Tatouage et objets 3D

Chapitre 1

Les techniques d'écriture secrète et leurs applications

1.1 Bref historique de l'écriture discrète

Il faut ici distinguer deux types de méthodes stéganographiques : celles reposant sur une avancée technique, et celles rendues possibles par une avancée purement scientifique. Dans la première catégorie, on peut ranger des stratagèmes aussi variés que l'encre sympathique[29], le crâne d'un émissaire, des tablettes de cire apparemment vierges, les micro-impressions des imprimantes laser, etc. On se souvient moins que Giacomo Casanova, afin de planifier son évasion de la prison des Plombs à Venise, échangeait force missives avec son complice en les cachant dans la doublure d'un livre, que leur gardien commun se faisait une joie de faire circuler naïvement entre eux, se réjouissant de contribuer à l'élévation morale des deux détenus. Casanova fut, dans la longue histoire de cette prison autrement plus redoutable qu'Alcatraz, le seul à s'en être échappé[30]. L'histoire regorge d'exemples d'astuces de cet acabit, et il est à parier que la plupart des prisonniers du monde ont un jour songé au problème de la communication secrète... Nous n'aborderons pas davantage ces techniques, pour nous concentrer sur les méthodes plus scientifiques, dans lesquelles une méthode est seule à l'œuvre.

Le premier traité abordant la stéganographie semble être celui de l'abbé Trithemius, *Steganographia* (écrit en 1499, publié en 1606). Le livre IV propose une étude des acrostiches stéganographiques et donne une liste de mots dont la deuxième lettre peut servir à trans-

[29]Dans *Le Scarabée d'or*, Poe ne met pas seulement en scène un cryptologue averti : William Legrand est aussi versé dans l'art de rendre l'écriture invisible. "Vous savez bien qu'il y a, il y en a eu de tout temps, des préparations chimiques, au moyen desquelles on peut écrire sur du papier ou sur du velin des caractères qui ne deviennent visibles que lorsqu'ils sont soumis à l'action du feu. On emploie généralement le safre, digéré dans l'eau régale et délayé dans quatre fois son poids d'eau ; il en résulte une teinte verte. Le régule de cobalt, dissout dans l'esprit de nitre, donne une couleur rouge. Ces couleurs disparaissent plus ou moins longtemps après que la substance sur laquelle on a écrit s'est refroidie, mais reparaissant à volonté par une application nouvelle de la chaleur." (Edgar Poe, *Le Scarabée d'or*, in *Histoires extraordinaires*, trad. Ch. Baudelaire.)

[30]Cette histoire, tirée des Mémoires de Casanova, est publiée sous le titre *Histoire de ma fuite des Plombs* (10/18, 1999). Mais Casanova fut encore, entre autres, le banni d'Italie qui fut chargé, par privilège royal, de fonder l'ancêtre de la Loterie Nationale en France, tant il avait rapidement su se mettre en cour de ce côté-ci des Alpes afin de fuir la justice de son pays...

mettre un message secret. La plupart des idées proposées dans cet ouvrage seront compilées par Gaspar Schott en 1665 dans son *Schola Steganographica*, il y rajoute une méthode permettant de cacher des messages dans une partition de musique en associant une lettre à une note. Il a fait école puisque nombre de musiciens, Bach le premier[31], se sont servi du thème musical en si bémol, la, do, si pour leurs œuvres : ce thème s'écrit B.A.C.H. dans la notation allemande. Schumann encore a rendu hommage à sa fiancée Ernestine von Fricken (Estrella dans le Carnaval), originaire du village de Asch en Bohême[32]. Pour cela, le Carnaval adopte les tonalités la, mi bémol, do, si (A-Es-C-H) et la bémol, do, si (As-C-H dans la notation allemande). L'enluminure était elle aussi un moyen de coder de l'information : les feuilles des arbustes généreux qui ornent les traités du mathématicien Viète ne sont pas disposées innocemment... Il faut attendre 1594 et la publication par Sir Hugh Platt de *The Jewel House of Art and Nature, conteining divers rare and profitable Inventions*, pour que le sujet trouve un nouveau souffle. L'auteur y expose une méthode de stéganographie permettant d'écrire secrètement un message, qui ne puisse être découvert ni même suspecté. Mais, sans se cantonner aux techniques subtiles, il faut reconnaître à Boccace (1313-1375) d'avoir écrit un des plus fameux acrostiches stéganographiques avec son *Amorosa Visione*.

Il est en général un "média" sur lequel on peut cacher de l'information et qui n'est pas souvent mentionné : le langage parlé. On opère une modulation secrète (pseudo-déterministe ou pas) des syllabes entendues (réellement dans le cas de l'argot ou marmonnées en lisant un grimoire hermétique). En effet, l'histoire montre que deux procédés ont été utilisés pour cacher (ou tout au moins bien dissimuler) un message dans le langage parlé. Le premier procédé est la dérivation synonymique, qui est au cœur de l'argot, du jargon, de la langue verte, du blason. Le second est la dérivation phonétique, qui concerne l'alchimie, ou Langue des Oiseaux, la transmission ésotérique de l'information. Nous esquissons rapidement la description de ces deux procédés, mais le lecteur *curieux* est invité à se reporter aux références pour plus de détails, souvent étonnants. Naturellement, des connexions existent : on trouve des ouvrages consacrés au blason hermétique...

Nous souhaitons évoquer un instant des procédés parfois oubliés qui montrent à quel point l'homme s'est intéressé au problème, dans la vie de tous les jours, en utilisant son "média" le plus immédiatement accessible : le langage parlé. La dérivation synonymique se comprend intuitivement, en réalité implicitement (elle est déterminée par des règles comme nous verrons) : elle est adaptée à une communication rapide, sans écrit. Par contre, le procédé de dérivation phonétique mène souvent à des constructions non intuitives, qui sont une *optimisation* de contraintes : ce procédé n'est donc utilisable qu'à l'écrit (il suffira de marmonner le texte lu pour commencer à faire apparaître son autre dimension[33]).

La dérivation synonymique consiste à *maquiller* le langage naturel. C'est *en référence*

[31]Citons parmi les plus connus "L'Art de la fugue", de J.-S. Bach, "Sechs Fugen über den Namen Bach", Op. 60, de Schumman, les "Fantaisie et fugue sur B.A.C.H." et "Prélude et fugue sur B.A.C.H." de Liszt, et la "Fantaisie et fugue sur B.A.C.H." de Reger (*Dictionnaire encyclopédique de la musique*, p. 172, Oxford, D. Arnold Ed., Robert Laffont, 1988).

[32]U. Michels, *Guide illustré de la musique*, p. 141, Fayard, 1988.

[33]Ce qui est précisément tout le contraire de la stratégie phonétique de Flaubert, qui hurlait les phrases de ses romans depuis son "gueuloir", dans sa propriété isolée, afin de s'assurer de leur fluidité (d'une certaine manière pour "gommer les ambiguïtés phonétiques") - le recours quasi-systématique à l'imparfait aidant passablement il est vrai.

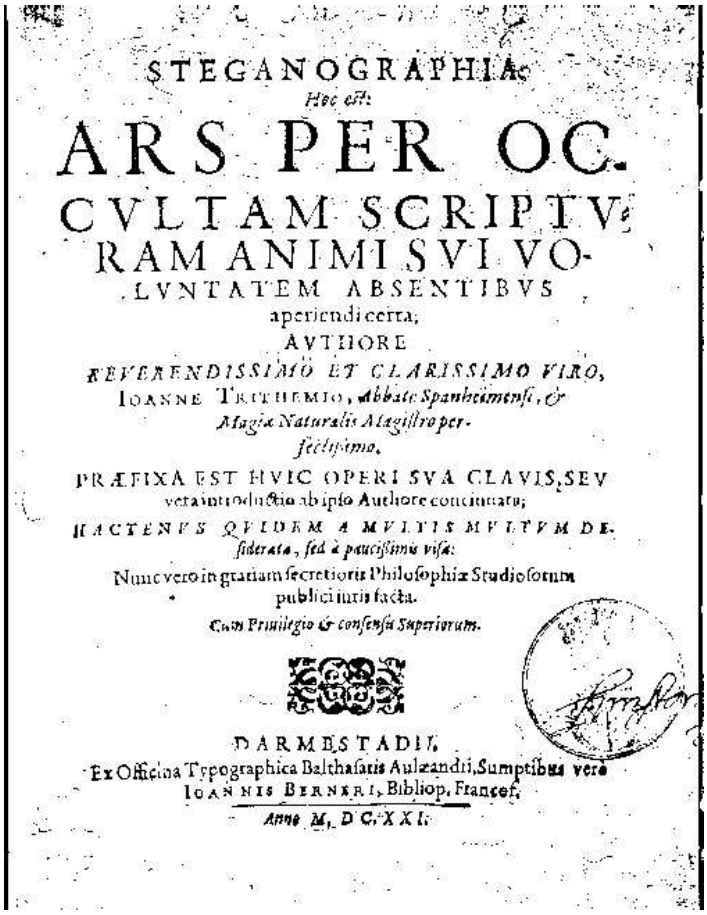
STEGANOGRAPHIA
Hoc eſt:
ARS PER OC.
CVLTAM SCRIPTV
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &
Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à paucißimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
DARMESTADII,
Ex Officina Typographica Balthaſaris Aulæandri, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DC. XXI.

FIG. 1.1 – Première page du *Steganographia* de l'abbé Trithemius (©Fabien Petitcolas).

au français que l'argot et le blason doivent être interprétés. La science du blason, ou héraldique (en quelque sorte l'ancêtre du rébus), vise à glisser une identité dans une composition graphique aux règles précises. Les illettrés, nombreux à l'époque, pouvaient ainsi deviner l'identité de la personne qui passait dans la rue en si grand équipage. Le blason, comme tout langage, a lui aussi été détourné pour y faire circuler des messages cachés, le plus souvent grivois ou licencieux, ou destinés à moquer le prince. Plus particulièrement, les modes de dissimulation du blason semblent à rapprocher du jargon Lanternois cher à Rabelais[34] (*Pantagruel*, IX), dont la phonétique donne l'impression de se rapprocher de celle d'une langue indo-européenne sans qu'il soit possible pour un non-initié d'y rien comprendre, seul Panurge le parle couramment[35] ! Le jargon est situé à la limite de la stéganographie et de la cryp-

[34]Afin de prémunir son identité réelle contre les multiples censures de ses œuvres par la Sorbonne, François Rabelais signait d'un anagramme : Alcofribas Nasier. Plus légèrement, il est encore l'auteur de la fameuse contrepèterie concernant les femmes folles de la messe. Toutefois, la banalité du procédé contrepétrique, et surtout la bienséance, dissuadent de s'y intéresser plus longtemps - bien qu'il s'agisse d'un procédé concernant pleinement notre propos, tout comme le palindrome.

[35]Voici un passage en Lanternois : "[...] Lors respondit Panurge. "Prug frest strinst sorgdmand strochdt drhds pag brleland. [..] Bouille kalmuch monach drupp delmeupplist rincq dlrnd dodelb vp drent loch minc stz

tographie. Marcel Schwob a assez bien montré dans ses *Etudes sur l'argot français* (Allia, 1999) que le jargon de la Coquille (célèbre bande de malfrats, tricheurs et voleurs assemblés en confrérie au XVIème siècle), ancêtre de l'argot[36], prend sa source dans la dérivation synonymique et le loucherbème, ou langage des bouchers, ancêtre de notre verlan (désormais supplanté par le "veul", une sorte de jusqu'auboutisme du verlan, dans les foyers de création argotique les plus en pointe). L'idée de la dérivation synonymique est qu'en jargon on exprime finalement peu de concepts, mais chacun avec de multiples mots. Le loucherbème est le nom du procédé générique de l'écriture inaccessible pour un non initié : le mot sera d'abord inversé, puis on lui ajoutera le préfixe "l" le plus souvent, et un suffixe, variable et peu important (le suffixe "-bème" a quasiment disparu mais il était très utilisé à l'époque). Le mot loucherbème veut donc dire boucher, car la profession des bouchers a été la première à systématiser ce procédé. C'est ce jargon des Coquillars qui a été utilisé par Villon dans ses *Ballades en Jargon*, car le poète, outre l'admiration qu'il vouait à Rabelais, était lié, au moins d'amitié disent les mauvaises langues, avec les gens de la Coquille. D'un point de vue cryptographique, la sécurité de l'argot (son incompréhension pour un non initié) repose sur le secret du procédé employé : sitôt éventé, les dictionnaires d'argot devenaient possibles, condamnant la langue verte à évoluer sans cesse. Toutefois, les catégories de Schwob permettent encore d'appréhender correctement l'argot moderne.

Si la dérivation synonymique est un des deux principaux procédés de l'argot (avec le loucherbème), le pendant de la Langue des Oiseaux est manifestement la dérivation phonétique[37]. Afin d'avoir l'idée la plus récente et claire du procédé[38], sans exhumer les ouvrages ésotériques de Fulcanelli, célèbre initié encore en activité à Paris au début du XXème siècle (et qui serait selon d'aucuns le pseudonyme de Camille Flammarion[39] (1842-1925) - célèbre astronome et érudit, fondateur en 1887 de la Société astronomique de France, et auteur en 1862 d'une curieuse *Pluralité des Mondes Habités*), il faut se reporter aux œuvres de quatre

rinquald de vins ders cordelis bur iocst stzampenards." À quoy dist Epistemon. "Parlez vous christian : mon amy, ou langaige patelinoys ? Non c'est langaige lanternoys." [...]" Rabelais, *Pantagruel*, Ch. IX, *Comment Pantagruel trouva Panurge lequel il ayma toute sa vie*, in *Œuvres Complètes*, Gallimard, Bibliothèque de la Pléïade, 1994, pp. 247 *sq.* Il n'est pas impossible que Rabelais ait jeté là les bases d'une nouvelle langue : il suffit de rappeler qu'il nous a légué environ 500 mots que nous utilisons encore (comme "encyclopédie"), parmi les milliers d'autres de son invention que nous n'avons pas conservés (à l'instar du trop obscène "circumbilivagination", auquel on a préféré tergiversation, qui illustre pourtant bien mieux par quel assemblage finalement surréaliste de latin mêlé de grec sont nés ces mots, leur conférant un sens quasi-implicite pour les *happy few* de l'époque). En réalité, il était plus difficile d'*entendre* Rabelais en 1535 qu'aujourd'hui, fut-ce dans le texte - ce qui augmentait l'effet comique.

[36]Schwob note que si le mot argot a d'abord désigné une bande de malfaiteurs avant de s'appliquer à leur langage, il faut alors sans doute chercher l'étymologie d'argot dans les quatre sections de la cour des Miracles : Egypte, Boëme, Argot, Galilée. Argot serait le mot d'argot pour désigner arabie, ainsi qu'en témoignent St-Lago pour St-Lazare, ou Italgo pour Italien ; les zouaves en expédition ont ramené Arbico pour Arabe (Schwob, *op. cit.*, p. 37).

[37]La tradition hermétique veut voir par exemple, dans l'image d'un St-François d'Assise familier des animaux et des oiseaux en particulier, une preuve à peine dissimulée de l'initiation du *Poverello* d'Ombrie aux connaissances occultes.

[38]En jazz vocal, André Minvielle utilise un procédé similaire : à travers un flot ininterrompu de mots, quelques-uns se détachent et forment ensemble un curieux assemblage du plus bel effet.

[39]Exemple de dérivation phonétique hermétique : Flammarion = Flamme d'Orion = ... = Fulcanelli. Le passage d'un terme à l'autre se fait en maniant des symboles (sel, soufre, soleil, pluton, etc.) dont les interactions sont codifiées, dans une langue ressemblant fort au grec ancien.

écrivains de sa connaissance qu'il fréquentait au Chat Noir : Gaston Leroux[40], Maurice Leblanc[41], Alfred Jarry[42] et Raymond Roussel. Une hypothèse souvent tue à leur sujet veut que leurs ouvrages aient tous pour canevas l'oeuvre de Fulcanelli, du point de vue des procédés introduisant le mystère (c'est dire la complexité supposée des ouvrages de l'alchimiste). Selon cet initié, l'étymologie du mot cabale doit être trouvée dans l'ancien grec $\kappa\alpha\rho\beta\alpha\nu$ ("qui parle un langage incompréhensible"). Le langage hermétique, à travers la cabale[43] du même nom, distincte et sans doute plus récente que la Cabale hébraïque, aurait donc "visé l'ésotérisme le plus absolu, en greffant sur les méthodologies classiques, dans les traités alchimiques, un système linguistique hybride fait des assonances qui détournaient les mots d'usage courant. Il fallait ainsi lire non seulement le sens commun mais aussi suivant les sens que les mots, par affinité phonétique, pouvaient prendre dans l'antique idiome hellénique." [44]. Ce procédé, dans les détails duquel nous n'entrerons pas davantage, interdit quasiment toute analyse fondée sur la logique classique[45]. Roussel nous a légué une idée d'un des procédés dans sa compilation d'oeuvres de grande jeunesse intitulée *Comment j'ai écrit certains de mes livres.* Il y pousse le procédé à fond et obtient un effet poétique inédit et très efficace en pratique[46]. Ces textes courts présentent tous la même particularité : les premiers et derniers mots étant fixés par leur proximité phonétique (à un phonème près en général), l'auteur en déduisait une histoire permettant de faire le lien. Par exemple, le texte *Parmi les Noirs* débute par les mots "Les lettres du blanc sur les bandes du vieux billard", et se termine par "LES... LETTRES... DU... BLANC... SUR... LES... BANDES... DU... VIEUX... PILLARD." Nous citons Roussel[47] : "Dans la première [phrase], "lettres" était pris dans le sens de "signes typographiques", "blanc" dans le sens de "cube de craie" et "bandes" dans le sens de "bordure". Dans la seconde, "lettres" était pris dans le sens de "missives", "blanc" dans le sens d'"homme blanc" et "bandes" dans le sens de "hordes guerrières". Les deux phrases trouvées, il s'agissait d'écrire un conte pouvant commencer par la première et finir par la seconde." Du propre aveu de Roussel, il s'agit d'un procédé purement poétique, qui a été appelé translittération[48]. En

[40]Faut-il rappeler les tenants et les aboutissants du *Mystère de la chambre jaune* ?

[41]Il multiplie les anagrammes pour son héros Arsène Lupin : Luis Perenna, Paul Sernine, etc.

[42]Dont le penchant avéré pour le déguisement des mots est connu : Ubu ne manie que trop la "pompe à phynances".

[43]Voici, naturellement enveloppée d'un mystère qui en est la marque de fabrique, la définition que donne Fulcanelli de la cabale hermétique : "Le latin caballus et le grec $\kappa\alpha\beta\alpha\lambda\lambda\eta\sigma$, signifient tous deux cheval de somme ; or, notre cabale soutient réellement le poids considérable, la somme des connaissances antiques et de la chevalerie ou "cabalerie" médiévale, lourd bagage de vérités ésotériques transmis par elle à travers les âges. C'était la langue secrète des cabaliers, cavaliers ou chevaliers. Initiés et intellectuels en avaient tous la connaissance. Les uns et les autres, afin d'accéder à la plénitude du savoir, enfourchaient métaphoriquement la cavale, véhicule spirituel dont l'image type est le Pégase ailé des poètes helléniques. Lui seul facilitait aux élus l'accès des régions inconnues ; il leur offrait la possibilité de tout voir et de tout comprendre, à travers l'espace et le temps..." (cité par A. Aromatico, *L'alchimie*, Gallimard, 1996, p. 45).

[44]A. Aromatico, *op. cit.*, p. 54.

[45]Au sujet de son *Ulysse*, James Joyce n'écrivait-il pas : "J'y ai mis tant d'énigmes que cela aura de quoi occuper les universitaires pendant encore quelques siècles... C'est ça l'immortalité."

[46]Le procédé de Roussel, à la différence du procédé hermétique, ne "suggère" pas un message en grec ancien, mais en français. Les musiciens potaches l'emploient dans une histoire sur la petite vertu supposée des filles de Lille car, paraît-il, le concerto en sol mineur (on notera que Simmons a proposé un cryptosystème avec des caractéristiques similaires de "double-décodage" [70]).

[47]Voir *Comment j'ai écrit certains de mes livres*, Gallimard, 1935.

[48]La théorie du sens caché dans les livres de Roussel ne trouve aucun écho chez Foucault dans son *Raymond*

liant ainsi deux phrases si proches phonétiquement par un récit-tampon, Roussel découvre au lecteur un nouvel espace de l'imaginaire qui interroge la nature même du texte. En ne donnant ainsi que *l'illusion* d'un sens caché, Roussel invente une sorte de "tatouage littéraire" de l'imaginaire, à considérer le tatouage en général comme l'écriture d'un message dans une langue imaginée pour l'occasion, donc factice. La marque que Raymond Roussel introduit dans ses textes est une sorte de bruit de fond poétique reconnaissable qui favorise également toutes les conjectures de l'imaginaire, et dont la "couleur poétique" dépend du problème littéraire combinatoire que l'on s'est proposé d'optimiser (l'effet poétique obtenu n'est probablement pas prévisible d'ailleurs, car dépendant trop des viscissitudes et des contraintes du langage). Ce procédé est à rapprocher de la Langue des Oiseaux, fonctionnant elle aussi par dérivation phonétique, et dont nous pouvons à présent proposer un exemple : Hubert Champagne, lui aussi initié, ne signait jamais que de sa devise latine "Uber Campa Agna", autre exemple de translittération, laissant ainsi deviner les liens, au moins littéraires, unissant les quatre écrivains habitués du Chat Noir à la tradition occulte. L'époque était aussi celle d'un Paris du début du XXème siècle encore baigné par l'orientalisme et son goût du mystère. Peut-être le coup de génie de ces écrivains fut-il d'avoir mis au point une mécanique littéraire qui introduit l'illusion du sens caché. Bien évidemment, d'autres procédés trop ardus pour être décrits ici, furent développés par les quatre écrivains[49].

Parallèlement, les techniques purement cryptographiques poursuivent leur développement. Mais c'est en 1605 que Sir Francis Bacon[50], dans *Proficience and Advancement of Learning Divine and Humane*, donne sa préférence aux méthodes n'attirant pas la suspicion, c'est à dire à la stéganographie : "in regarde of the rawnesse and unskilfulnesse of the handes, through which they passe, the greatest Matters, are many times carried in the weakest cyphars". En disséquant les œuvres de Shakespeare, avec les outils cryptographiques de l'époque et un alphabet élisabéthain, certains pensent y avoir trouvé en filigrane le nom de Francis Bacon, qui n'était pas seulement un des cryptologues les plus renommés de son temps, mais aussi poète. Il est vrai que la vie obscure et mal connue de Shakespeare, couplée à la réputation de Bacon de conseiller de l'ombre, a pu alimenter toutes les controverses. Suivant l'avis de Bacon, la stéganographie tend à devenir un art supérieur en finesse et en efficacité à la cryptographie. Ce point de vue reste à notre sens encore valable aujourd'hui : un pare-feu sur le réseau peut très bien interdire la transmission de messages à forte entropie (supposés cryptés), sans jamais pouvoir déceler aucun contenu caché dans une image ou un son[51].

Roussel (Gallimard, 1963), même s'il prend soin de ne pas réfuter totalement cette éventualité. Il pensait certainement à *Locus Solus* (Pauvert, 1965), objet paraît-il d'intenses conjectures hermétiques.

[49]Toujours chez Roussel, l'écriture de ses *Impressions d'Afrique* lui a réclamé pas moins de sept ans (long poème en alexandrins sur 7 sept niveaux d'imbrication de parenthèses...) Mais il faut encore souligner que Roussel, méprisé de son vivant en tant qu'écrivain, fut également un joueur d'échecs émérite, qui laissa son nom dans l'histoire du jeu pour en avoir proposé une vision révolutionnaire : faire jouer les pièces "en coopération". Il a ainsi pu résoudre le premier, en trois mois et demi, le mat difficile dit "avec Fou et Cavalier", en 1932. En regard du degré de sophistication des procédés d'écriture qui ont pu être utilisés, l'anecdote est de taille.

[50]Dont l'appartenance hypothétique à l'ordre secret de la Rose-Croix, souvent évoquée, semble à rejeter.

[51]La légende des messages subliminaux prétendûment contenus dans les chansons de rock jouées à l'envers doit rester pour ce qu'elle est : une fiction inquisitrice égarée en plein XXème siècle. Le procès intenté à Judas Priest a permis de mettre en évidence que quantité de chansons jouées à l'envers peuvent suggérer des

Plus près de nous, Gustavus Simmons a mis en évidence l'existence d'un canal subliminal [69, 70] dans l'algorithme DSA (Digital Signature Algorithm) utilisé par le gouvernement américain. L'algorithme ElGamal est lui aussi susceptible de transmettre quelques dizaines de bits de manière subliminale. Toujours dans le domaine des outils cryptographiques, il est pour le moins surprenant que le protocole SSH (Secure SHell) n'impose pas de "Self-Describing Padding" mais un bourrage aléatoire, invérifiable, offrant par là un boulevard à l'évaporation des clefs chiffrant la connexion en cours, entre autres. Voilà qui plaide éloquemment pour l'utilisation de logiciels dont le code source est accessible. La découverte de canaux subliminaux par Simmons date de la guerre froide, lorsque les deux super-puissances devaient chacune pouvoir vérifier le nombre de têtes nucléaires de l'adversaire sans divulguer leur emplacement, variable dans le temps. Les USA et l'URSS se mirent d'accord sur un protocole cryptographique, dont Simmons a prouvé qu'il autorisait la transmission d'un bit d'information cachée au moins, augmentant potentiellement d'autant la connaissance de l'adversaire sur la localisation des missiles.

1.2 Tatouage et distribution des œuvres : une situation

Nous venons de dresser un bref panorama de la stéganographie et de son utilisation au cours des siècles, mais le tatouage son descendant trouve son origine dans le filigrane. C'est au XIVème siècle à Fabriano en Italie que les ouvriers produisant le papier renommé de cette région, eurent l'idée d'y inclure les premiers filigranes, essentiellement à des fins d'authentification de la provenance du papier. On visite aujourd'hui le musée dédié à ces premiers filigranes. Le filigrane trouva naturellement son cadre d'application privilégié dans les billets de banque. Voisin de la technique du filigrane, la flétrissure royale imposée sur l'épaule du criminel permettait de marquer à vie la félonie du sujet. Dans *Les trois mousquetaires*, Alexandre Dumas met en scène la flétrissure de Milady, qui permettra à D'Artagnan de la reconnaître à Béthune, même et surtout *Vingt ans après*. De nos jours, on utilise le marquage à l'encre pour tracer la provenance des viandes. Chez les Maori, entre autres, le tatouage marque le passage du garçon dans l'âge adulte à la suite d'une cérémonie initiatique[52]. Si le marquage autre que symbolique est récent chez l'homme, les canidés utilisent le marquage olfactif à l'urine pour délimiter leur territoire sans doute depuis qu'ils existent.

On peut argumenter que les besoins en tatouage étaient relativement limités dans un monde alors uniquement analogique, et la révolution numérique n'a fait que remettre au goût du jour cette technique. En effet, copier un document analogique implique nécessairement une perte de qualité de la copie par rapport à l'original, alors que la duplication de symboles numériques ne nécessite aucune transcription matérielle, autorisant la duplication parfaite à l'infini de l'original. Le tatouage numérique doit son développement pratique à celui d'internet essentiellement, et surtout au fait que les limites du système sensoriel hu-

messages cachés, mais qui n'ont pas souvent de sens...

[52]"[...] De même dans les traditions occidentales le tatouage a longtemps passé pour mettre à l'abri des démons, des mauvais esprits, des maladies et des accidents. Les marins, qui ont un engouement particulier pour les tatouages, croient, dit-on, que ceux-ci protègent des maladies vénériennes. [...] Dans la marine américaine, un cochon et un coq, tatoués sur le cou-de-pied gauche, préservent de la noyade." E. Mozzani, *Le livre des superstitions*, Robert Laffont, 1995, p. 1693.

main ne lui permettent pas de distinguer deux objets très proches en apparence. Mais nous ne percevons que trop bien quelle est la finalité plus profonde du tatouage. Cette finalité consiste à pouvoir dégager artificiellement, par des moyens purement techniques, l'authenticité d'une œuvre d'art (et par là, de nos jours, sa valeur[53]). Benjamin[54] notait en 1972 qu' "à la plus parfaite reproduction il manquera toujours *une* chose : le *hic* et *nunc* de l'œuvre d'art - l'unicité de son existence au lieu où elle se trouve."[55] Il définit ainsi l'authenticité de l'œuvre d'art, et poursuit : "Tous ces caractères [d'authenticité] se résument dans la notion d'aura, et on pourrait dire : à l'époque de la reproductibilité technique, ce qui dépérit dans l'œuvre d'art, c'est son aura."[56] La perception de l'œuvre change alors : à sa transcendance passée, réelle ou supposée, se substitue de nos jours une pure immanence. Le rapport à l'art, ce succédané de religion pour d'aucuns, est bouleversé, glissant à peu de choses près de l'extase du croyant s'étant déplacé tout exprès pour admirer la Vierge de la chapelle Sixtine, à la névrose compulsive du collectionneur de gigaoctets de MP3.

Se pose alors le problème de l'économie artistique : "[...] le fait qui est ici décisif : pour la première fois dans l'histoire universelle, l'œuvre d'art s'émancipe de l'existence parasitaire qui lui était impartie dans le cadre du rituel. De plus en plus, l'œuvre d'art reproduite devient reproduction d'une œuvre d'art conçue pour être reproductible. De la plaque photographique, par exemple, on peut tirer un grand nombre d'épreuves ; il serait absurde de demander laquelle est authentique. [...] La reproductibilité technique des films est inhérente à la technique même de leur production. Celle-ci ne permet pas seulement, de la manière la plus immédiate, la diffusion massive des films, elle l'exige."[57] On appréhende alors plus finement la dynamique qui cette fois lie le producteur d'une œuvre à ceux qui en jouissent : "Des calculs ont montré qu'en 1927 l'amortissement d'un grand film exigeait qu'il fût vu par neuf millions de spectateurs. Au début, il est vrai, l'invention du parlant a constitué une régression ; son public a été limité par les frontières linguistiques, à l'époque même où le fascisme insistait sur les intérêts nationaux. Cette régression, vite atténuée par l'usage de la post-synchronisation, doit moins nous retenir que le rapport avec le fascisme. Les deux phénomènes sont simultanés car ils sont liés à la crise économique. Les mêmes perturbations qui, à l'échelle générale, ont conduit à chercher les moyens de sauvegarder les rapports de propriété par la force, ont amené le capital investi dans le cinéma, menacé par la crise, à hâter la mise au point du parlant."[58] Le tatouage numérique, dans sa composante orwellienne fantasmée, s'inscrit précisément dans la collection des "moyens de sauvegarder les rapports de propriété par la force." Naïvement, le tatouage aurait donc eu pour objet, au début, d'insuffler de l'aura à une œuvre numérique, de garantir son authenticité (au sens de Benjamin) et par là sa valeur, marchande aujourd'hui.

Pourtant, Benjamin nous avait mis en garde : "dès lors que le critère d'authenticité n'est plus applicable à la production artistique, toute la fonction de l'art se trouve bouleversée. Au lieu de reposer sur le rituel, elle se fonde désormais sur une autre pratique : la poli-

[53]Une copie faite au XVIème d'une œuvre originale datant de l'Antiquité, est *aujourd'hui* considérée comme authentique.

[54]W. Benjamin, *L'œuvre d'art à l'époque de sa reproductibilité technique*, Allia, 2003, trad. M. de Gandillac.

[55]W. Benjamin, *op. cit.*, II, p. 13.

[56]W. Benjamin, *op. cit.*, II, p. 16.

[57]W. Benjamin, *op. cit.*, IV, p. 24.

[58]W. Benjamin, *op. cit.*, IV, p. 25.

tique."[59] Le tatouage, en tant qu'il est censé participer du processus de reproductibilité et de distribution des œuvres numériques, doit donc avant tout être compris dans sa dimension politique pratique, *en rapport* avec l'idée fondamentale de reproduction en série qui est un bouleversement récent. En suivant Benjamin, il faut éviter le contrens selon lequel c'est le caractère *numérique* des œuvres à protéger qui aurait impulsé l'effort autour du tatouage numérique. C'est bien plutôt que les machines devaient enfin pouvoir rendre son utilisation *automatique*, voire *systématique* (le climat politique des années 1930 influencerait donc d'une certaine manière encore notre conception de la protection des droits[60], mais en démocratie sociale ce sont les pratiques qui tempèrent les lois et non l'inverse, et le législateur manque encore de recul sur l'étendue et la nature des pratiques réelles en la matière).

En effet, les cahiers des charges en tatouage pour la protection des droits stipulent tous une robustesse face à la conversion numérique/analogique/numérique - on n'a jamais vraiment souligné les implications d'une telle extension *de facto* au monde analogique, trahissant la chronologie réelle : ce sont les progrès en traitement du signal et des images qui ont permis l'actualisation d'une idée rendue nécessaire, en son temps, par la seule reproductibilité technique de l'œuvre d'art. Les problèmes de *distribution* liés à Internet sont en cela un épiphénomène, certes aggravant. Le défi politique porté par le tatouage robuste est donc en réalité l'ultime tentative d'affirmation *systématique* des rapports de propriété dans le domaine des œuvres, problématique datant très exactement selon Benjamin de la photographie et de la reproduction en série en général. Contrairement à la cryptographie, les techniques de tatouage sont utilisées en vue d'annexer même les œuvres de l'ancien monde purement analogique, *parce que* leur mode de reproduction technique (et de transmission) est aujourd'hui essentiellement numérique. En dernier lieu, le tatouage numérique pour la protection des droits doit se comprendre *en réponse* au développement technique de la reproduction en série des œuvres, et donc aussi comme son complément historique dans un monde devenu numérique entre-temps. Ce qui est en jeu est donc la proximité économique entre un artiste et son public : s'il devient de moins en moins possible de distribuer de manière rentable un artiste dans le monde entier, il se produira mécaniquement une restriction du public jusqu'à des échelles jamais connues. Une caméra DV et un PC standards permettent même de rêver d'un cinéma entre *happy few*... pour des projections forcément moins fréquentes et plus variées, recréant les conditions d'un nouveau rapport à l'art. Simplement parce que la renommée deviendrait plus locale, on rendrait à nouveau possible les légendes : ce que seulement quelques-uns ont vu. Stratégiquement, il eut sans doute été plus judicieux de la part des majors de tenter de maintenir inabordable pour un particulier le niveau d'équipe-

[59] W. Benjamin, *op. cit.*, IV, p. 26. Et comme le rappelle Benjamin en terminant son étude, on ne sait que trop par quels autres funestes moyens la politique peut se continuer...

[60] Par le même jeu d'analogie, Sade le premier, qui a passé la moitié de sa vie *au secret*, rapprochait *logique* de *cruel*... Pour Sade, la logique *est* cruelle - et c'est bien là l'aspect le plus angoissant et précurseur de son œuvre, pour qui prend la peine de passer outre son prime abord logorrhéïque. Il faut encore ajouter que la littérature contemporaine de Sade comportait un courant dit réglementariste (par exemple, Rétif de la Bretonne, l'adversaire farouche de Sade, prenait dans son *Pornographe* le prétexte d'une correspondance entre deux amis pour discuter un règlement des maisons closes). Sur ce sujet, voir G. Bataille, *La littérature et le mal*, Sade, Gallimard, 1957. Voir encore le film de Pier Paolo Pasolini, *Salò ou les 120 journées de Sodome*, qui met en scène le calvaire de 18 jeunes gens sous la contrainte d'un règlement sadique, brimés par des notables de la république fantoche que Mussolini avait proclamée à Salò, en Lombardie, de septembre 1943 à avril 1945.

ment technologique nécessaire à la *création* des contenus. Mais, comme Sony et Philips le démontrent (toutes deux produisent des artistes et vendent des graveurs de CD), personne n'a encore vraiment choisi.

Prenant le contrepied de ces considérations, il faut aussi s'intéresser aux autres applications du tatouage, non moins chargées politiquement, que son aptitude, réelle ou pas, à assurer la conservation des rapports de propriété. Par exemple, garantir l'intégrité d'un média numérique peut s'avérer de la plus haute utilité[61]. De même, le tatouage peut encore servir à augmenter l'accès à l'information par les déficients, trop facilement assimilés à des poids morts depuis le XVIème siècle[62]. Nous allons à présent nous attarder sur le tatouage numérique, et détailler ses variantes mises chacune en regard de leur cadre applicatif respectif.

1.3 Techniques numériques et cadres applicatifs

Nous détaillons à présent les principaux cadres applicatifs dans lesquels les techniques d'écriture secrète jouent un rôle prépondérant. Partant de la stéganographie pure et de ses relations avec la cryptographie, nous abordons les deux types de tatouage : fragile et robuste. Pour commencer, nous donnons une classification de ces techniques sur la Fig. 1.2. Nous n'aborderons pas davantage les spécificités des techniques cryptographiques outre me-

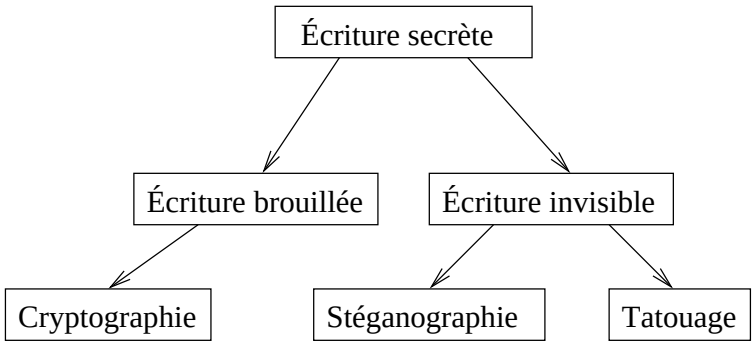

Fig. 1.2 – Classification des différentes techniques d'écriture secrète.

sure. Il faut cependant distinguer les deux formes possibles de chiffrage : privé et public. Le chiffrage privé, ou symétrique, nécessite la même clef pour brouiller les données que pour les déchiffrer. A l'inverse, la cryptographie publique, ou asymétrique, nécessite seulement que les clefs de chiffrage et de déchiffrage vérifient une certaine relation. L'exemple le plus utilisé de cryptographie asymétrique est l'algorithme RSA, du nom de ses trois co-inventeurs (Rivest, Shamir et Adelman). En pratique, les opérations de cryptographie publique nécessitent

[61] On ne connait que trop la tendance des autocrates, Staline en tête, à effacer des photos officielles les personnalités gênantes. Lorsque Benjamin souligne le déplacement du rapport à l'art vers la politique, il pensait au cinéma de propagande soviétique, au culte de la personnalité démultiplié par les reproductions en série, etc.

[62] Dans son *Histoire de la Folie à l'âge classique*, Gallimard, 1972, Foucault montre que les sourds et muets avaient été un peu trop rapidement considérés comme fous, et enfermés (selon le fameux axiome qui veut qu'un néant de langage implique un néant de pensée). Depuis, leur alphabétisation a été rendue possible par d'autres techniques - mais leur accès égal à l'information n'est toujours pas garanti.

beaucoup plus de calculs que leurs équivalents symétriques, d'où leur limitation au chiffrage de la clef de déchiffrage d'un algorithme symétrique uniquement (par exemple dans Pretty Good Privacy, de Philip Zimmermann).

Nous nous devions de rappeler cette différence car le tatouage nécessite lui aussi l'utilisation de clefs, et le plus souvent ces algorithmes sont symétriques, même si Teddy Furon [30] a proposé une méthode de tatouage asymétrique (le mot asymétrique ne peut pas être entendu strictement de la même manière ici que dans le cas de la cryptographie, pour des raisons que nous ne détaillerons pas).

1.3.1 Stéganographie et contenus augmentés

La stéganographie peut avoir d'autres applications que la communication secrète, nous renvoyons à l'introduction pour cet aspect. Parmi ces autres applications, nous souhaitons mentionner l'augmentation de contenus. Par augmentation de contenu, on entend l'ajout d'information cachée dans un média afin qu'un utilisateur équipé du décodeur approprié puisse exploiter des fonctionnalités supplémentaires. Les deux exemples que nous citons concernent la mise à disposition des sourds et malentendants d'un terminal spécial, et la transition douce entre le monde des récepteurs analogiques et numériques. Bien entendu, les applications de communication secrète restent le principal motif de développement de telles techniques.

Les contraintes pesant sur les systèmes de cryptographie sont au nombre de deux :
- la modification du média doit être imperceptible ;
- la capacité du canal stéganographique doit être élevée.

Aide aux sourds et malentendants

Aujourd'hui, l'accès des sourds et malentendants à la télévision est limité par le faible nombre de programmes sous-titrés, ou utilisant le télétexte. Une solution proposée consiste à enfouir dans le signal vidéo l'information nécessaire à l'animation d'un clône tridimensionnel synthétique qu'un décodeur ad hoc viendrait superposer à l'image reçue dans un coin de l'écran. L'avantage de ce système est de ne requérir aucun changement de matériel chez les utilisateurs (ils gardent leur télévision), et ceux qui en ont besoin s'équipent du décodeur capable de séparer l'information cachée du signal vidéo, et d'animer le clône 3D. C'est l'objet du projet Artus[63].

Transition tout-analogique vers tout-numérique

En télévision, le passage du tout-analogique vers le tout-numérique est prévu à l'horizon 2010 pour la France. Cependant, la technologie des récepteurs est fondamentalement différente. Or, on ne peut décemment envisager une transition brutale pour les utilisateurs, qui devraient pouvoir pour certains continuer à recevoir leurs programmes analogiques, alors que les premiers équipés demanderont à profiter immédiatement des avantages du numérique. Pour cela, on utilise le fait que la compression du flux numérique autorise de faire passer davantage de données qu'avec une transmission analogique, sur la même bande passante.

[63] http ://www.telecom.gouv.fr/rnrt/projets/res_01_37.htm

L'idée consiste à récupérer une partie du spectre des transmissions analogiques pour y placer l'information numérique souhaitée. De cette manière, on peut opérer en douceur la transition entre les deux modes de communication. Plusieurs canaux numériques peuvent ainsi être véhiculés dans le spectre d'un seul canal analogique [63]. Cela peut se faire en utilisant l'idée de Costa [18].

Communication secrète

On dénombre environ une vingtaine de logiciels spécialement dédiés aux communications secrètes[64] qui utilisent la stéganographie. La plupart des médias ont été mis à contribution : le texte[65], le son (WAV[66], MP3[67]), l'image (essentiellement les formats non compressés[68], mais aussi JPEG[69]). Toutefois, il existe quelques logiciels qui cachent l'information dans les parties du fichiers de média réservées d'ordinaire aux commentaires[70]. Dans ce cas, la taille du fichier média augmente en fonction de ce que l'on y cache, et cela peut attirer la suspicion. Le principal avantage devant rester de ne pas attirer l'attention sur le fichier échangé, ces méthodes doivent être proscrites ou réservées à de petits fichiers à cacher. Pour donner une idée de la capacité du canal stéganographique dans une image non compressée, il faut savoir qu'il est possible d'utiliser, avec la modification des LSB (Least Significant Bits), les quatre derniers plans de bits (en utilisant de la diffusion d'erreur pour atténuer les désagréments visuels). Ainsi, une image bitmap en niveaux de gris peut être divisée en deux parties : les quatre plans de bits les plus importants véhiculent l'information visuelle de l'image, tandis que les quatre derniers peuvent être entièrement dévolus au codage d'un fichier caché, moyennant l'emploi de techniques de diffusion d'erreur afin d'adoucir l'aspect visuel obtenu.

La principale contrainte pesant sur ces systèmes est celle de l'imperceptibilité, tant perceptuelle que statistique - tout en cherchant à maximiser la capacité du canal caché.

1.3.2 Tatouage fragile, authentification et intégrité

L'authentification a pour but de procurer une information sur une modification éventuelle d'un média. Une manière d'y parvenir est d'insérer dans le média un tatouage fragile. Un tatouage fragile a pour objet de disparaître à la moindre modification. Ainsi, s'attendant à retrouver une marque fragile, on pourra décider de l'authenticité du média considéré. Si la marque fragile a disparu, on n'accordera plus aucune confiance au média, et on évitera de l'utiliser.

Si l'on désire obtenir davantage d'information sur les modifications éventuelles subies par le média, on aborde le problème de l'intégrité. Dans ce cas, la marque à cacher de manière fragile sera constituée d'information grossière sur le média lui-même. Il devient ainsi possible de détecter l'endroit et la nature des changements opérés sur le média.

[64] http ://www.cl.cam.ac.uk/ fapp2/steganography/stego_soft.html
[65] http ://www.ctgi.net/nicetext
[66] ftp ://idea.sec.dsi.unimi.it/pub/security/crypt/codes/s-tools4.zip
[67] http ://www.cl.cam.ac.uk/ fapp2/steganography/mp3stego/index.html
[68] http ://www.outguess.org
[69] ftp ://ftp.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz
[70] http ://camouflage.unfiction.com/

Les contraintes pesant sur ce genre de système sont :
– la modification du média doit être imperceptible ;
– la capacité du canal caché est faible (authenticité) ou moyenne (intégrité) ;
– la robustesse de la marque doit être faible.

1.3.3 Tatouage robuste et protection des documents

Il s'agit ici de ce qui représentait l'espoir le plus important au milieu des années 1990 lorsque naissait le tatouage. Par protection des documents, nous entendons d'une part protection de la copie, et d'autre part protection du droit d'auteur. Ces deux applications ont en commun de devoir mettre en œuvre une marque très résistante à différentes manipulations.

La protection de la copie se propose d'inscrire dans le média les modes d'accès autorisés au média : lecture (une fois), lecture (nombre indéfini de fois), copie (une seule fois, à des fins de sauvegarde), ou copies multiples. Ce genre de système est utilisé dans le système de protection du DVD Millenium. Le contenu d'un DVD est d'abord tatoué, puis crypté. Lorsqu'un contrevenant cherche à décrypter le contenu du DVD, il reste le tatouage. Ainsi, un lecteur commercial standard est prévu pour ne pouvoir jouer que deux types de contenus : les DVD cryptés et tatoués, ou alors les DVD ni cryptés ni tatoués. Si on cherche à jouer un DVD décrypté dans un lecteur standard, la lecture sera refusée car pour le lecteur, le contenu est probablement piraté. En outre, lorsqu'un utilisateur réalise son propre DVD, il ne cherchera vraisemblablement pas à protéger son contenu (ou tout au moins, pas avec la même technologie de tatouage). Ce système permet de jouer les DVD du monde commercial, et ceux réalisés par l'utilisateur lui-même. Du point de vue du tatouage, un tel système requiert une capacité très faible du canal de tatouage, deux ou trois bits suffisent.

Dans le cadre de la protection du droit d'auteur, on cherche à inscrire dans le média un identifiant relatif à l'ayant-droit de l'œuvre. Généralement, cet identifiant mesure 64 bits. Naturellement, l'inscription de la marque doit être très robuste. Plus précisément, on souhaite que la marque disparaisse seulement dans le cas d'attaques tellement sévères sur le média qu'elles en empêchent toute utilisation commerciale du fait de la perte de qualité due à ces attaques. L'identifiant est ensuite stocké chez une tierce partie de confiance qui fait le lien entre l'identifiant et le nom de l'ayant-droit. A ce jour, aucune jurisprudence sur le sujet n'est disponible.

Ces deux applications requièrent quant à elles de satisfaire aux contraintes suivantes :
– la modification du média doit être imperceptible ;
– la capacité du canal de tatouage varie de faible (protection de la copie) à moyenne (protection du droit d'auteur) ;
– la marque doit être très robuste.

En général, on cherchera à pouvoir insérer deux tatouages dans un média : l'un robuste et l'autre fragile. Ainsi, on arrive à protéger à la fois le contenu et les droits.

1.4 Le tatouage et son environnement

1.4.1 Vocabulaire

Après avoir donné une liste des applications dans lesquelles les techniques de tatouage ou de stéganographie sont centrales, il convient de préciser le lexique que nous utiliserons par la suite, relativement aux notions de tatouage. Nous détaillons à présent les principaux termes utilisés :

- Média : le contenu pouvant subir une modification de nature à enfouir de l'information cachée à l'intérieur ;
- Signature, marque : ce que l'on cache dans le cadre du tatouage, fragile comme robuste ;
- Marquage, tatouage, filigranage, incrustation, insertion, enfouissement : les opérations agissant sur l'information en vue de la cacher ;
- Attaque : du point de vue de la marque, n'importe quelle manipulation sur le média. On distingue les attaques autorisées des attaques malveillantes (destinées à attaquer spécifiquement la marque) ;
- Extraction, relecture : l'opération visant à récupérer la marque ;
- Capacité : le nombre de bits d'information cachée que l'on peut inscrire à l'aide d'un schéma particulier de tatouage ;
- Robustesse : ensemble des attaques auxquelles résiste tel schéma particulier de tatouage ;
- Resynchronisation : procédé visant à s'affranchir des attaques modifiant le positionnement absolu du tatouage.
- Clef : le paramètre secret sur lequel repose la possibilité de relecture ;
- Tatouage additif (linéaire) : le message à cacher est transformé en un signal que l'on ajoute de manière additive au média ;
- Tatouage substitutif (non linéaire) : consiste à isoler une caractéristique du média et à la forcer à l'état désiré pour chaque bit à cacher ;
- Tatouage aveugle : le média original n'est pas nécessaire à l'étape d'extraction ;
- Tatouage supervisé : le média original est nécessaire à l'étape d'extraction, principalement à des fins de resynchronisation ;
- Espace de tatouage : espace dans lequel a lieu l'incrustation.

1.4.2 Le tatouage comme problème de télécommunication

Parmi d'autres points de vue possibles, le tatouage a pu être formulé comme un problème de communication classique : le canal de communication est le média, et le message à transmettre est la marque. Les pertes sur le canal modélisent les attaques. Nous récapitulons cette modélisation sur la figure suivante :

Notre travail s'inscrit clairement dans cette approche. Ainsi, nous nous fixerons comme objectif d'optimiser la capacité du canal caché sous contraintes de quelques attaques autorisées, considérées comme non intentionnelles.

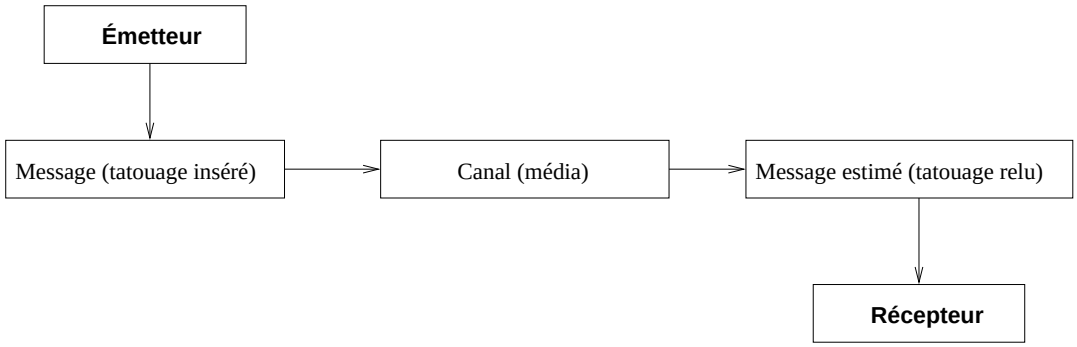

FIG. 1.3 – Modélisation du tatouage comme un problème de communication : le canal de communication est le média dans lequel on cherche à retrouver le message inséré à l'aide de la clef secrète.

1.4.3 Typologie des attaques

Il convient également de présenter une typologie des différentes manières d'attaquer la marque. Le but ici n'est pas de donner une liste d'attaques pour tel média, mais plutôt de classer les attaques en fonction de l'aspect du processus de tatouage qui est mis en déroute.

- Attaques géométriques : on classe dans cette catégorie les modifications du support sur lequel vit le signal de tatouage. Par exemple, dans le cas de l'image, une rotation, une déformation de tapis[71], etc. Le principal écueil à craindre ici est une désynchronisation du signal de tatouage entre l'incrustation et l'extraction : la marque est toujours présente mais le décodeur ne sait plus où la chercher,
- Attaques sur le signal de tatouage : ce sont les manipulations s'apparentant à un filtrage. On range dans cette catégorie les différents filtrages connus : lissage, réhaussement de contraste, ainsi que la compression avec perte, etc. Ici c'est la puissance du signal de tatouage qui risque de devenir trop faible pour que l'extraction s'opère correctement (l'attaque consistant à effacer un signal de resynchronisation est donc à ranger dans cette catégorie) : c'est typiquement le mode d'action d'une *averaging attack*[72],
- Attaques de protocole : ces attaques opèrent à un niveau d'abstraction supérieur. On cherche ici à induire en erreur le processus d'extraction par différentes manières, dont les plus courantes consistent à insérer plusieurs signaux de tatouage au lieu d'un seul comme s'y attendrait le module d'extraction (par exemple, la *copy attack*[73] ou le surmarquage[74]). On peut également faire en sorte de créer un nouveau média en moyennant plusieurs versions tatouées du même média (*averaging attack*)

Précisons d'emblée qu'aucune méthode de tatouage pour aucun média ne propose une robustesse suffisamment élevée face à ces trois types d'attaques. C'est la raison pour laquelle il convient en premier lieu d'identifer clairement les attaques qu'aura à subir la marque. Le

[71] La déformation de tapis consiste en de petites déformations locales de la grille d'échantillonnage.
[72] Estimer le signal de tatouage, puis le "soustraire" le mieux possible du médium.
[73] Recopier un signal de tatouage associé à un médium sur un autre médium.
[74] Introduire plusieurs tatouages sur un médium déjà tatoué, suivant la même technique.

tatouage reste un art auquel la science prête ses moyens.

1.4.4 Sociologie économique de la piraterie

Au jeu du chat et de la souris, il n'est jamais inutile de bien cerner l'adversaire et ses motivations. Nous présentons ici une brève typologie des pirates et de leurs moyens, présentée sous un angle économique. Nous tirons ce formalisme de [65]. On se propose de donner un modèle simple de l'économie de la piraterie face à l'industrie de loisirs. Pour cela, il faut considérer que le coût des biens piratés est une fonction du coût de la création de la première copie pirate, noté e, et du coût de la distribution de chaque copie pirate, noté d. Ainsi, il en coûtera $d + \frac{e}{n}$ de créer et distribuer chacune des n copies pirates d'un contenu. Aujourd'hui seul vraiment subsiste le problème du coût e de création de la première copie pirate (il ne coûte rien, en regard de e, de distribuer une version pirate sur un réseau *peer-to-peer* ou d'utiliser un réseau de redistribution maintes fois amorti ; d peut donc être quasi-nul). Ici, la qualité de la copie est fonction des moyens financiers : on trouve sur eMule des copies de films acquis dans la salle de projection elle-même (le bon sens réclame donc de rémunérer correctement le projectioniste pour plus de sécurité), mais le même jour circule déjà en Asie un DVD du même film, de qualité optimale, car le pirate aura eu accès à la matrice de duplication. Il faut donc classer les pirates selon leurs moyens, évaluer les risques qu'ils représentent, et établir une politique de sécurité en conséquence. Nous appelons artisan, industriel et État les trois types de pirates potentiels, suggérant ainsi une gradation dans la quantité et la qualité de leurs moyens, et aussi des besoins différents. Par pirate, nous entendons quelqu'un qui recherche un accès frauduleux à une information, supposée protégée par un système de sécurité (cryptographie et/ou stéganographie). Le motif du piratage tient successivement du défi (pour l'artisan), de l'enjeu économique (pour l'industriel), voire de la surveillance des individus (pour l'État). Les mafias sont un cas à part qui relève à la fois de l'industriel et de l'État (elles peuvent se servir de la piraterie pour subvenir à la fois à des besoins économiques et de surveillance). Bien entendu, chacun de nos trois personnages conceptuels (artisan, industriel, État) peut éventuellement découvrir (voire organiser) une faille dans le système de sécurité, se réservant pour lui seul la possibilité d'un coût e faible. Mais seul un artisan pourra avoir la naïveté d'en faire part au reste du monde. C'est en ce sens que l'artisan est le principal garant des systèmes de sécurité actuels.

L'artisan

L'artisan, même s'il peut utiliser un réseau *peer-to-peer* pour transmettre efficacement les contenus pirates qu'il a créés, ne peut jamais consacrer que de faibles moyens à la création de sa première copie pirate. Ainsi, son investissement sur e est-il très faible, de l'ordre de quelques dizaines de milliers d'euros au maximum (quelques gros PC et du matériel électronique). L'histoire économique de l'industrie de loisirs se borne à imposer un coût e moyen dépassant les possibilités d'un artisan. Cela peut être un simple particulier comme une personne connaissant les détails du problème. Il arrive qu'une personne seule casse un système dont on croyait que cela était au-dessus de ses moyens : c'est le cas de Serge Humpich qui, profitant d'une faille d'implantation mathématique de l'algorithme de cryptage de la carte à puce, a menacé la sécurité, et donc l'existence, du système bancaire pour particuliers. Une

tentative réussie de piraterie s'appelle, pour l'artisan, un *exploit* - et il est de bon ton de se prévaloir de ses exploits sur un forum. L'artisan cherche à relever un défi pour des raisons esthétiques, voire politiques : il représente le piratage romantique. Toutefois, il peut arriver qu'il travaille ensuite, par désillusion ou vénalité, pour un industriel ou un État.

L'industriel

L'industriel est appelé ainsi en raison de sa capacité déjà conséquente de création et de distribution propre des copies pirates. Il peut s'agir d'une branche d'une organisation criminelle, comme d'une multinationale recherchant des informations sur un concurrent. Un coût e de plusieurs dizaines de millions d'euros leur est parfaitement envisageable. D'autant que pour eux, n n'est jamais très grand non plus (au besoin). L'industrie de loisirs cherche à ce qu'un industriel du piratage mette plusieurs mois à forcer le système de sécurité, environ le temps qu'un contenu ait été rentabilisé par les producteurs du contenu. Toutefois, les industriels de la piraterie multimédia trouvent souvent plus efficace en première approche d'infiltrer un agent ayant accès au contenu original. C'est généralement un industriel qui corrompt les projectionistes des salles de cinéma.

L'État

L'État, en tant que personnage conceptuel, désigne ici une entité ayant un besoin spécifique de *surveillance* des individus qui le composent. Un État considère que la connaissance d'informations sur ses individus est un gage de sa survie. Les moyens qu'il peut consacrer à cet objectif sont sans équivalent : il dispose de moyens tant matériels que financiers ou humains. Un État n'a pas nécessairement besoin de distribuer des copies pirates (à moins de considérer une mafia, qui dispose en général déjà de son propre réseau de distribution), forcer le système de sécurité lui suffit : il peut concentrer tous ses efforts dessus.

1.5 Conclusion

L'écriture secrète sur les médias numériques est un défi qui mobilise les compétences de milliers de personnes dans le monde, vers des objectifs très divers. On peut, comme nous l'avons fait, choisir de modéliser ce problème par une approche télécommunications : le canal de transmission est le contenu sur lequel on écrit le message à transmettre. Le bruit sur le canal de transmission correspond aux attaques, intentionnelles ou non, subies par la marque qui est la représentation physique du message à transmettre. Par attaque, on entend n'importe quelle manipulation appliquée au média. Les développeurs de méthodes de tatouage cherchent à proposer des solutions dont le niveau de sécurité dissuade un artisan ou un industriel du piratage.