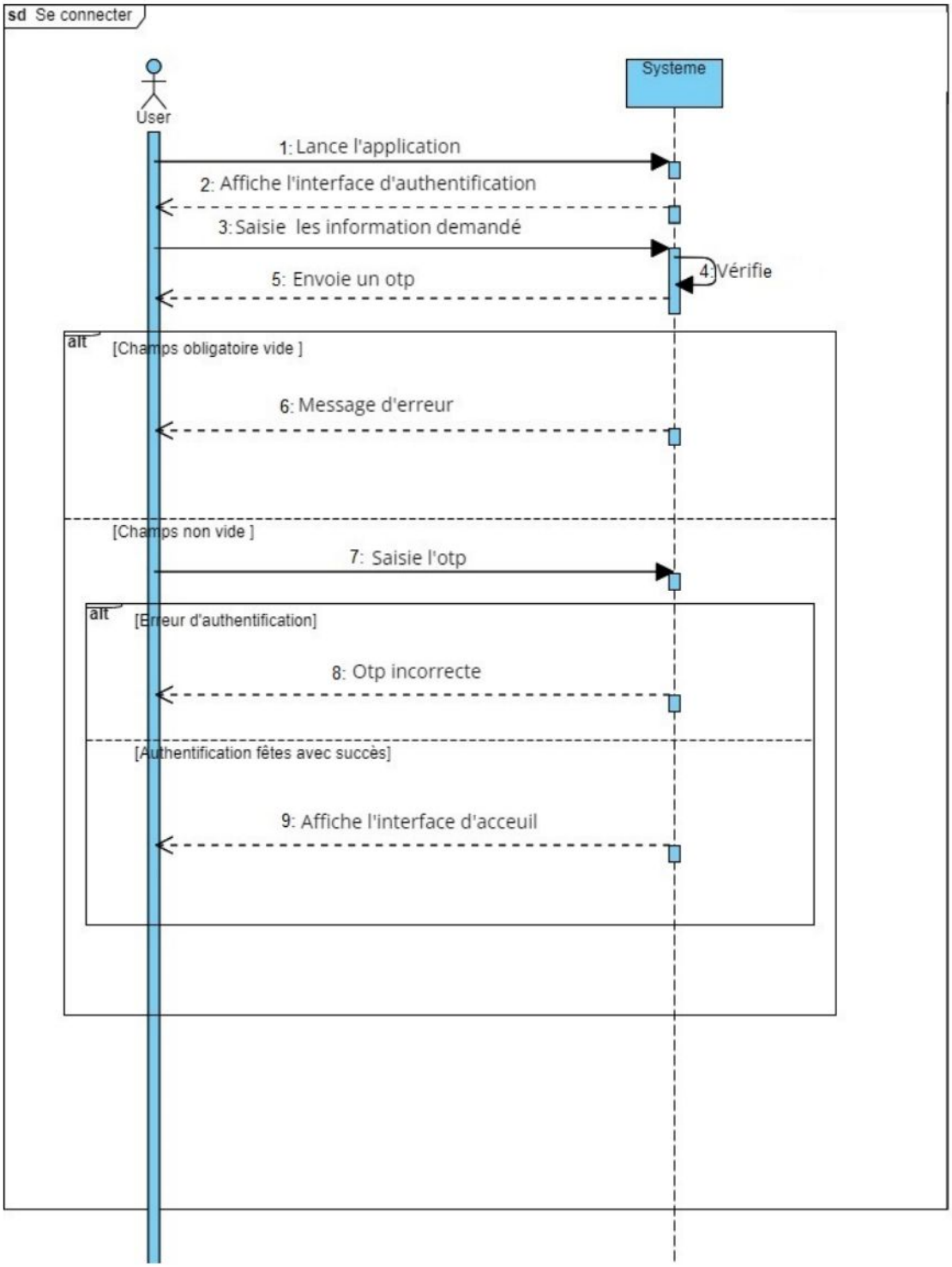

FIGURE 3.3 – Diagramme de séquence de cas d'utilisation « se connecter »

3.6.3 Diagramme de séquence « Gérer les invitations »

La figure 3.4 représente le diagramme de séquence de cas d'utilisation "Gérer les invitations" :

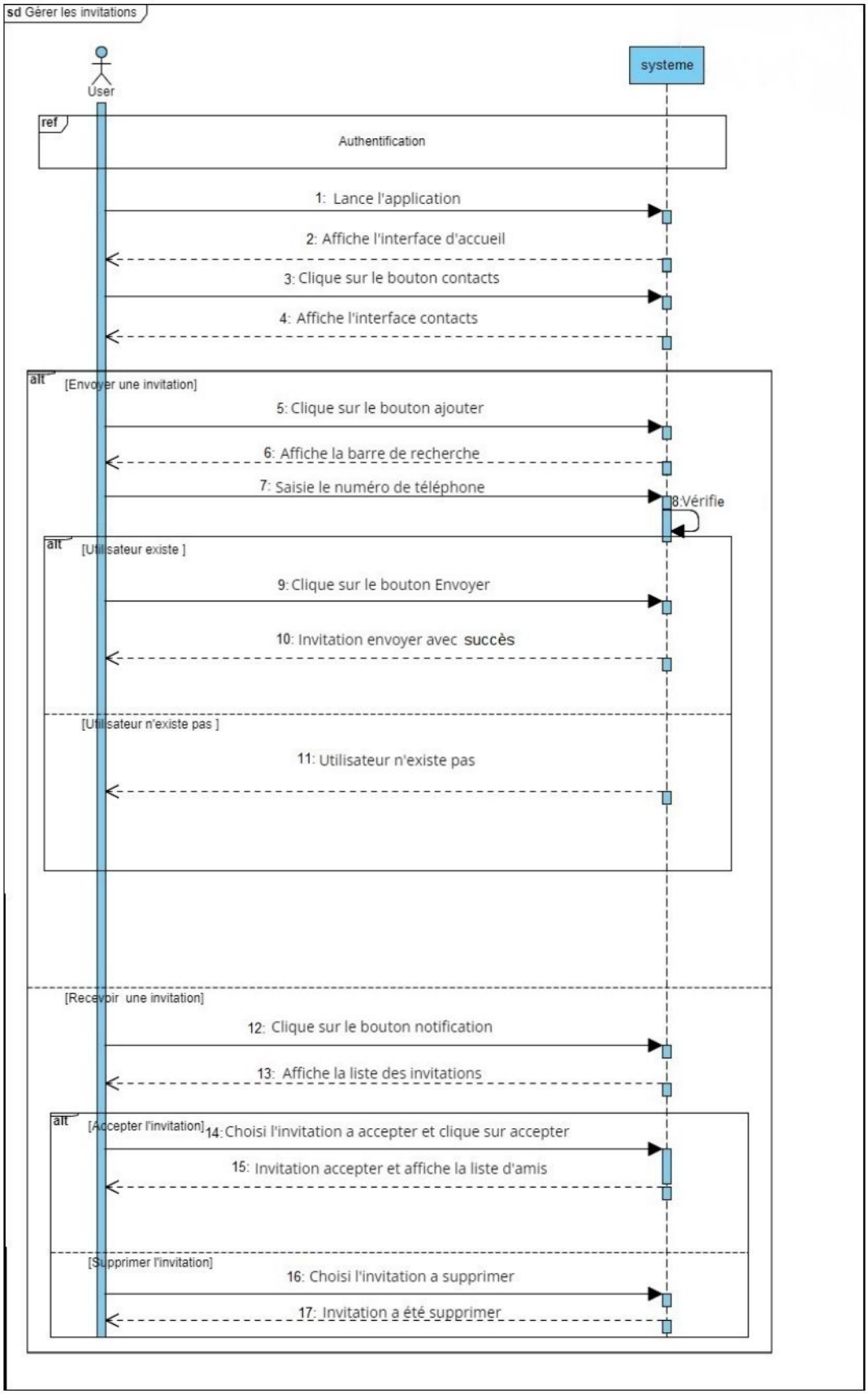

FIGURE 3.4 – Diagramme de séquence de cas d'utilisation « Gérer les invitations »

3.6.4 Diagramme de séquence « Gérer son compte »

Les deux figures qui suivent représentent les deux diagrammes de séquence relatifs à "Gérer son compte " , à savoir « Modifier un compte » et « Supprimer un compte ».

3.6.4.1 Diagramme de séquence « Supprimer son compte »

La figure 3.5 représente le diagramme de séquence de cas d'utilisation "Supprimer son compte" :

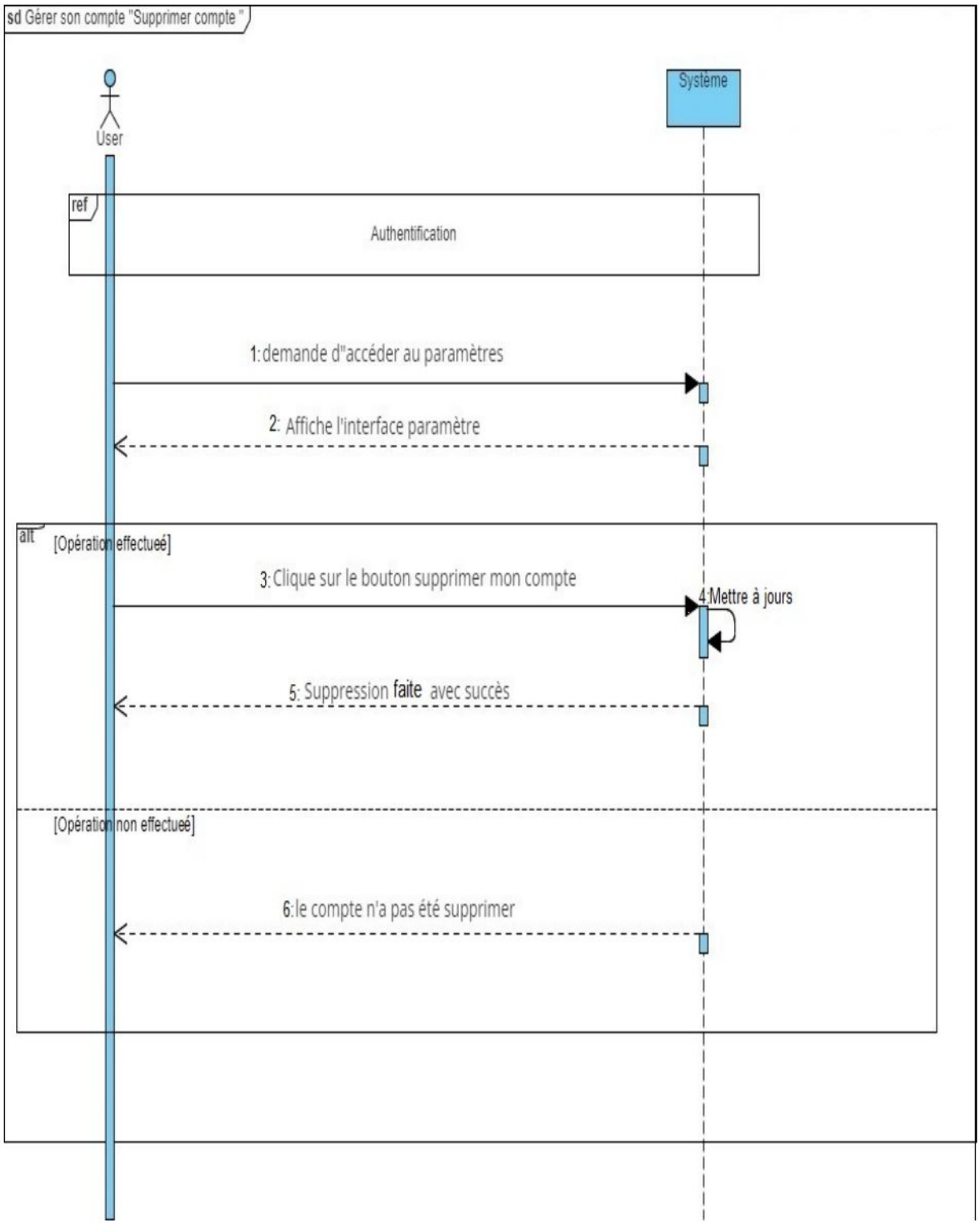

FIGURE 3.5 – Diagramme de séquence de cas d'utilisation « supprimer son compte »

3.6.4.2 Diagramme de séquence « Modifier son compte »

La figure 3.6 représente le diagramme de séquence de cas d'utilisation "Modifier son compte" :

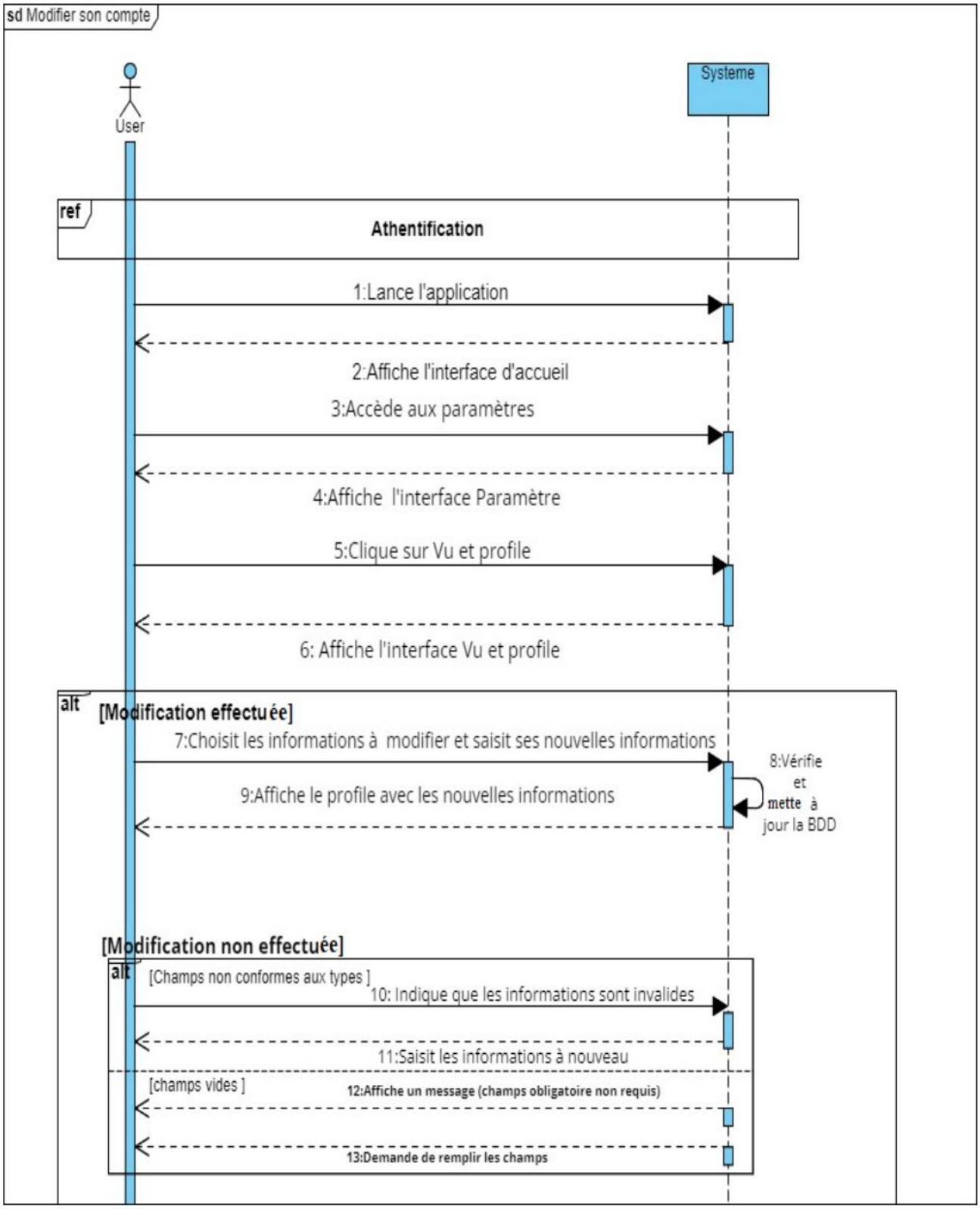

FIGURE 3.6 – Diagramme de séquence de cas d'utilisation « Modifier son compte »

3.6.5 Diagramme de séquence chatter avec contacts

Les figures qui suivent représente les diagrammes de séquence relatifs à « Chatter avec contact »

3.6.5.1 Diagramme de séquence de cas d'utilisation « Envoyer un message non dissimulé»

La figure 3.7 représente le diagramme de séquence de cas d'utilisation "Envoyer un message non dissimulé" :

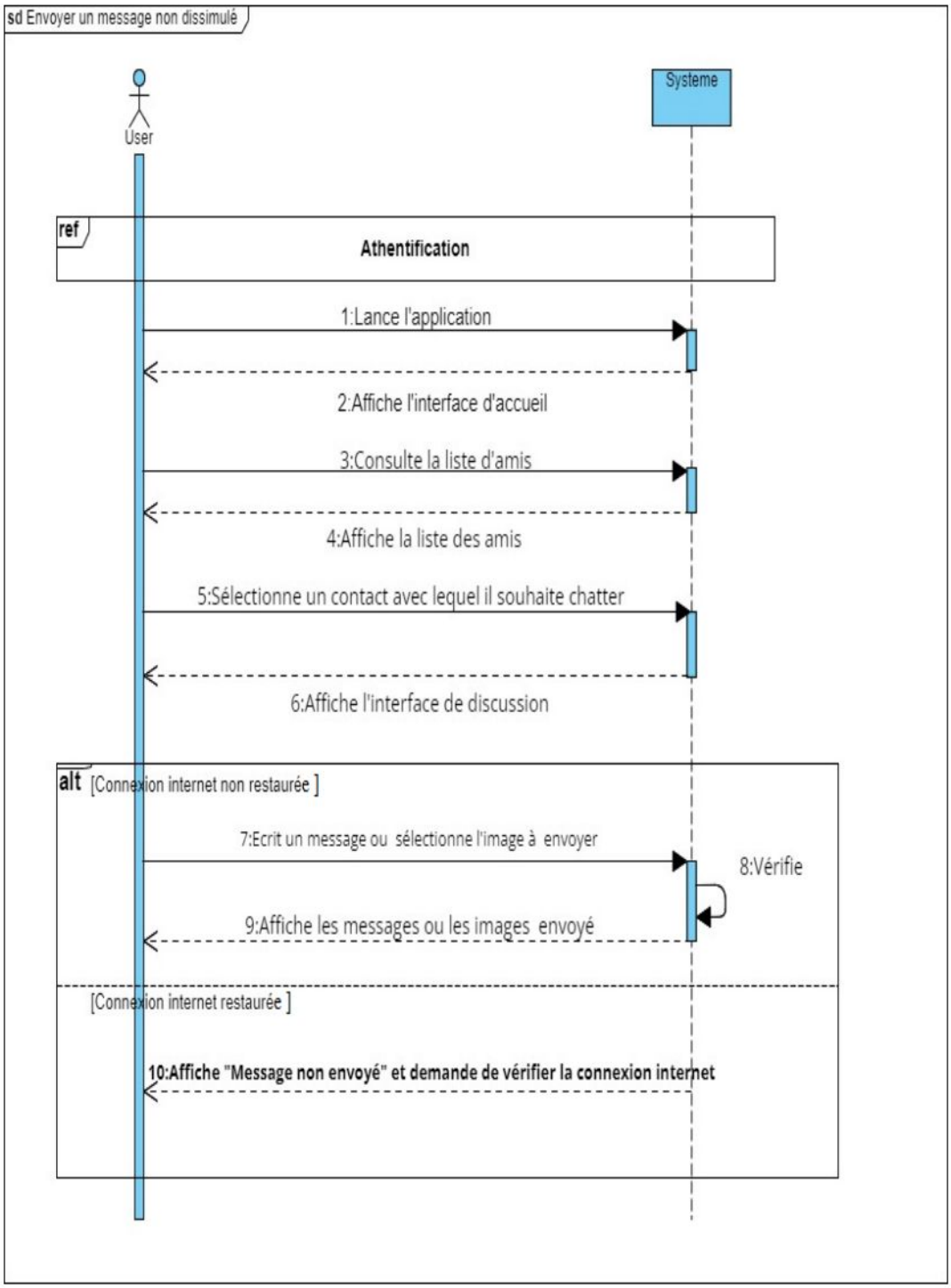

FIGURE 3.7 – Diagramme de séquence de cas d'utilisation « Envoyer un message non dissimulé »

3.6.5.2 Diagramme de séquence de cas d'utilisation « Envoyer un message dissimulé dans une image »

La figure 3.8 représente le diagramme de séquence de cas d'utilisation "Envoyer un message dissimulé dans une image" :

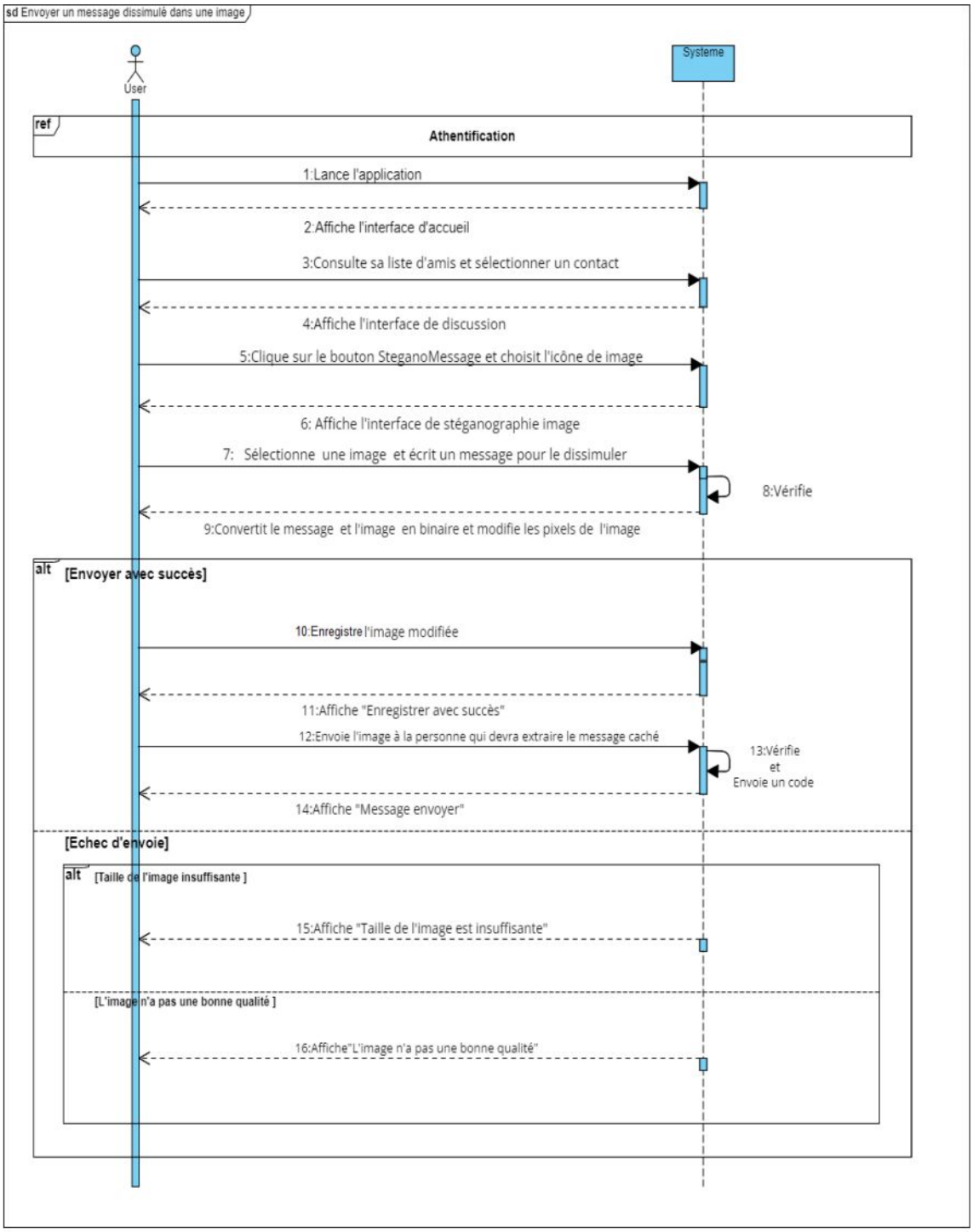

FIGURE 3.8 – Diagramme de séquence de cas d'utilisation « Envoyer un message dissimulé dans une image »

3.6.5.3 Diagramme de séquence de cas d'utilisation «Envoyer un message dissimulé dans un audio»

La figure 3.9 représente le diagramme de séquence de cas d'utilisation "Envoyer un message dissimulé dans un audio" :

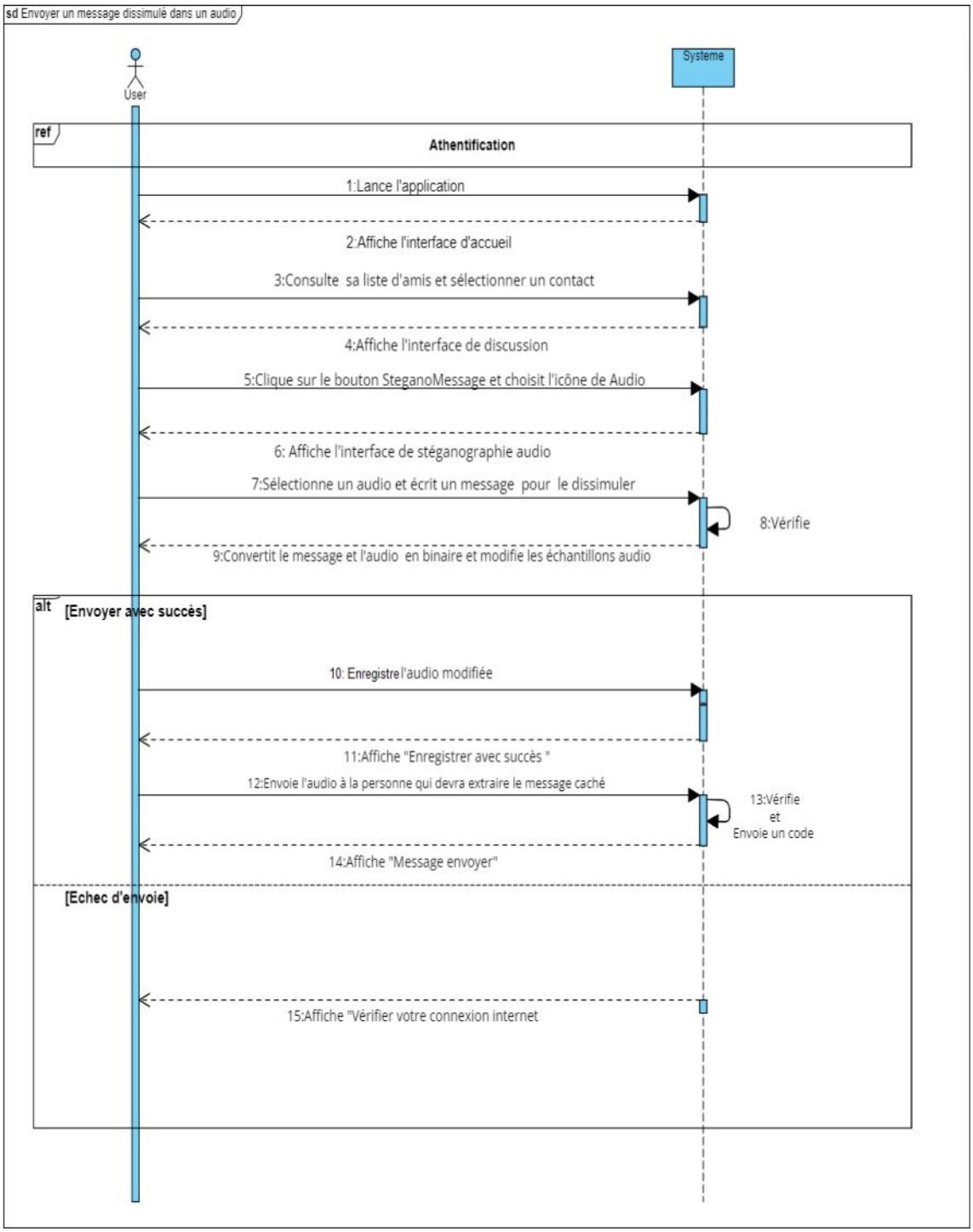

FIGURE 3.9 – Diagramme de séquence de cas d'utilisation « Envoyer un message dissimulé dans un audio »

3.6.5.4 Diagramme de séquence de cas d'utilisation «Envoyer un message dissimulé dans une vidéo»

La figure 3.10 représente le diagramme de séquence de cas d'utilisation "Envoyer un message dissimulé dans une vidéo".

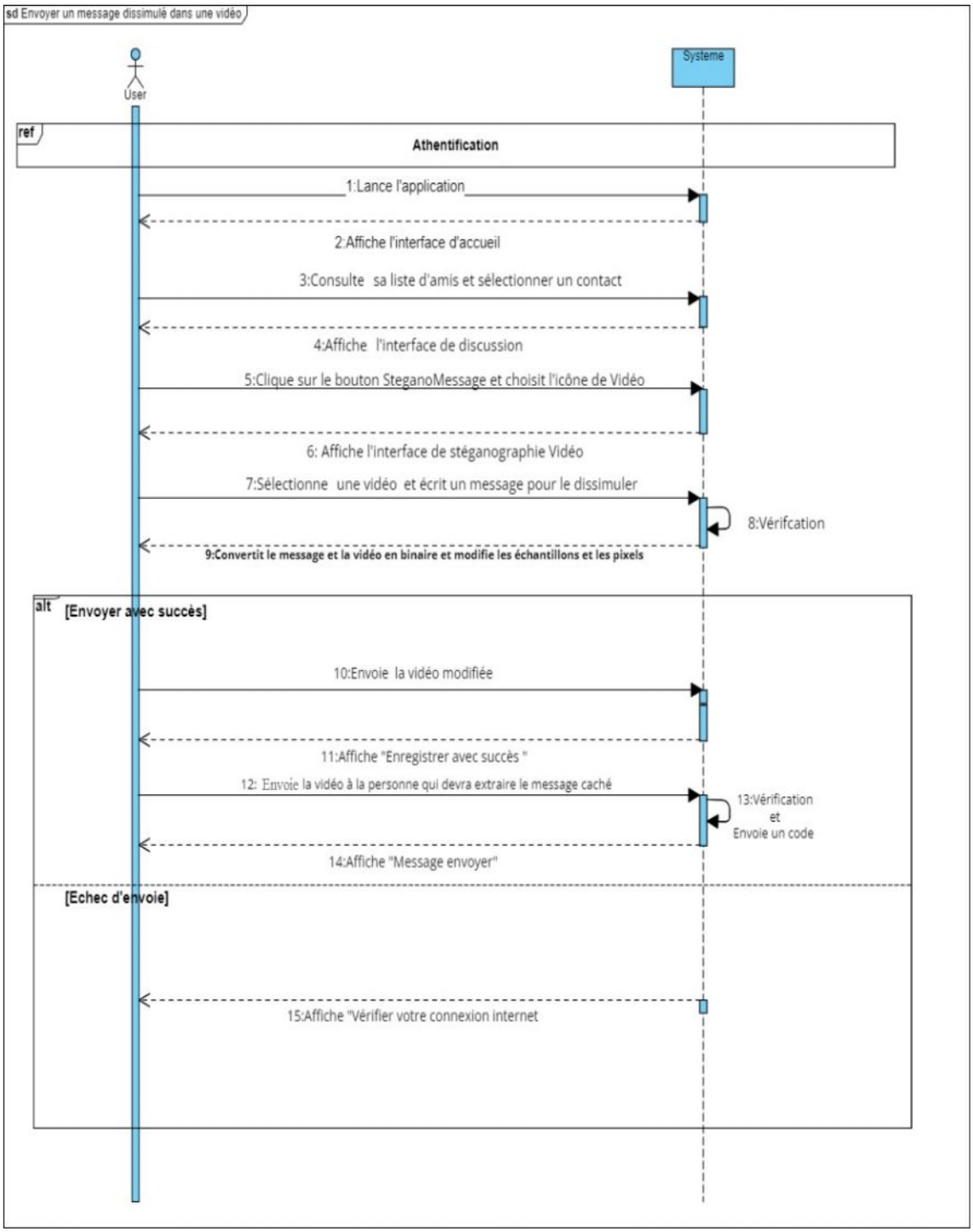

FIGURE 3.10 – Diagramme de séquence de cas d'utilisation « Envoyer un message dissimulé dans une vidéo »

3.6.5.5 Diagramme de séquence de cas d'utilisation «Recevoir un message non dissimulé»

La figure 3.11 représente le diagramme de séquence de cas d'utilisation "Recevoir un message non dissimulé".

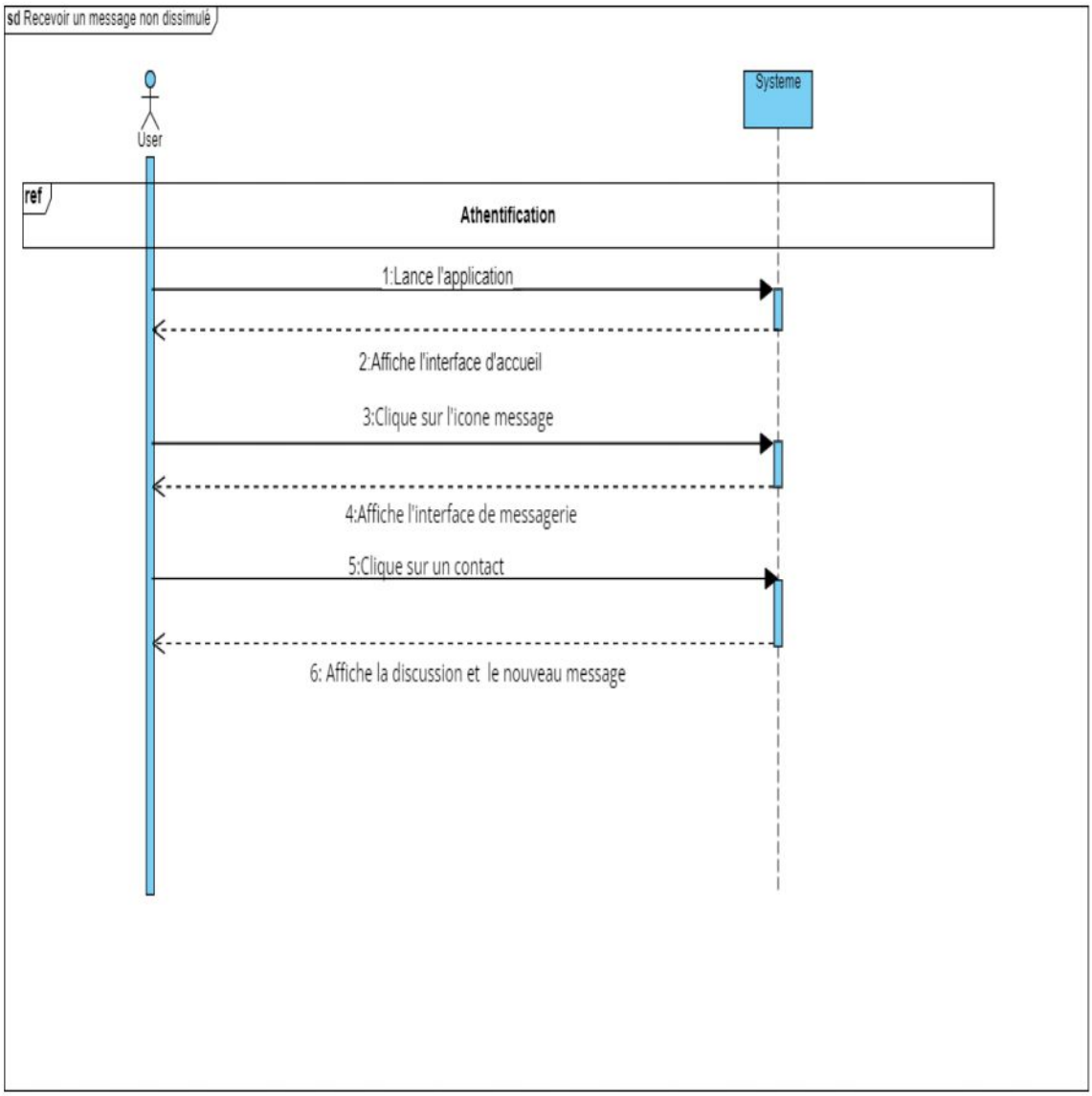

FIGURE 3.11 – Diagramme de séquence de cas d'utilisation « Recevoir un message non dissimulé »

3.6.5.6 Diagramme de séquence de cas d'utilisation «Recevoir un message dissimulé»

La figure 3.11 représente le diagramme de séquence de cas d'utilisation "Recevoir un message dissimulé".

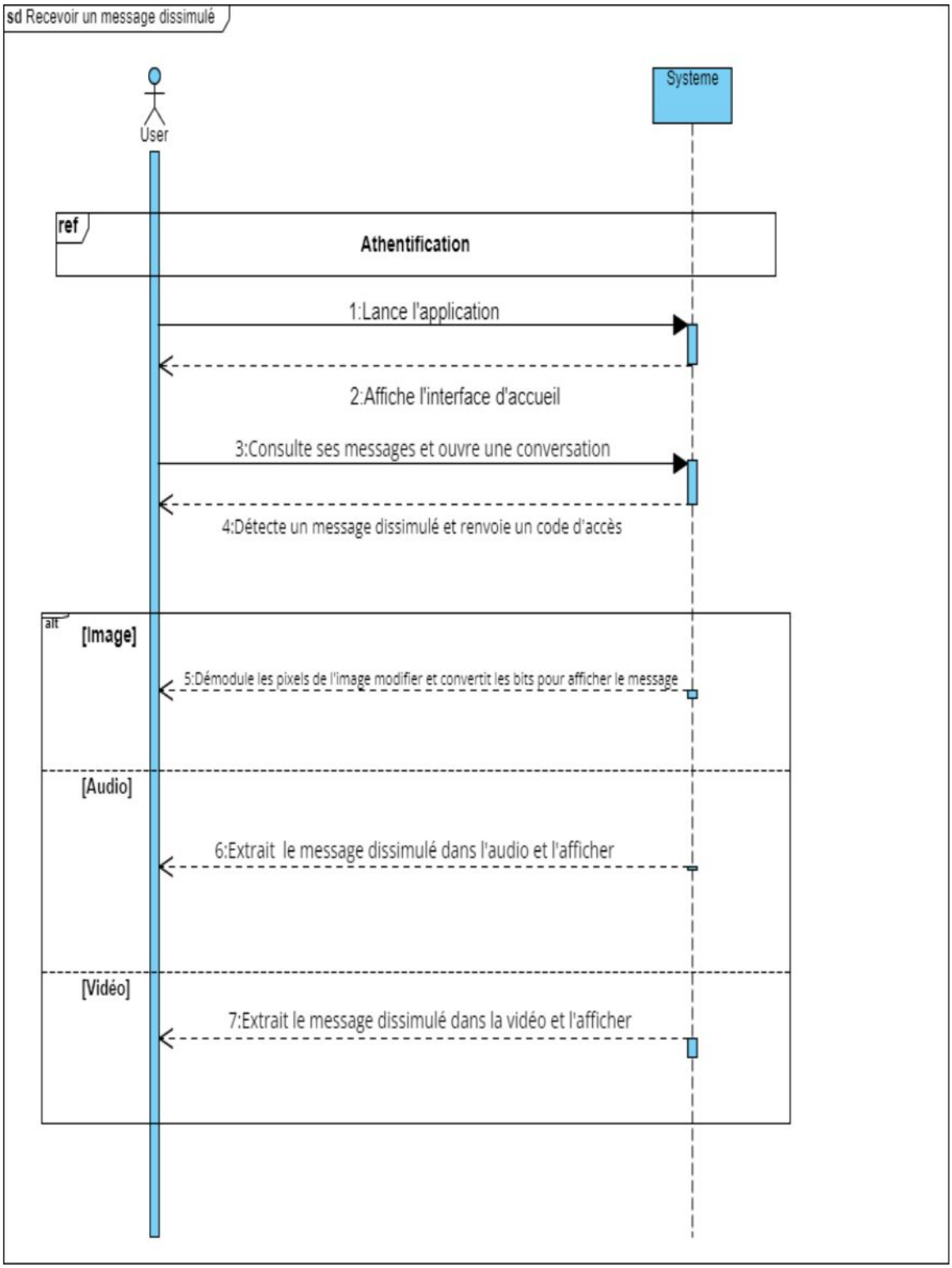

FIGURE 3.12 – Diagramme de séquence de cas d'utilisation « Recevoir un message dissimulé »

3.6.5.7 Diagramme de séquence de cas d'utilisation « Se déconnecter»

La figure 3.14 représente le diagramme de séquence de cas d'utilisation " Se déconnecter".

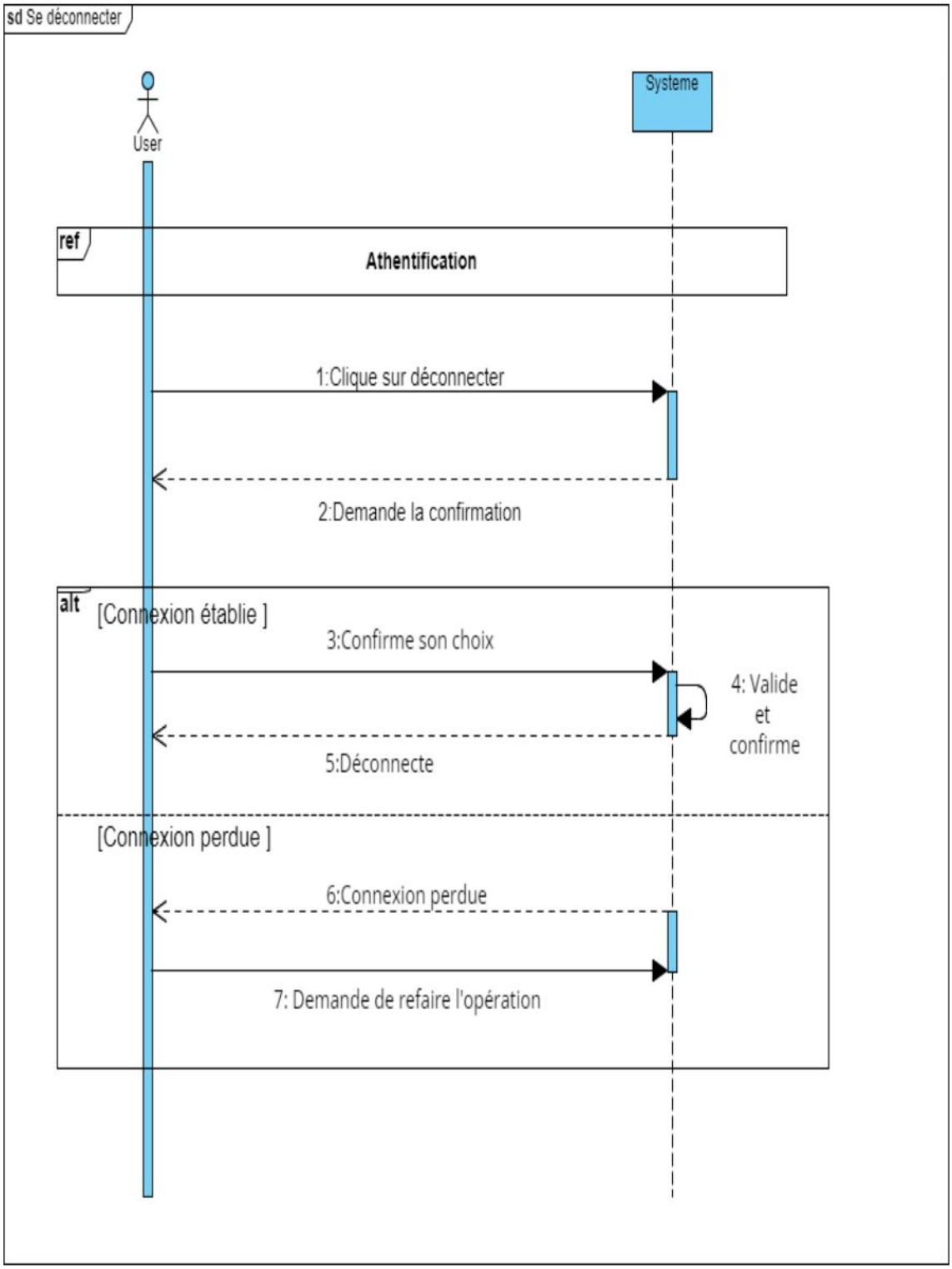

FIGURE 3.13 – diagramme de séquence de cas d'utilisation « Se déconnecter »

3.7 Définition d'un diagramme d'activité

Le diagramme d'activité est un diagramme dynamique de UML décrivant les activités séquentielles et parallèles d'un système. Ils permettent ainsi de représenter graphiquement le comportement d'une méthode ou le déroulement d'un cas d'utilisation [**2**]. La figure 3.14 représente le diagramme d'activité :

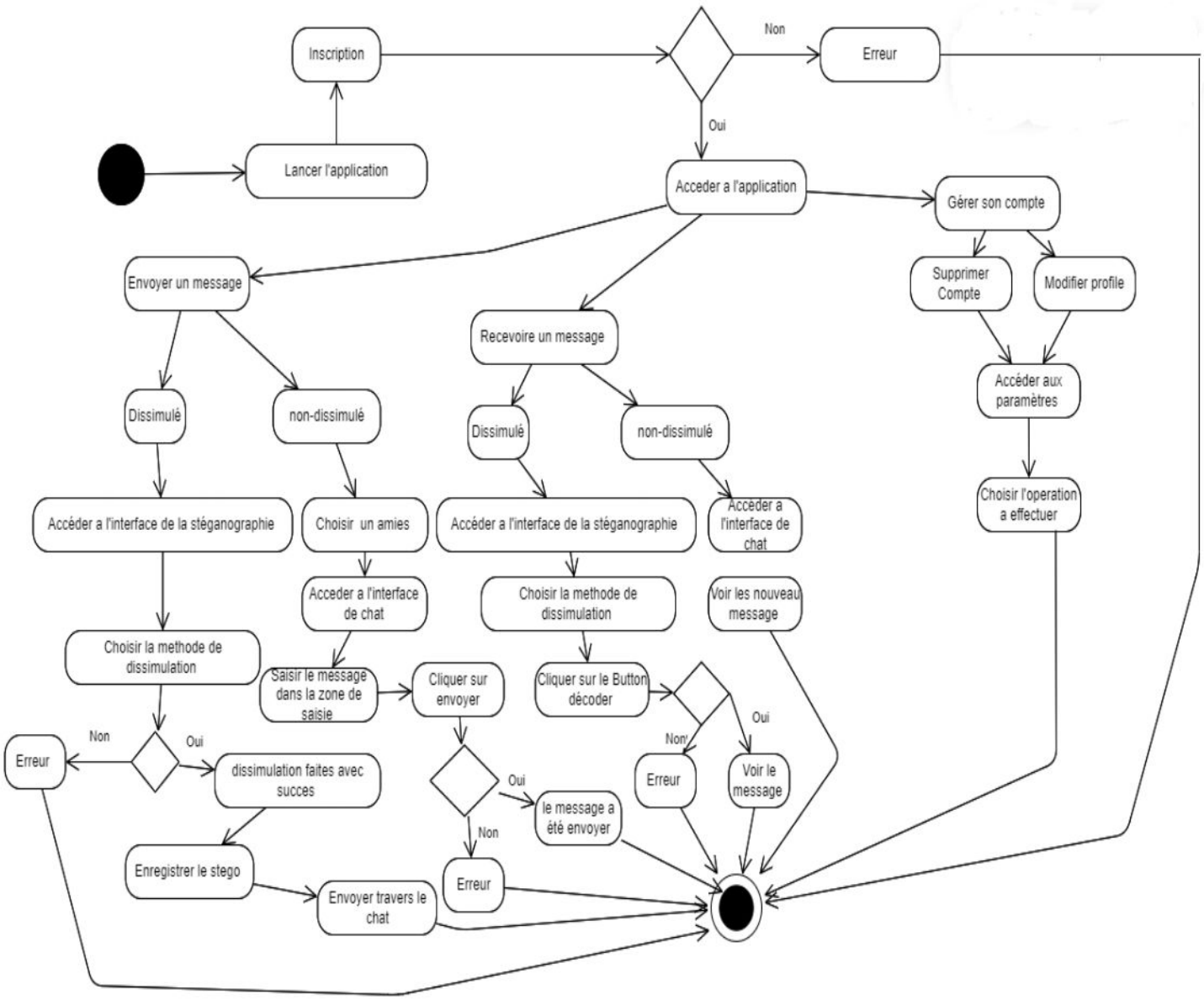

FIGURE 3.14 – Diagramme d'activité

3.8 Définition d'un diagramme de classe

Un diagramme de classe fournit une vue globale d'un système. Il permet de modéliser les classes du système et leurs relations [**2**]. La figure 3.15 représente le diagramme de classe

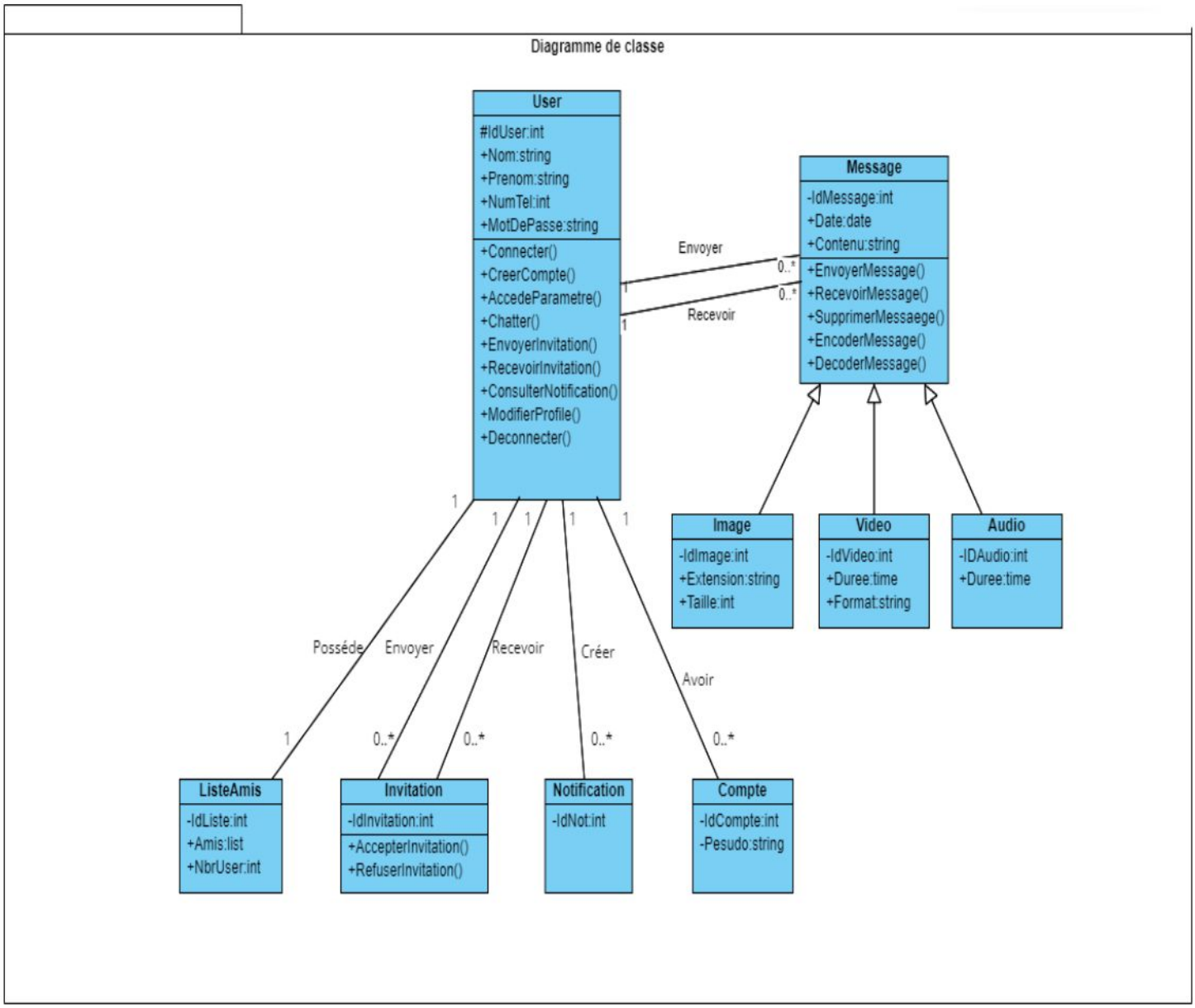

FIGURE 3.15 – Diagramme de classe

3.9 Dictionnaire de données

Dans le tableau ci-dessus sont décrits et expliqués toutes les données qui sont relatives aux classes de notre application.

Classe	Attributs	Description	Types	Taille
User	IdUser	Identifiant de client	int	11
	Nom	Nom de l'utilisateur	string	50
	Prénom	Prénom de l'utilisateur	string	50
	NumTel	Numéro de téléphone de l'utilisateur	string	15
	MotDePasse	Mot de passe de l'utilisateur	string	50
Message	Idmessage	Identifiant du message	int	11
	Date	Date d'envoi et réception du message	date	
	Contenue	Le Contenue de message	string	1000
Image	Idimage	Identifiant de l'image	int	11
	Extension	Extension de l'image	string	10
	Taille	Taille de l'image	int	11
Video	Idvideo	Identifiant de la vidéo	int	11
	Durée	La durée de la vidéo	time	
	Format	Format de la vidéo	string	10
Audio	IdAudio	Identifiant de l'audio	int	11
	Duree	La durée de L'audio	time	
Compte	IdCompte	Identifiant du compte	int	11
	Pesudo	Pesudo du compte	string	50
Invitation	IdInvitation	Identifiants de l'invitation	int	11
ListeAmis	IdList	Identifiant de la liste	list	11
	Amis	Les amis de l'utilisateur	string	50
	NbrUser	Nombre d'utilisateur	list	
Notification	IdNot	Identifiant de notification	int	11

TABLE 3.14 – Dictionnaire de données

3.10 Passage au modelés relationnelle

User : (IdUser, Nom, Prénom, NumTel,MotDePasse)
Message (IdMessage, Date, Contenu, #IdUser)
Image (IdImage, Extension, Taille, #IdMessage, #IdUser)
Vidéo (IdVideo, Durée, Format, #IdMessage, #IdUser)
Audio (IdAudio, Duree, #IdMessage, #IdUser)
Compte (idCompte, Pesudo, #IdUser)
Invitation (IdInvitation, #IdUser)
ListeAmis (IdList, Ami, NbrUser)
Notification (IdNot, #IdUser)

3.11 Conclusion

Dans cette section, nous avons effectué l'analyse et la conception de notre projet en identifiant les besoins du système et en les traduisant en cas d'utilisation. Nous avons utilisé différents types de diagrammes pour représenter les échanges d'informations, les flux d'activité et les relations entre les entités. De plus, nous avons transformé le diagramme de classes en un modèle relationnel, ce qui nous a permis de représenter les entités sous forme de tables et de définir leurs relations. Cette approche facilite la gestion des données et prépare le terrain pour la phase de développement à venir.

Chapitre 4

Implémentation

4.1 Introduction

Après avoir achevé l'étape d'analyse et de conception, nous passerons à la mise en pratique des éléments examinés et conçus dans les chapitres précédents. Dans ce chapitre, nous commencerons par présenter les langages, les outils et les logiciels que nous avons utilisés. Ensuite, nous décrirons l'organigramme de notre application, en expliquant sa structure et ses différentes composantes. Enfin, nous présenterons les interfaces principales de notre application, en mettant l'accent sur leurs fonctionnalités et leur conception visuelle.

4.2 Outils et logiciels utilisés

Dans cette section, nous allons présenter une gamme variée d'outils et de logiciels que nous avons utilisés pour accomplir nos tâches.

4.2.1 Visual Studio Code (VS Code)

Vs code [**26**] est un éditeur de code source léger, open-source et multiplateforme développé par Microsoft. Il est conçu pour être rapide, facile à utiliser et extensible, offrant des fonctionnalités avancées pour les développeurs tels que la coloration syntaxique, la complétion de code, le débogage, l'intégration de Git et d'autres outils de gestion de version, ainsi que des extensions pour prendre en charge différents langages de programmation et Framework. VS Code est disponible sur Windows, MacOs et Linux et est devenu l'un des éditeurs de code les plus populaires et les plus utilisés dans la communauté des développeurs [**26**]. La figure 4.1 représente le logo de Visual studio code :

FIGURE 4.1 – Logo de Vs code
[**25**]

4.2.2 Android studio

Android studio[**16**] est un environnement de développement intégré officiel pour les développeurs d'applications Android, créé par Google à partir de la plateforme IntelliJ IDEA. Il propose une gamme complète d'outils avancés pour aider les développeurs à concevoir, déboguer, compiler, profiler, vérifier les performances et gérer les versions de leurs applications Android. Il comprend également un émulateur Android qui permet de tester les applications sur des périphériques virtuels. Android Studio est gratuit et fonctionne sur Windows, macOS et Linux. C'est l'outil de développement privilégié pour de nombreux développeurs d'applications Android dans le monde [**16**]. La figure 4.2 représente le logo de android studio

FIGURE 4.2 – Logo de Android studio
[**13**]

4.2.3 FireBase

Firebase [**17**] est une plateforme de développement d'applications mobiles et web créée par Google. Elle propose une suite complète d'outils et de services pour faciliter la création d'applications de haute qualité de manière plus rapide et plus facile. Les fonctionnalités offertes par Firebase incluent l'authentification, le stockage cloud, les bases de données en temps réel, les notifications push, l'analyse de l'utilisateur, la messagerie, l'hébergement et bien d'autres encore. Cette plateforme est largement utilisée par des millions de développeurs à travers le monde, et elle est particulièrement prisée par les startups et les petites entreprises en raison de sa facilité d'utilisation et de sa flexibilité. Grâce à Firebase, les développeurs peuvent se concentrer sur la création d'une expérience utilisateur exceptionnelle sans avoir à se soucier de l'infrastructure[**17**]. La figure 4.3 représente le logo de Firebase

FIGURE 4.3 – Logo de Firebase
[17]

4.3 Technologies utilisées

Dans cette section nous allons présenter les langages de programmation utilisés.

4.3.1 Dart

Dart [15] est un langage de programmation développé par Google qui se concentre sur le développement d'applications multiplateformes. Il est utilisé pour créer des applications mobiles, de bureau, de serveur et web. Dart est un langage orienté objet avec une syntaxe similaire à celle du langage C++. Il dispose d'un ramasse-miettes intégré, ce qui signifie qu'il gère automatiquement la gestion de la mémoire. Il offre également des fonctionnalités avancées telles que les interfaces, les mixins, les classes abstraites, les génériques réifiés et l'inférence de types[15]. La figure 4.4 représente le logo de Dart.

FIGURE 4.4 – Logo de Dart
[15]

4.4 Les Framework

4.4.1 Flutter

Flutter [18] est un kit de développement logiciel (SDK) d'interface utilisateur open-source créé par Google. Il est utilisé pour développer des applications pour Android, iOS, Linux, Mac, Windows, Google Fuchsia et le web à partir d'une seule base de code[18] La figure 4.5 représente le logo de flutter

FIGURE 4.5 – Logo de flutter
[18]

4.5 Les interfaces graphiques

Dans cette partie, nous présenterons quelques interfaces graphiques de notre application "MysterMessage".

4.5.1 SplashScreen

Lorsque l'utilisateur lance notre application "MysterMessage", la SplashScreen est la première interface qui s'affiche.

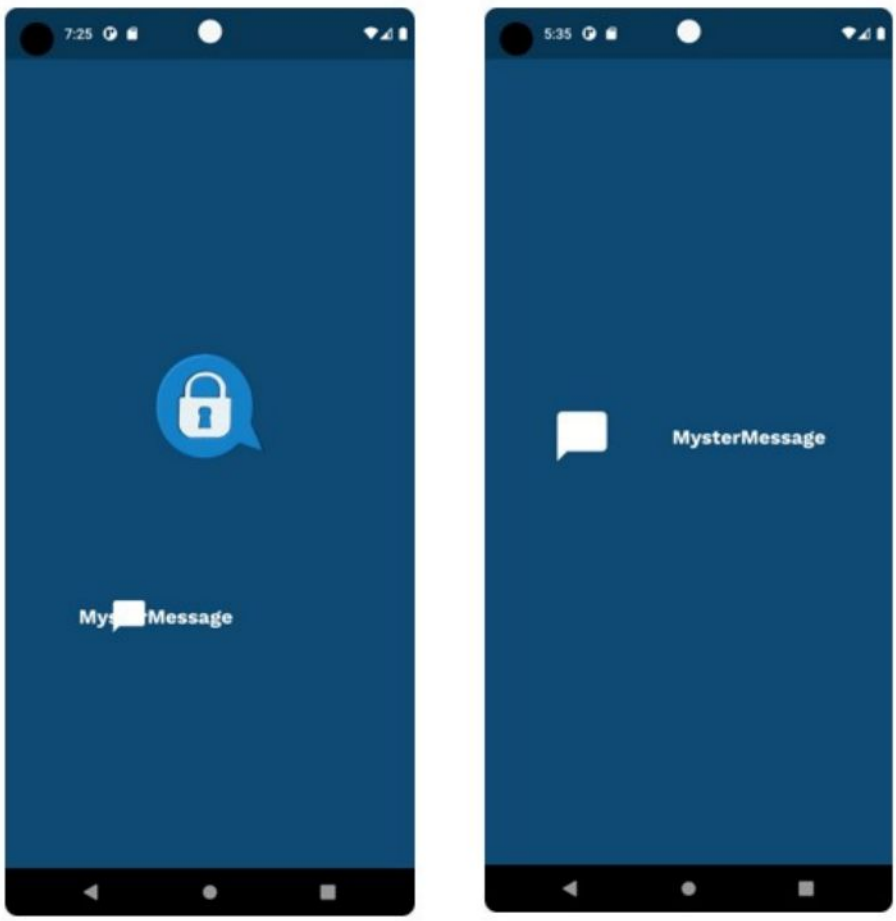

FIGURE 4.6 – SplashScreen

4.5.2 Interfaces d'accueil

Après le splashScreen, une page d'accueil s'affiche, cette page d'accueil constitue le point de départ de l'interaction avec l'application "MysterMessage" .

FIGURE 4.7 – Interfaces d'accueil

4.5.3 Interfaces d'inscription

Une fois que l'utilisateur clique sur le bouton "Inscrire", une interface d'inscription s'affiche, mettant en avant un champ spécifique réservé au numéro de téléphone. L'utilisateur est invité à y saisir son numéro de téléphone. Par la suite, un code OTP (One-Time Password) est envoyé au numéro de téléphone fourni. Une fois que l'utilisateur reçoit le code, une interface de vérification d'OTP s'affiche, permettant à l'utilisateur de saisir le code reçu cette étape de vérification garantit la sécurité et l'authenticité du processus d'inscription.

Une fois que l'utilisateur a vérifié avec succès le code OTP, l'interface de création de compte se poursuit. L'utilisateur est alors invité à saisir son nom d'utilisateur et à sélectionner une photo de profil. Ces éléments permettent à l'utilisateur de personnaliser son compte et d'établir son identité au sein de l'application "MysterMessage" . L'interface peut offrir des fonctionnalités supplémentaires, telles que le chargement d'une photo depuis la galerie de l'appareil ou la possibilité de prendre une photo en temps réel.

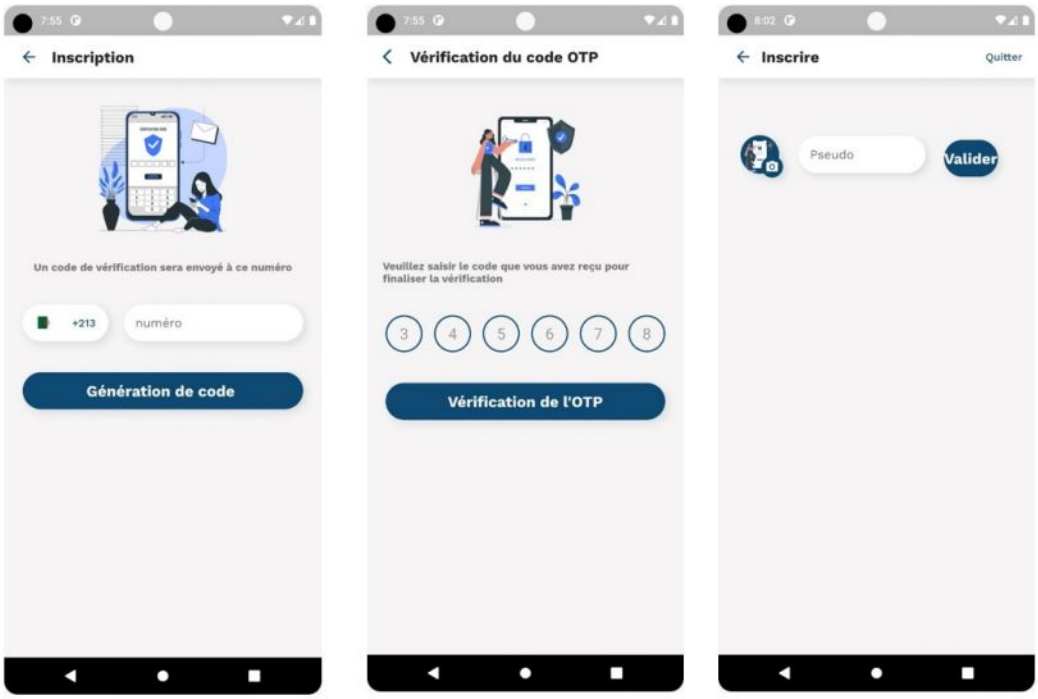

FIGURE 4.8 – Interface d'inscription

4.5.4 Interface de Paramètres

L'interface de paramètres permet aux utilisateurs de modifier les informations de leur compte, y compris leur nom et leur photo. Une fois connecté à l'application "MysterMessage", les utilisateurs peuvent accéder à cette interface dédiée, accessible à partir d'un menu. L'interface de paramètres offre aux utilisateurs la possibilité de modifier leur nom d'utilisateur en saisissant un nouveau nom dans le champ dédié. Cela permet aux utilisateurs de mettre à jour leur identité affichée au sein de l'application.

En ce qui concerne la photo de profil, les utilisateurs peuvent également modifier cette dernière en sélectionnant une nouvelle image depuis la galerie de leur appareil ou en utilisant la fonction de prise

de photo en temps réel. Cela offre aux utilisateurs la possibilité de personnaliser leur représentation visuelle au sein de l'application "MysterMessage". L'interface de paramètres permet également aux utilisateurs de supprimer leur compte. Une fois qu'ils accèdent à cette interface, ils peuvent trouver l'option de suppression du compte. Lorsqu'un utilisateur choisit de supprimer son compte, il est invité à confirmer sa décision pour des raisons de sécurité et pour éviter les suppressions accidentelles. Cela peut se faire en affichant un message de confirmation.

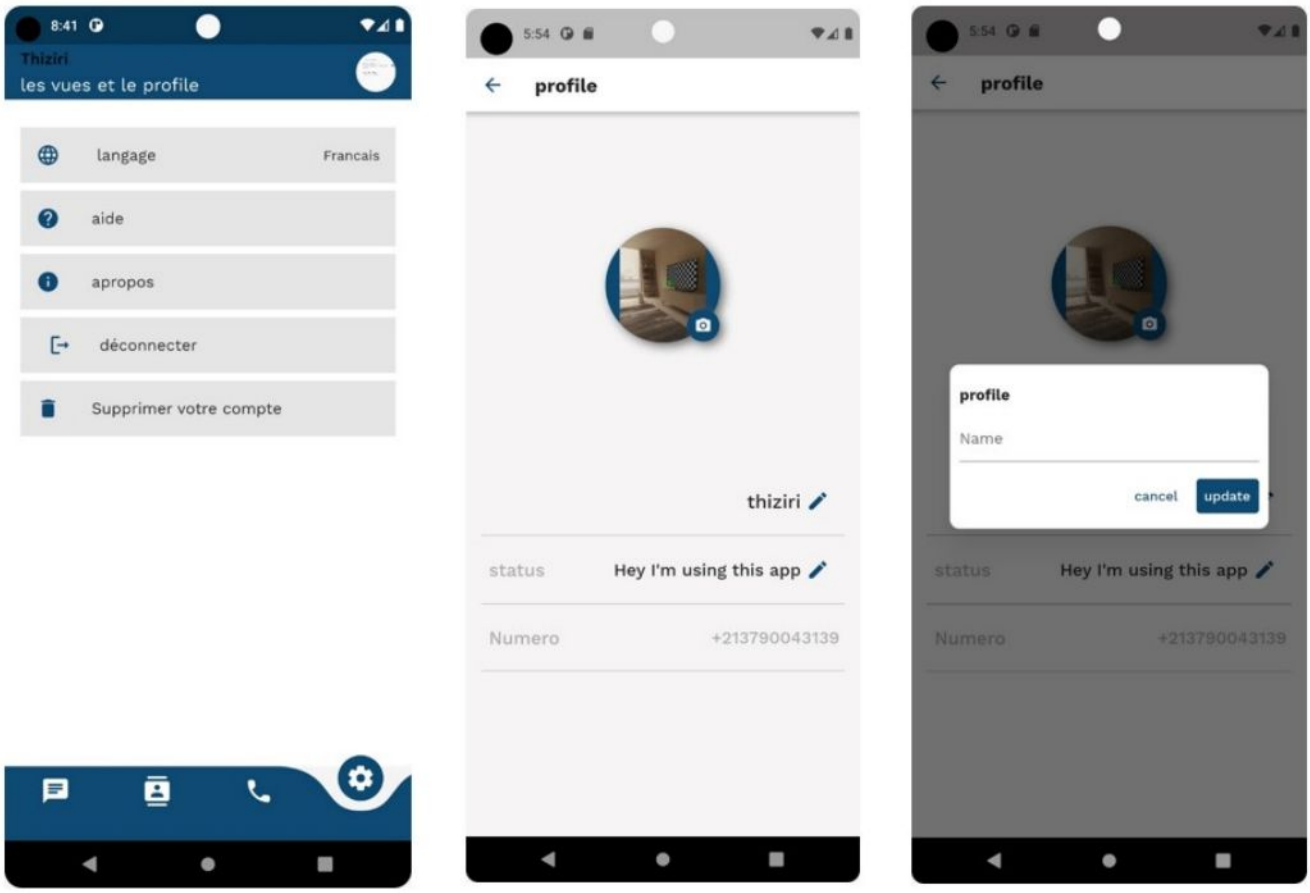

FIGURE 4.9 – Interface de paramètres cas "modifier le profil"

4.5.5 Interface de chat

L'interface de chat est la fenêtre graphique qui permet aux utilisateurs de communiquer et d'échanger des messages en temps réel dans notre application "MysterMessage".

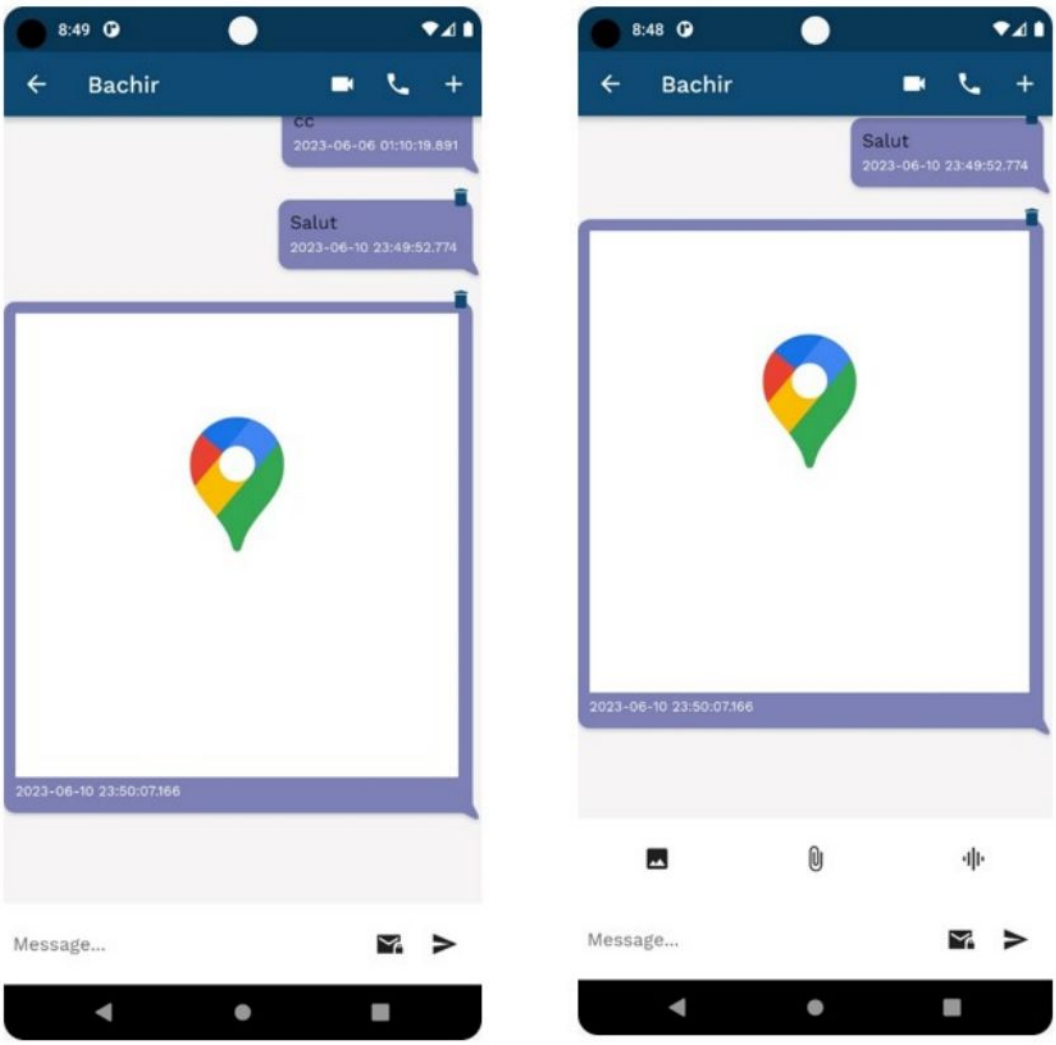

FIGURE 4.10 – Interface de chat

4.5.6 Interface Contacts

L'interface de contacts est une composante essentielle dans notre application "MysterMessage" qui présente de manière organisée une liste de contacts ou de personnes avec lesquelles un utilisateur peut établir des communications. Son rôle est de faciliter la gestion des contacts en offrant des fonctionnalités telles que l'accès aux informations détaillées des contacts, la possibilité de rechercher des contacts spécifiques et d'envoyer/recevoir des invitations pour établir une connexion. Cette interface permet à l'utilisateur de gérer efficacement sa liste de contacts en lui offrant la possibilité d'ajouter de nouveaux contacts, de supprimer des contacts existants.

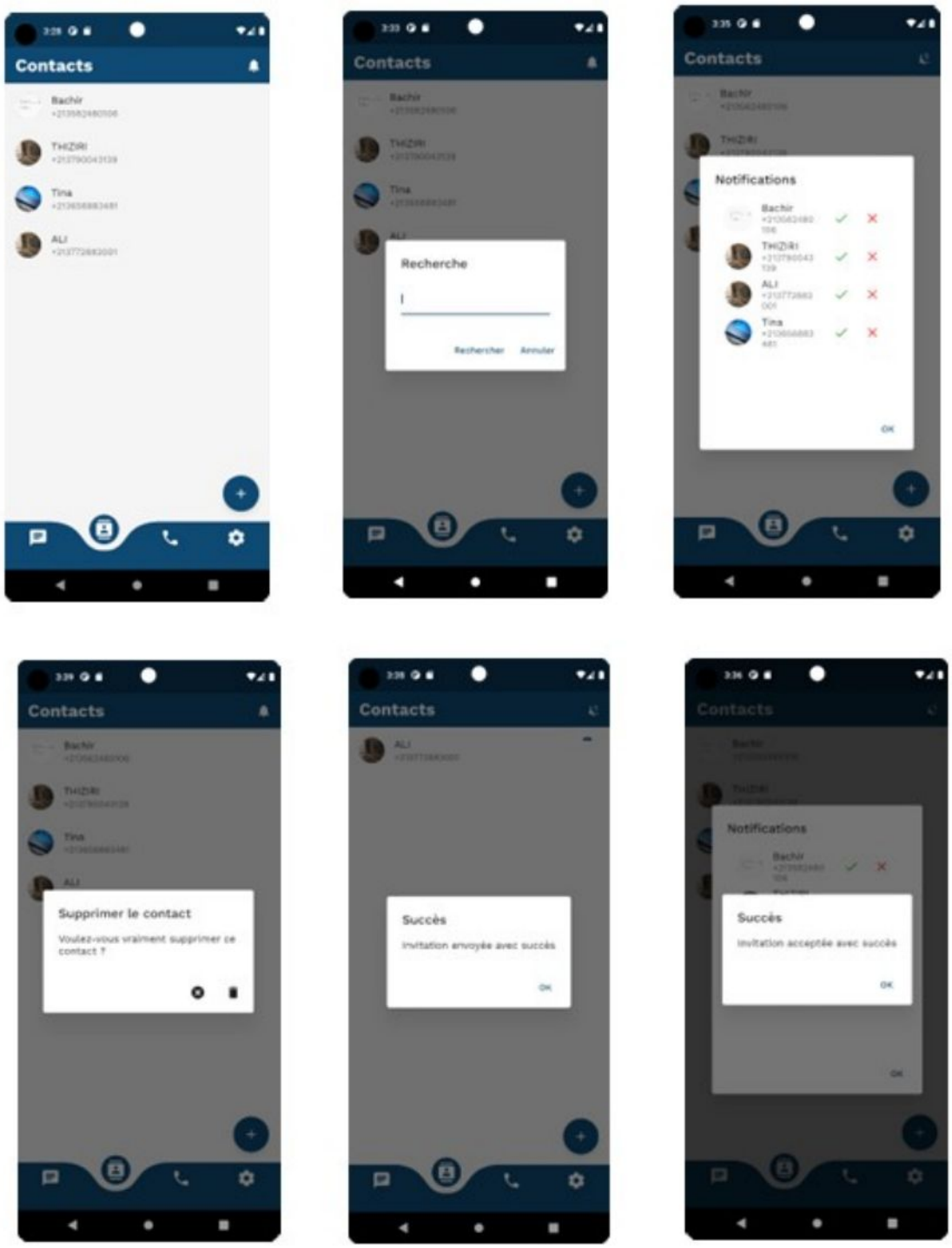

FIGURE 4.11 – Interface de contacts

4.5.7 Interfaces stéganographie image

Les interface de stéganographie d'image sont des parties dans notre application "MysterMessage" qui permet aux utilisateurs d'effectuer des opérations de dissimulation et de récupération de données secrètes au sein d'une image. Ces interfaces fournissent les outils nécessaires pour cacher des informations confidentielles de manière invisible au premier regard, tout en préservant l'apparence normale de l'image.

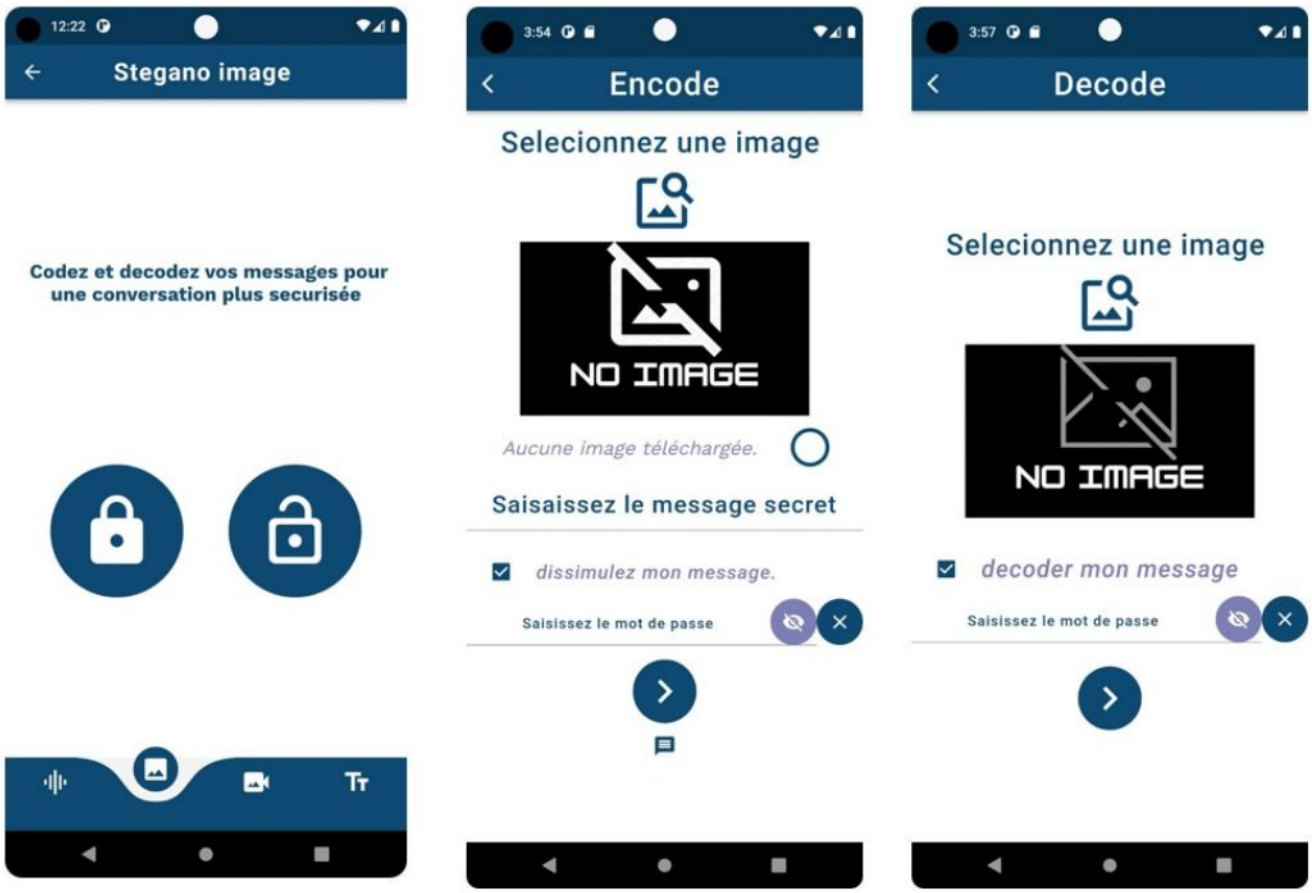

FIGURE 4.12 – Interface de la stéganographie image

4.5.8 Interfaces stéganographie audio

Les interfaces de stéganographie audio de notre application "MysterMessage", permet aux utilisateurs d'effectuer des opérations de dissimulation et récupération de données secrètes dans un audio. Ces interfaces fournissent les outils nécessaires pour cacher des informations confidentielles .

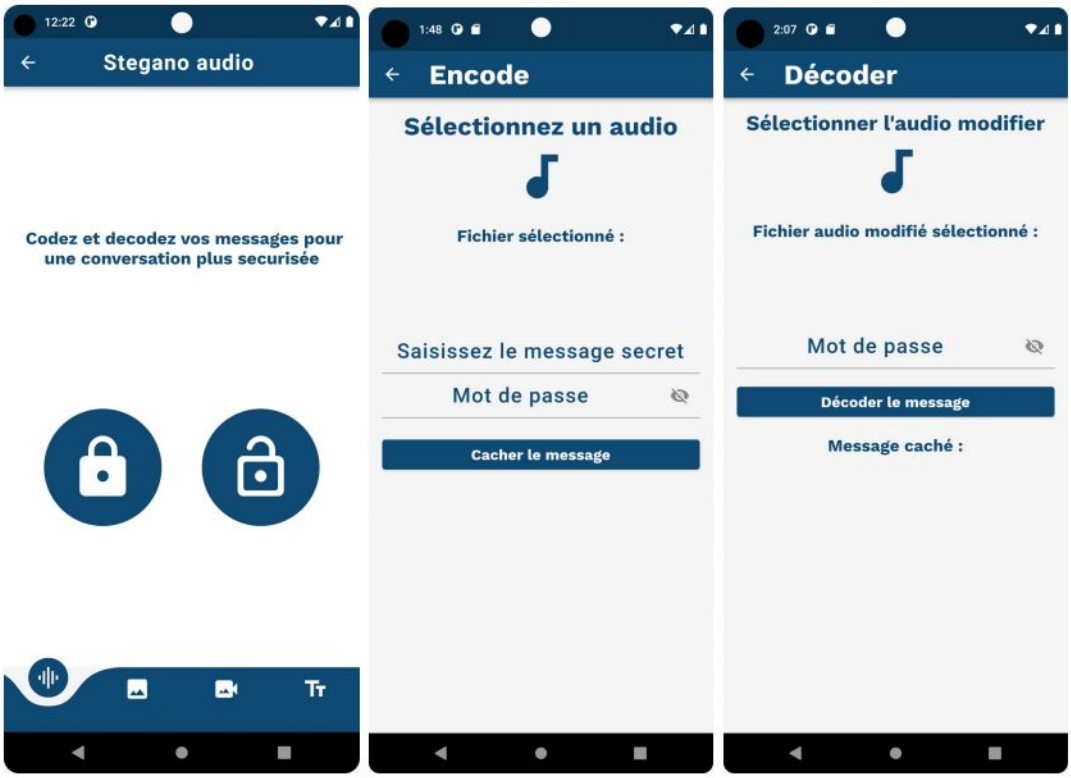

FIGURE 4.13 – Interface de la stéganographie audio

4.5.9 Interfaces stéganographie texte

Les interfaces de stéganographie texte de notre application "MysterMessage" , permet aux utilisateurs d'effectuer des opérations de dissimulation et récupération de données secrètes dans un texte. Ces interfaces fournissent les outils nécessaires pour cacher des informations confidentielles .

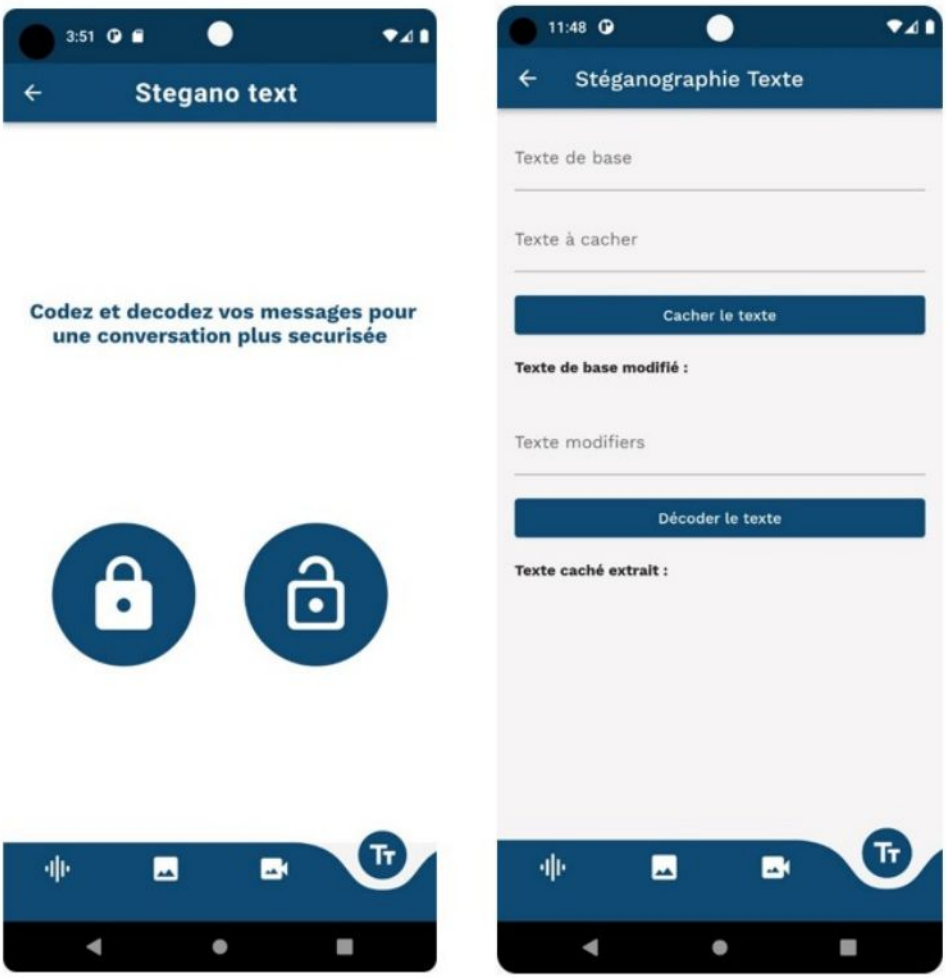

FIGURE 4.14 – Interface de la stéganographie texte

4.5.10 Interfaces stéganographie vidéo

Les interfaces de stéganographie vidéo de notre application "MysterMessage" , permet aux utilisateurs d'effectuer des opérations de dissimulation et récupération de données secrètes dans un vidéo. Ces interfaces fournissent les outils nécessaires pour cacher des informations confidentielles .

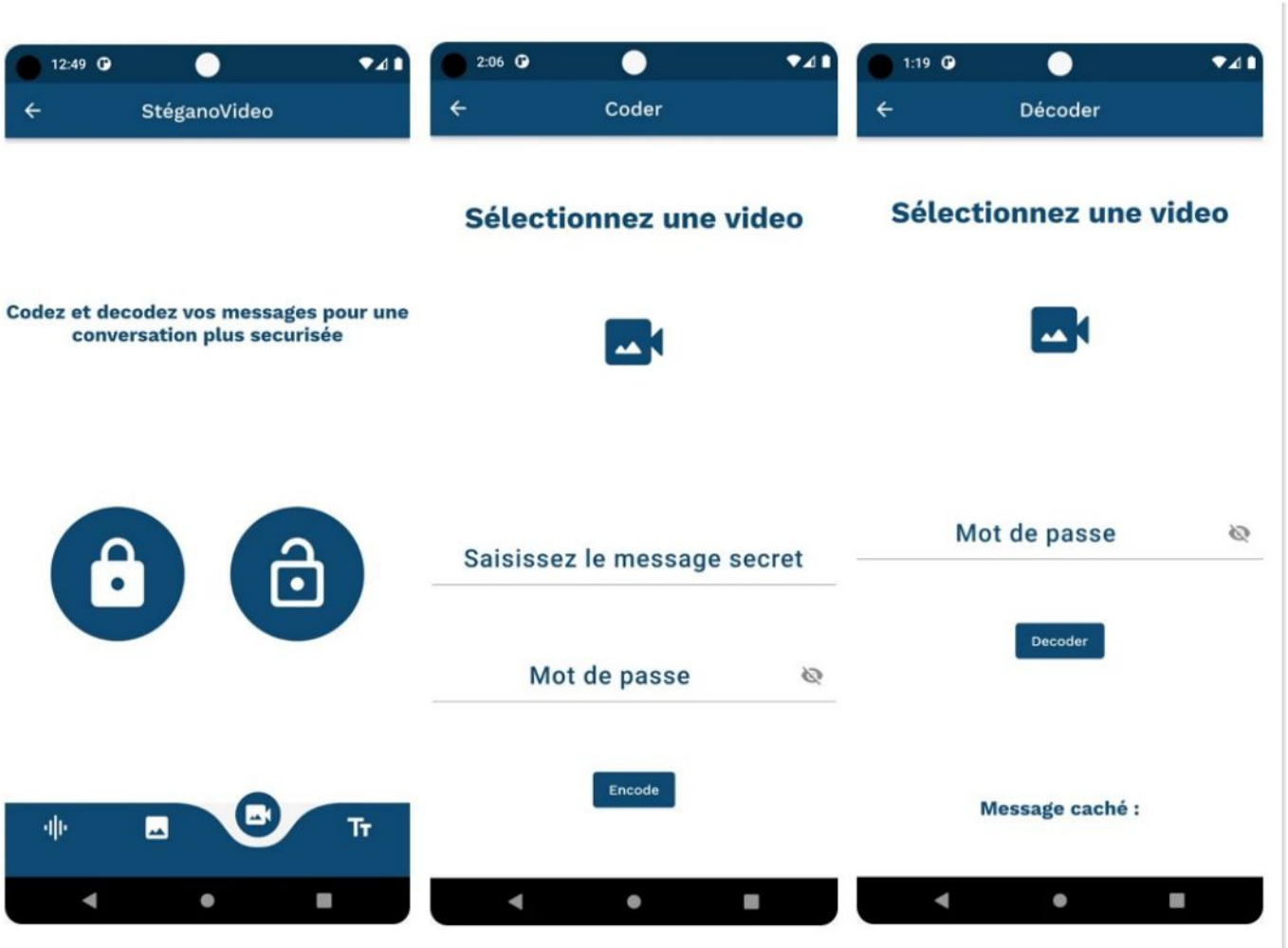

FIGURE 4.15 – Interface de la stéganographie vidéo

4.6 Conclusion

En conclusion, cette section a introduit les différents outils et logiciels que nous avons utilisés pour la mise en pratique de notre projet, suite à l'étape d'analyse et de conception. Nous avons présenté une variété de langages, d'outils et de logiciels qui ont été essentiels pour la réalisation de notre application "MysterMessage" . De plus , nous avons mis en avant les interfaces principales de "MysterMessage" , en soulignant leurs fonctionnalités et leur conception visuelle. Ces éléments constituent une base solide pour la suite de notre projet, nous permettant de passer à l'étape suivante avec confiance et clarté.

conclusion générale et perspectives

En conclusion, ce mémoire a exploré en profondeur le domaine de la conception et de la réalisation d'un système de messagerie basé sur la stéganographie. Notre objectif principal était de développer une solution sécurisée et confidentielle pour la communication entre les utilisateurs, en utilisant des techniques de dissimulation d'informations au sein de supports numériques.

Tout au long de notre travail, nous avons étudié les fondements théoriques de la stéganographie, en comprenant ses principes, ses types de supports et ses méthodes d'insertion. Nous avons également réalisé une analyse approfondie des besoins et des fonctionnalités attendues pour notre système de messagerie stéganographique.

En mettant en pratique nos connaissances théoriques, nous avons procédé à la conception et à l'implémentation de notre application "MysterMessage" de messagerie. Nous avons développé des fonctionnalités telles que la dissimulation des messages dans des images, la gestion des contacts et la sécurité des données échangées.

Au cours de notre travail, nous avons rencontré des défis techniques et conceptuels, mais nous avons réussi à les surmonter grâce à des recherches approfondies et à des efforts de programmation. Nous sommes convaincus que notre système de messagerie stéganographique offre un niveau de sécurité supplémentaire en permettant aux utilisateurs de communiquer de manière discrète et confidentielle.

Ce mémoire nous a permis de consolider nos connaissances en stéganographie et en développement d'applications sécurisées. Nous sommes fiers d'avoir réussi à concevoir et à réaliser un système de messagerie basé sur la stéganographie, qui répond aux besoins de confidentialité et de sécurité dans les communications numériques.

Et comme tout projet, qui nécessite une continuité et des améliorations , nous proposons pour des futures travaux les perspectives suivantes :

- Effectuer des appels audio et vidéo afin de permettre aux utilisateurs de passer des appels audio et vidéo en temps réel.
- Utiliser d'autres supports en stéganographie pour renforcer la confidentialité des informations dissimulées et permet de trouver des solutions adaptées à différents scénarios de confidentialité.
- Synchroniser cette application mobile avec une application web.

Bibliographie

Livres :

[1] AVINASH K. GULVE SATISH BHALASHANKAR. Audio steganography : LSB Technique Using a Pyramid Structure and Range of bytes. International journal of Advanced computer research, page 233, 2015.

[2] DAVID GABAY et JOSEPH CABAY. UML2 Analyse et conception. Livre, édition Dunod, Paris,2008.

[3] MOHAMMAD J. ALHADDAD DOAA A. SHEHAB.Comprehensive Survey of Multimedia Stéganalysis : Techniques, Evaluations, and Trends in Future Research, symmetry, Page 8. PhD thesis,2022

[4] PREETI SONDHI, SHIVANI GUPTA et GARAGI KALIA. Vidéo Steganography Using Discrete Wavelet Transform and Artificial Intelligence. Journal of trend in scientific research and development (ijtsrd), page 1211,2019

Mémoires et thèses :

[5] BENDJERIOU RAMZI et ARAR ABDELHAKIM. Une étude comparative entre la stéganographie jpeg et la stéganographie TCP/IP pour une meilleure technique de dissimulation de données. Thèse doct. Thèse master académique, Université KASDI MERRBAH OUERGLA.2016.

[6] DJEBRI LEILA et DEMMOUCHE SABRINA. Réalisation d'un système de dissimulation de données secrètes dans les images (la steganographie). Mémoire fin d'étude master 2, Université AKLI MOHAND OULHDJ BOUIRA,2017-2018.

[7] DR. BARIKH. Sécurité de l'information par stéganographie basée sur les séquences chaotiques. Thèse de doctorat, Université de BAYROUTH(LIBAN) ,18/05/2015.

[8] HUGO ALTARISTA SALAS. La steganographie moderne l'art de la communication secrète. Mémoire stage de master 2, Université MONPELLIER 2, 2009-2010.

[9] KOBSI KOUIDER. La stéganologie (stéganologie et stéganalyse). Mémoire fin d'étude master 2 intelligence artificielle et traitement de l'information, Université BADJI MOKHTAR, ANNABA, 2020-2021.

[10] RAHOUA AHMED. Steganographie d'images à l'aide de l'apprentissage automatique. Mémoire de fin de cycle master, Université MOHAMED KHIDER – BISKRA, 2020-2021.

[11] SARRA KOUIDER Insertion adaptative en steganographie : application aux images numériques dans le domaine spatial. Thèse de doctorat, Université MOPELLIER 2, 2013

Webographie :

[12] BMP Tools sur le site blogdumoderateur. https://www. blogdumoderateur.com/Tools/Telegram, Consulté le 28/05/2023.

[13]CLUBIE.https://www.clibic.com/pro/entreprises/google/actualite-17297-android-studio-4-1-debarque-a html, Consulté le 28/05/2023.

[14] CNETFRANCE. http://www.cnetfrance.fr/,Consulté le 28/05/2023.

[15] DART.https://www.dart.dev/, Consult´e le 28/05/2023.

[16] DEVELOPER.https://developer.anderoid.com/studio. Consulté le 28/05/2023.

[17]DEVELOPER.https://developers.googleblog.com/2016/05/firebase-expands-to-become-unified-app.html, Consulté le 28/05/2023.

[18] FLUTTER. https://flutter.dev/, Consulté le 28/05/2023.

[19] FIXTHEPHOTO. https://fixthephoto.com/best-private-photo-sharing-app.html, Consulté le 30/05/2023.

[20]LA STEGANOGRAPHIE – e-learning-facsci-univ-annaba.dz. https://elearning-facsci.univ-annaba.dz/pluginifile.php/9429/mod-resurce/content/1/Steganographie%20IATI.pdf.

[21] MUZLI Search. https://search.muz.li/ODc0N2VkYMI0, Consulté le 12/05/2023

[22] PHONEWORLD. https://phoneworld.com/whatsapp-adroid-update-a-major-redesigned-interface-is-comin, Consulté le 29/05/2023.

[23]PROCESSUS DE DEVLOPPEMENT-LOGICIEL Université Paris 13. https://docplayer.fr/1027770-Processus-de-developemment-logiciel.html

[24] SECURITE DES APPLICATIONS DE MESSAGERIE. https://www.Kaspersky.fr/resource-center/preemptive-safety/messaging-app-security. Consulté le 29/05/2023.

[25] STICK PNG. https://www.stickpng.com/img/icons-logos-emojis/tech-companies/visual-studio-code-full-logo, Consulté le 28/05/2023.

[26] VISUAL STUDIO CODE. https://code.visualstudio.com/docs, Consulté le 28/05/2023.

Résumé

La préservation de la confidentialité des informations des utilisateurs dans les réseaux sociaux est devenue une préoccupation grandissante, suite aux nombreux incidents de violations de données signalés. Face à cette problématique, les utilisateurs sont à la recherche de solutions leur permettant de sécuriser leurs échanges et de préserver la confidentialité de leurs communications. C'est dans cette optique que nous avons entrepris la création d'une application mobile de messagerie "MysterMessage" reposant sur la stéganographie. Pour réaliser ce projet, nous avons opté pour le Framework Flutter, qui permet le développement d'applications mobiles multiplateformes. Flutter offre une grande flexibilité et des fonctionnalités avancées pour créer des interfaces utilisateur réactives et attrayantes, essentielles pour offrir une expérience utilisateur optimale. En ce qui concerne le stockage et la gestion des données, nous avons choisi Firebase, une plateforme de développement d'applications mobiles en nuage. Firebase offre une base de données en temps réel, une authentification sécurisée, ainsi que des fonctionnalités de messagerie et de notification, qui sont essentielles pour une application de messagerie performante et sécurisée. L'association de Flutter et de Firebase nous permet de bénéficier des avantages d'un développement rapide et efficace, tout en assurant la sécurité et la confidentialité des données de nos utilisateurs.

Mots clés : Application mobile , Messagerie, Stéganographie, Flutter .

Abstract

Preserving user information confidentiality in social networks has become an increasingly prominent concern due to numerous reported data breaches. Faced with this issue, users are actively seeking solutions that can secure their exchanges and safeguard the privacy of their communications. With this objective in mind, we embarked on creating a mobile messaging application "MysterMessage" based on steganography. To realize this project, we choose the Flutter framework, which enables the development of cross-platform mobile applications. Flutter offers great flexibility and advanced features for creating responsive and visually appealing user interfaces, which are crucial for delivering an optimal user experience. Regarding data storage and management, we selected Firebase, a cloud-based mobile application development platform. Firebase provides real-time database capabilities, secure authentication, as well as messaging and notification functionalities, all of which are essential for a performant and secure messaging application. By combining Flutter and Firebase, we benefit from the advantages of rapid and efficient development while ensuring the security and confidentiality of our users data.

Keywords : Mobile Application , Messaging , Steganography , Flutter