Préface de Gildas Avoine

Gildas AVOINE
Directeur du GdR Sécurité informatique,
IRISA, Université de Rennes, CNRS, Inria, INSA Rennes, Rennes, France

La recherche académique et industrielle française en cybersécurité se place au tout premier plan sur la scène internationale. Si la France ne peut prétendre posséder une souveraineté technologique dans ce domaine, elle possède indéniablement une souveraineté des compétences, tant l'expertise française couvre l'intégralité des domaines de la cybersécurité.

La recherche en cryptographie illustre l'excellence française mais elle ne doit pas éclipser d'autres domaines où l'influence française est tout aussi remarquable, parmi lesquels les méthodes formelles pour la sécurité, la protection de la vie privée, la sécurité des systèmes, des logiciels et des réseaux, la sécurité des systèmes matériels, et la sécurité des données multimédia, selon la classification proposée par le Groupement de recherche (GdR) Sécurité informatique du CNRS.

C'est justement la sécurité des données multimédia qui est admirablement couverte dans cet ouvrage. L'évolution de notre société de l'écrit vers le son et l'image avec notamment l'avènement du téléphone portable et la démocratisation d'Internet a fait apparaître de nouveaux besoins en termes de sécurité. Il ne s'agit ici que des prémices de la transformation de notre société, et le déploiement récent de la visio conférence démontre que la recherche en sécurité des données multimédia est perpétuellement confrontée à de nouveaux défis scientifiques.

La complexité du sujet et sa dimension multidisciplinaire, qui allie en premier lieu le traitement du signal et la cryptographie, sont parfaitement illustrées par la variété

Sécurité multimédia 2,
coordonné par William PUECH. © ISTE Editions 2021.

des sujets détaillés au fil des pages. Les chapitres dévoilent ainsi à tour de rôle les verrous scientifiques à traiter par la communauté, en les ancrant sur des scénarios réels, comme la copie frauduleuse de films, la tromperie d'une intelligence artificielle ou la diffusion d'images trafiquées sur les réseaux sociaux.

Cet ouvrage composé de deux volumes est ainsi promis à devenir une référence francophone du domaine de la sécurité des données multimédia, une initiation à la fois exhaustive et approfondie que les étudiants, ingénieurs et chercheurs pourront apprécier à travers ces plus de 600 pages enrichies de nombreuses références. Lecture linéaire ou lecture errante, chacun pourra s'adonner à sa pratique préférée.

J'aimerais enfin remercier l'ensemble des auteurs pour leur engagement à faire vivre la communauté scientifique francophone, et je remercie en particulier William Puech pour l'édition de cet ouvrage. William qui, aux côtés de Patrick Bas puis de Caroline Fontaine, porte la thématique de la sécurité des données multimédia au sein du GdR Sécurité informatique, permettant ainsi à l'ensemble de la communauté de la cybersécurité de mieux appréhender ce sujet passionnant.

Bonne lecture.

Préface de Cédric Richard

Cédric RICHARD
Directeur du GdR ISIS, OCA, Université Côte d'Azur, CNRS, Nice, France

Avec l'augmentation sans relâche de la bande passante et des espaces de stockage, ainsi que la prolifération des appareils mobiles et le développement de nouveaux standards, les données multimédia marquent profondément nos sociétés en modifiant l'accès à l'information et le rapport à la culture, en transformant les interactions entre individus et leurs rapports avec les organisations. Les activités multimédia sont omniprésentes dans tous les grands secteurs d'activité (sécurité, santé, télécommunications, etc.), et ont accompagné leurs évolutions successives grâce au fil conducteur qu'elles tissent, du support de l'information jusqu'à l'application et à l'usager.

Dans ce contexte, sécuriser les données multimédia par la protection de la confidentialité, la protection des droits d'auteur, la vérification de l'intégrité, l'analyse et l'authentification des contenus, le traçage des copies et le contrôle d'accès, pose des questions particulièrement critiques. Par exemple, les stratégies de protection mises en œuvre doivent tenir compte des besoins spécifiques au multimédia tout en répondant aux exigences des moyens de communication, et établir ainsi un compromis. Une mauvaise approche peut en effet entraîner un codage excessif des données, ou altérer leur qualité perceptive, et échouer ainsi dans les objectifs de sécurité visés.

Discipline d'interface par nature, que l'art de la sécurité multimédia est difficile !

Pourtant, par cet opus en deux volets, William Puech et ses co-auteurs relèvent le défi avec brio en brossant un panorama exhaustif et actuel de la sécurité multimédia. Ainsi proposent-ils une analyse approfondie des méthodes d'authentification et d'insertion de données cachées, des technologies biométriques, et des procédés de protection et de chiffrement multimédia. Sans céder à un formalisme suranné qui pourrait

Sécurité multimédia 2,
coordonné par William PUECH. © ISTE Editions 2021.

nuire à la fluidité de leurs exposés, les auteurs captivent le lecteur en lui présentant sans détour et de façon illustrée l'état de l'art de chaque sujet.

William Puech et les contributeurs à cet ouvrage ont fourni un travail considérable au service de leurs communautés de l'information, du signal, de l'image, de la vision, et de la sécurité informatique, représentés par les deux GdR idoines du CNRS. Je leur exprime toute ma gratitude.

Avant-propos

William PUECH
LIRMM, Université de Montpellier, CNRS, Montpellier, France

De nos jours, plus de 80 % des données transmises sur les réseaux et archivées dans nos ordinateurs, tablettes, téléphones portables ou sur les Clouds sont des données multimédia. Ces données multimédia sont principalement des images (photographies, images de synthèse), des vidéos (films, animations) ou du son (musiques, podcasts), mais également de plus en plus des données 3D et des scènes 3D, pour des applications allant du jeu vidéo aux données médicales, en passant par la conception assistée par ordinateur, la vidéo surveillance et la biométrie. Il devient nécessaire, urgent, pour ne pas dire vital, de sécuriser ces données multimédia, que ce soit pendant leur transmission, leur archivage, mais également pendant leur visualisation. En effet, avec le tout numérique, il devient de plus en plus facile de copier ces données multimédia, de les visualiser sans droit, de se les approprier, mais aussi de les falsifier.

Depuis 30 ans, nous constatons un bouillonnant développement autour de la sécurité multimédia, que ce soit au niveau international comme au niveau national. En effet, au niveau national, plusieurs dizaines d'équipes de recherche dans des laboratoires, mais aussi un grand nombre d'industriels, focalisent leurs activités sur ces aspects. Cette activité se retrouve également au niveau de plusieurs GdR (Groupements de recherche) du CNRS, mais en particulier le GdR ISIS (Information, signal, image et vision) et le GdR Sécurité informatique.

La sécurité multimédia est une thématique relativement jeune, comme l'attestent les dates de publication des articles cités en référence dans les différents chapitres de ces deux volumes. En effet, sur plus de 900 références, près de 50 % d'entre elles ont moins de 10 ans et plus de 35 % ont entre 10 et 20 ans. Bien évidemment, n'oublions

Sécurité multimédia 2,
coordonné par William PUECH. © ISTE Editions 2021.

pas certains auteurs, comme par exemple Auguste Kerckhoffs (1835-1903) et Claude Shannon (1916-2001), sans qui notre communauté n'aurait pas avancé de la même manière. L'histoire de la sécurité multimédia commence vraiment à la fin des années 1990 par le début du tatouage, de la stéganographie mais de manière très timide, cela étant motivé par la numérisation des contenus et la protection des ayants droit. En 2001, motivées par les attentats du 11 septembre, les recherches en stéganalyse, détection de signaux cachés et détection statistique, prennent une grande importance. Durant la décennie 2000-2010, au niveau national et international, c'est l'explosion de la sécurité en tatouage. Il apparaît également des contributions majeures en stéganographie et stéganalyse. Durant cette même décennie, la recherche en sécurisation des données multimédia par chiffrement spécifique voit le jour avec les aspects chiffrement sélectif ou partiel, crypto-compression tout en garantissant la préservation des formats et des normes internationales. À partir de 2010, des nouvelles facettes de la sécurité des données multimédia voient le jour avec les aspects *forensics*/criminalistiques ainsi que les approches statistiques. Se développent également très fortement à partir de 2010 le traitement du signal dans le domaine chiffré ainsi que le traçage de traîtres. En 2020, les recherches en *forensics*/criminalistiques et en stéganalyse montent en force, en particulier avec l'apparition de l'apprentissage automatique et surtout avec l'exploitation et le développement de réseaux de neurones convolutifs profonds. Les avancées récentes sont très variées dans cette thématique, de la stéganographie (GAN), méthodes adversarielles, méthodes par génération de contenus, au traitement de contenus chiffrés en passant par les liens entre l'apprentissage et la fuite d'information, les applications en biométrie et l'analyse de contenus « real-life ».

Ce projet d'ouvrages a commencé il y a plus de 2 ans et me tenait vraiment à cœur. En effet, au niveau national nous avons une force certaine dans ce domaine, et de nombreuses pépites que nous nous devions de mettre en lumière. Rien n'aurait pu être réalisé sans le soutien du GdR ISIS et du GdR Sécurité informatique. C'est en grande partie grâce à ces GdR que nous avons réussi à cartographier d'un point de vue national les activités de recherche dans le domaine de la sécurité multimédia. Les villes représentées dans ces deux ouvrages illustrent la richesse et la diversité nationale (Caen, Grenoble, La Rochelle, Lille, Limoges, Lyon, Montpellier, Paris, Poitiers, Rennes, Saint-Étienne et Troyes), sachant que certaines de ces villes, comme vous pourrez le constater pendant votre lecture, sont représentées par plusieurs laboratoires et/ou universités.

Comme vous allez pouvoir vous en apercevoir tout au long de ces deux volumes, même si elles sont regroupées autour la sécurité multimédia, les thématiques de recherche sont très larges et les applications très variées. De plus, les domaines couvrent un large spectre, du traitement du signal à la cryptographie, en passant par le traitement des images, la théorie de l'information, le codage et la compression. De nombreuses thématiques en sécurité multimédia consistent en un jeu entre le chat et la souris, où le défenseur des droits doit régulièrement se transformer en contre-attaquant afin de résister à l'attaquant.

Le premier volume se concentre principalement autour de l'authentification de données multimédia, des codes et de l'insertion de données cachées, du côté défenseur comme du côté attaquant. Concernant l'insertion de données cachées, il aborde également les aspects invisibilité, couleur, traçage et données 3D, tout comme la détection de message caché dans une image par stéganalyse. Le second volume se concentre principalement autour de la biométrie, de la protection, de l'intégrité et du chiffrement de données multimédia. Il aborde des aspects tels que la crypto-compression d'images et de vidéos, le chiffrement homomorphe, l'insertion de données cachées dans le domaine chiffré ainsi que le partage de secrets. J'invite le lecteur, étudiant, enseignant, chercheur ou industriel à se plonger dans ces ouvrages, pas forcément en suivant l'ordre proposé mais à aller d'un chapitre à un autre, ainsi que d'un volume à un autre.

Ces deux volumes, même s'ils couvrent un très large spectre en sécurité multimédia, n'ont pas la prétention d'être exhaustifs. Je pense, j'espère, qu'un troisième volume viendra compléter ces deux premiers. En effet, je pense au son (musique et parole), à la vidéo surveillance/vidéo protection, à l'authentification des appareils photo, à la protection de la vie privée ainsi qu'aux attaques et contre attaques que nous voyons fleurir tous les jours.

Je tiens à remercier tous les auteurs, responsables de chapitres, leurs co-auteurs, leurs collaborateurs ainsi que leurs équipes, pour tout le travail fourni. Je suis vraiment désolé de les avoir relancés de nombreuses et nombreuses fois afin de trouver parfois les meilleurs compromis entre timing, contenu et longueur des chapitres. Merci à Jean-Michel, Laurent, Philippe ($\times$ 2), Patrick ($\times$ 2), Teddy, Sébastien ($\times$ 2), Christophe, Iuliia, Petra, Vincent, Wassim, Caroline et Pauline ! Merci à vous tous pour votre ouverture d'esprit ainsi que votre bonne humeur ! Je remercie également les GdR ISIS et Sécurité informatique au travers de Gildas et Cédric, mais aussi Christine et Laure pour leurs relectures ainsi que pour avoir fait le lien avec ISTE Editions. Je tiens également à remercier tous les collaborateurs proches avec qui je travaille depuis plus de 25 ans sur les différentes thématiques que j'ai eu la chance d'aborder tout au long de ces années. Doctorants, ingénieurs, stagiaires, collègues, tous se reconnaîtront, que ce soit dans mon équipe de recherche (équipe ICAR) ou dans mon laboratoire de recherche (LIRMM, Université de Montpellier, CNRS). Je remercie en particulier Vincent, Iuliia, Sébastien et Pauline pour avoir accepté de se lancer dans l'aventure afin de rédiger certains chapitres. Pauline, en plus de rédiger certains chapitres, a été une immense collaboratrice pour l'avancement de ces ouvrages. Tous les responsables de chapitres l'ont compris, Pauline a été, pendant ces deux années, dans mon ombre pour que ces deux ouvrages puissent voir le jour en 2021. Merci Pauline ! Pour terminer, je tiens à remercier très chaleureusement tous les membres de ma famille, et en particulier Magali et nos trois enfants, Carla, Loriane et Julian, que j'aime très fort et qui ont la lourde tâche de me supporter au quotidien.