Nouvelle méthode d'évaluation de robustesse des algorithmes de tatouage vidéo : jeu d'attaque

Asma Kerbiche, Saoussen Ben Jabra, Ezzedine Zagrouba, Axel Carlier, Vincent Charvillat

Nouvelle méthode d'évaluation de robustesse des algorithmes de tatouage vidéo: Jeu d'attaque

Asma Kerbiche[1], Saoussen Ben Jabra[1], Ezzeddine Zagrouba [1], Axel Carlier[2,3] et Vincent Charvillat[3]

[1]Université Tunis El Manar
Lab. RIADI - Equipe SIIVA

[2]Université de Toulouse
Lab. IRIT - Equipe Vortex

[3]Université de Singapore

Résumé
L'évaluation d'une technique de tatouage a été toujours une étape critique et importante. En effet, l'évolution progressive des outils de traitement et de communication de vidéos a fait naître de nombreuses et différentes techniques de tatouage dont l'efficacité varie d'un algorithme à un autre. Cette efficacité est toujours évaluée en se basant sur plusieurs contraintes dont les plus importantes sont l'invisibilité et la robustesse face aux attaques. Cette dernière est souvent évaluée en testant des attaques classiques et simples telles que la compression, la rotation, la translation et l'ajout de bruit. Des techniques simples de tatouage peuvent résister à des attaques simples sans pour autant être robustes aux attaques observées dans le monde réel comme le "Camcording" d'un contenu vidéo. En situation réelle, un utilisateur mal intentionné (ou un pirate) va filmer illégalement un contenu projeté, recadrer l'image, transcoder le contenu obtenu. La question que nous nous posons est l'évaluation de méthodes de tatouage dans ce type de contexte. Dans le cadre de l'élaboration d'un nouveau protocole d'évaluation de techniques de tatouage vidéo, nous proposons, dans ce papier, un jeu d'attaques de vidéos tatouées mis à disposition d'un ensemble d'utilisateurs qui vont interagir afin de détruire la marque qui a été insérée. Ceci sera réalisé en leur fournissant une liste d'attaques qu'ils peuvent librement appliquer et combiner à ces vidéos tatouées. Cette liste va comprendre les attaques les plus importantes et réelles que peut subir une vidéo telles que le camcording, la déformation, l'ajout de couleur et la compression. Ce jeu nous a permis non seulement d'évaluer n'importe quel algorithme de tatouage vidéo, mais surtout, d'identifier, à partir de l'étude de choix des utilisateurs les attaques les plus importantes pour eux.

Résumé
Watermarking techniques evaluation presents a critical and very important step. In fact, with the progressive evolution of video processing and communication, many watermarking approaches are proposed and their efficiency varies from an approach to another one. This efficiency is generally evaluated based on several constraints where the most important are invisibility and robustness in front of attacks. This last one is often estimated by testing classical and simple attacks such as rotation, translation and noise add. Nevertheless, a simple watermarking technique can easily resist to this type of attacks. So, it is necessary to study the impact of other attacks which are always applied in reality such as camcording attack. The integration of these important attacks will allowed a more efficient comparison between the various proposed techniques. In this paper, a new attacking game is proposed. In this game, different marked videos will be at the disposal of a set of users who can interact to destroy the inserted mark. Indeed, a list of different attacks will be given to users who can apply a combination of several of them to the marked videos. This list will contain the most important and dangerous attacks such as camcording, color add compression. This game allowed us to evaluate our video watermarking technique. In more, based on users' choices, we can identify the most important attacks for them.

Mots clé : tatouage, vidéo, crowdsourcing, camcording, attaques, jeu...

Mots clé : Watermarking, video, crowdsourcing, camcording, attacks, game...

1. Introduction

Avec l'avènement de l'ère numérique, l'information est devenue volatile et facilement interceptée et produite. Le

développement des réseaux à haut débit, notamment Internet, et l'évolution des nouvelles normes de décompression ont facilité la transmission et le partage de l'information. En conséquence, il est devenu très aisé de gérer les données volumineuses en termes de stockage et de traitement puisque il est devenu possible maintenant de faire des vidéo conférences en temps réel, d'envoyer par e-mail des fichiers de taille importante, de regarder des films depuis un serveur distant, etc. Les documents numériques sont donc soumis à plusieurs problèmes tels que le piratage et le non-contrôle de la copie qui peuvent provoquer une répercussion économique non négligeable. Il est devenu donc nécessaire pour les créateurs de contenus numériques de rechercher des solutions afin de lutter contrer ces problèmes. Le tatouage, appelé aussi "Watermarking" en anglais, s'avère une technique de sécurisation des données qui permet de remédier à ces problèmes. En effet, il permet d'insérer dans un document numérique une signature non perceptible puis de tenter à la récupérer après d'éventuelles attaques subies par le document tatoué. Nous nous sommes intéressés dans notre travail au tatouage des flux vidéo. Ce type de tatouage est un domaine assez récent qui a rencontré un intérêt croissant au sein de la communauté scientifique. En effet, de multiples méthodes de tatouage vidéo sont apparues et chacune d'elles possède ses avantages et ses inconvénients mais aucune ne parvient encore à s'imposer. En effet, un bon algorithme de tatouage doit obéir à deux principales contraintes : l'invisibilité de la signature insérée et sa robustesse contre les attaques. Cependant, malgré l'évolution des algorithmes de tatouage et des techniques de piratage, la robustesse de chaque algorithme de tatouage est toujours évaluée en testant les mêmes attaques 'usuelles' classiques. En effet, de nos jours on ne retrouve plus d'algorithme de tatouage qui n'est pas robuste face à la rotation ou l'ajout de bruit, cela fait partie des bases d'un bon algorithme de tatouage... Pour autant la résistance à ces attaques "artificielles" n'est pas équivalente à la robustesse face aux pratiques malveillantes observées dans le monde réel. Nous nous intéressons une attaque très répandue appelée « camcording » qui consiste en l'enregistrement des films dans les salles de cinéma à l'aide d'un Smartphone ou d'une caméra et qui peut être suivie de transformations colorimétriques, d'une compression ou d'une déformation ... Ces attaques doivent alors être prises en considération dans le processus d'évaluation des techniques de tatouage vidéo. Afin d'élaborer cette évaluation, nous avons eu recours au crowdsourcing qui permet d'utiliser l'intélligence collective de beaucoup d'utilisateurs. Nous avons conçu un jeu d'attaques o*ù* nous avons fait interagir des utilisateurs qui vont essayer de détruire le tatouage inséré dans la vidéo et ceci en appliquant plusieurs combinaisons d'attaques disponibles, tout en gardant une bonne visibilité de la vidéo attaquée. Cette interaction va nous permettre de savoir quelles sont les attaques les plus intéressantes pour les utilisateurs. La suite de ce papier sera organisée comme suit : dans la section suivante, un état de l'art concernant le tatouage vidéo, les protocoles d'évaluation existants ainsi que la technique du crowdsourcing sera présenté. La deuxième partie sera consacrée à la description du jeu d'attaques proposé tout en exposant la liste d'attaques choisies pour l'évaluation. Les résultats obtenus feront l'objet de la troisième section et nous finirons par une conclusion et certaines perspectives.

2. Evaluation des techniques de tatouage vidéo

Tout algorithme de tatouage doit obéir à certaines contraintes dont les plus importantes à prendre en compte pour l'évaluation sont l'invisibilité, la capacité et la robustesse cette derniére étant la plus critique. En effet, la marque doit être capable de résister à plusieurs types d'attaques. On appelle "attaque" une transformation que l'on va faire subir à l'image et qui va plus ou moins l'endommager mais qui risque d'être fatale au marquage [A.P99]. La robustesse d'un marquage dépend de sa capacité à résister à une attaque. En fait, cette attaque peut avoir deux buts : le premier est d'accentuer ou de masquer certaines caractéristiques de l'image. Le deuxième est de rechercher la marque et la lire, la détruire ou la changer de façon à rendre impossible sa détection [FJB99]. La détection doit alors être possible quelque soit l'attaque appliquée. Pour la vidéo, les attaques les plus utilisées pour les tests de robustesse sont des attaques simples que nous jugeons pas assez réalistes et classiques qui peuvent être aussi classées selon l'intention de leurs utilisations. Dans ce cas, nous distinguons deux grandes familles : les attaques innocentes comme la compression, les transformations géométriques (Translation, rotation, changement d'échelle...), le filtrage ou l'ajout de bruit et les attaques malveillantes telle que la collusion qui consiste essentiellement à moyenner les images successives d'une vidéo dans le but d'éliminer la marque sans nuire à la qualité de la séquence.

Plusieurs protocoles ont été proposés pour les algorithmes de tatouage vidéo, cependant, ils utilisent généralement les mêmes attaques classiques pour l'évaluation de la robustesse. Parmi ces protocoles, nous pouvons citer le projet Européen Certimark [Rol] qui a été lancé en mai 2001 sous la direction de C. Rollin. Ce protocole travaille principalement sur la réalisation de tests génériques pour l'évaluation des méthodes de tatouage d'images et vidéo. Les attaques testées pour les vidéos sont : la compression, la conversion numérique en analogique et analogique en numérique (D/A et A/D), application des formats de stockage de la vidéo avec perte, ajout de logos ou sous-titrage, transformations géométriques (rotation, translation, Cropping, changement d'échelle...), ajout d'autres marques, bruit et collusion. Plusieurs autres protocoles d'évaluation ont été proposés pour les algorithmes de tatouage d'image tel que le projet Stirmark benchmark [Pet00] qui a été lancé en 1998 proposé par Fabien A. P. Petitcolas, le projet « BOWS : Break Our Watermarking System » [BF] qui a été lancé en 2007 qui évaluent la performance d'un algorithme de tatouage en se basant sur plusieurs contraintes (capacité, invisibilité, rapidité, robustesse...) et qui teste la vulnérabilité de ces algorithmes face aux attaques standards certes importantes mais qui ne présentent plus de risque pour les algorithmes de tatouage actuels.

3. La technique du Crowdsourcing

Avec le développement et le grand progrès qu'ont vécus les technologies Web 2.0, de nombreux systèmes so-

ciotechniques ont attiré l'attention des praticiens et des universitaires. Le Crowdsourcing est un nouveau phénomène émergent du Web 2.0 qui est devenu un mécanisme d'approvisionnement reconnu pour résoudre les problèmes des organisations et sociétés par l'externalisation de ces problèmes à une foule. Pour cela, le domaine du Crowdsourcing est devenu un secteur de recherche très dynamique et est en pleine croissance au fil de ces années. Le terme Crowdsourcing a été inventé par Howe, dans un article de Wired Magazine en juin 2006 [J.06] : "Simply defined, crowdsourcing represents the act of a company or institution taking a function once performed by employees and outsourcing it to an undefined (and generally large) network of people in the form of an open call. This can take the form of peer-production (when the job is performed collaboratively), but is also often undertaken by sole individuals. The crucial prerequisite is the use of the open call format and the large network of potential laborers". Le Crowdsourcing est basé sur un simple mais puissant concept : Presque tout le monde a un potentiel pour diffuser des informations précieuses [GF11]. En effet, il s'agit de mobiliser les compétences et l'expertise qui sont réparties dans la foule [C.08]. Le Crowdsourcing n'est pas seulement utilisé pour des fins commerciales. En effet, de nombreuses organisations à but non lucratif l'ont adapté comme un modèle efficace pour la résolution de problèmes [C.10] [J.08]et ca a également attiré l'attention de la communauté universitaire. En effet, plusieurs études récentes sont basées sur la technique du Crowdsourcing. Xie & al. [XLGyM05] ont proposé une nouvelle méthode pour détecter les cartes d'intérêt des utilisateur en se basant sur le crowdsourcing cette méthode à montré une meilleure efficacité que celles basées sur l'analyse d'image, en représentant l'intérêt réel des utilisateurs. Carlier & al. [CCOM10] aussi ont proposé une méthode basée sur le Crowdsourcing qui déduit les régions d'intérêts d'une vidéo en analysant le comportement de visualisation implicite d'un grand nombre d'utilisateurs en utilisant le zoomin. Notre approche méthodologique, dans cet article, consiste dans la même voie à collecter des traces d'utilisateurs à qui nous demandons d'attaquer des vidéos tatouées. Nous motivons ces utilisateurs en leur lançant une forme de défi ludique : "Trouver la meillure attaques qui supprime la marque sans trop altérer la vidéo.

4. Jeu d'attaques proposé

Nous avons ainsi construit un "jeu" d'attaques que nous livrons à une foule d'utilisateurs/joueurs. La conception a été guidée par une attaque réelle appelée Camcording. Le camcording revient à filmer la vidéo affichée ou projetée à l'aide d'un Smartphone ou une caméra et puis à la diffuser après lui avoir appliqué certaines transformations afin de détruire la marque qui a été insérée. En effet, la copie illicite des films est une grande préoccupation de l'industrie cinématographique et le développement technologique au cours de ces dernières années a fait du piratage une menace encore plus grande. L'unité de recherche et développement de la société Kodak s'est rendue compte de l'importance de cette attaque et a conçu un algorithme de tatouage qui a montré ses preuves face au camcording et qui permet aussi d'identifier la salle de cinéma où la projection a eu lieu ainsi que l'heure et la date de diffusion [CMR01]. Philipp Schaber & al. [SKWE14], ont conçu un outil qui simule une ré-acquisition d'un contenu avec un caméscope pour soutenir les recherche comme la notre. Partant de ces travaux, nous avons choisi de concevoir un jeu d'attaques en se basant sur la technique du crowdsourcing. En effet, il s'agit de mettre à la disposition des utilisateurs une interface qui leurs permet d'appliquer à des vidéos tatouées un ensemble d'attaques que nous avons jugées les plus importantes et dangereuses. L'interface proposée est illustrée dans la figure 1, elle comporte trois parties principales : la première contient un aperçu de la vidéo originale, la deuxième contient la liste des attaques choisies et la dernière montre un aperçu de la vidéo tatouée. Chaque utilisateur a droit à trois essais au cours desquels il va tenter de détruire la signature. Il pourra appliquer les combinaisons qu'il désire à condition qu'il ne détériore pas trop la qualité visuelle de l'image attaquée.

En se basant sur des enquêtes faites avec des spécialistes de cinéma, nous avons choisi d'intégrer dans l'interface proposée les attaques suivantes : le camcording, la compression, la déformation, le cropping et la modification de couleur.

4.1. Le camcording

La première étape que peut appliquer un utilisateur en accédant au jeu est de choisir soit une vidéo originale soit celle camcordée. Pour ce faire, nous avons choisi de camcorder la vidéo à partir de 4 prises de vue. Au début nous avons positionné le caméscope en face de l'écran, puis à droite, puis à gauche et pour finir en bas comme le montre la figure 2. Par conséquent, chaque utilisateur peut choisir de travailler sur la vidéo originale ou une de ces quatre versions camcordées.

4.2. La compression

La compression MPEG4 est la norme de compression la plus populaire et la plus utilisée de nos jours. Ce format de compression est parfaitement adapté à la haute définition qu'il diffuse sans prendre trop de place sur le vecteur utilisé (satellite, câble, TNT).Vu l'importance de ce système de compression, tout bon algorithme de marquage doit pouvoir lui résister au moins dans les faibles taux de compression. C'est pour cette raison, que la deuxième étape dans notre jeu d'attaques consiste à permettre aux utilisateurs de choisir de travailler avec la version compressée ou non de la vidéo tatouée. Ils auront alors le choix entre 3 débits de compression (1000 kbit/s, 500 kbit/s et 200 kbit/s). La figure 3 présente la vidéo compressée pour chaque débit.

4.3. La déformation

Après le choix de la compression, les utilisateurs peuvent appliquer, dans le cas des vidéos camcordées, des modifications pour recadrer ces vidéos (figure 4) et ceci en sélectionnant les coordonnées de la région qu'ils veulent rectifier. Une prise de vue latérale en Camcording nécessite en effet un recalage homographique de l'image.

4.4. Le cropping

L'attaque du cropping ou rognage d'une séquence vidéo consiste à en extraire un morceau. Elle permet de couper horizontalement ou verticalement les images de la vidéo. Cette

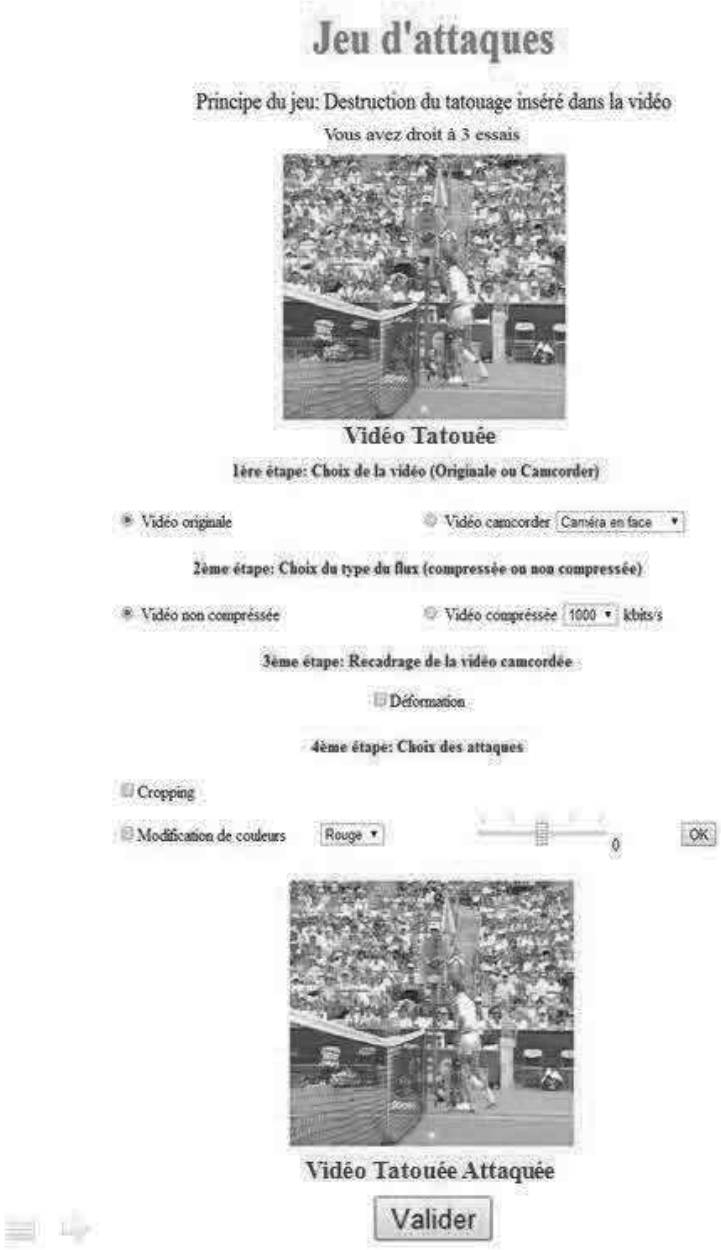

Figure 1: *Interface du jeu d'attaques proposé.*

attaque peut détruire totalement la marque. Dans le jeu d'attaques proposé, les utilisateurs peuvent sélectionner la région de la vidéo qu'ils désirent conserver à condition de garder une bonne visibilité de la vidéo (figure 5).

4.5. L'ajout de couleur

La dernière attaque disponible dans le jeu proposé est l'ajout de couleur qui revient à modifier les couleurs de la vidéo en rajoutant soit du rouge, du vert, ou du bleu aux couleurs initiales des images de la vidéo (figure 6).

5. Résultats expérimentaux

Afin d'étudier et d'analyser les choix des différents utilisateurs participant au jeu proposé ainsi que le comportement du tatouage à tester, nous avons choisi d'évaluer l'algorithme de tatouage basé sur l'insertion multi-fréquentielle dans les régions d'intérêts que nous avons proposé dans nos travaux précédents [KJZ12] et la méthode proposé par Chan & al [CL03] qui propose un algorithme de tatouage vidéo basé sur la transformée en ondelette. Ces deux algorithme on présenté une bonne robustesse en les évaluant face aux attaques usuelles de tatouage vidéo comme la rotation, l'ajout de bruit, al suppression d'images et la compression... Ces al-

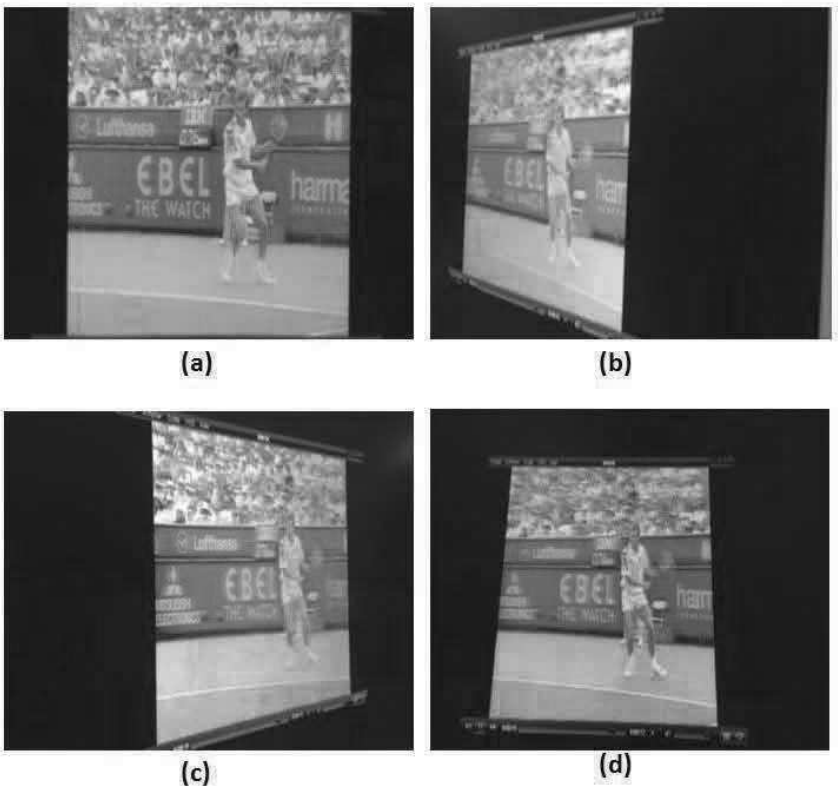

Figure 2: *Prises de vue : (a) caméra en face, (b) caméra à droite, (c) caméra à gauche, (d) caméra en bas.*

gorithmes ont été alors appliqués sur la séquence vidéo couleur Stefan composée de 300 images. La vidéo résultante a été mise à disposition de 20 utilisateurs qui vont essayer de détruire sa marque. Ces utilisateurs auront droit à trois essai pour chaque essai ils auront la possibilité d'appliquer autant d'attaques qu'ils veulent mais à condition de conserver une bonne qualité visuelle de la vidéo attaquée. En effet, après chaque choix d'attaque par l'utilisateur, un critère d'invisibilité est calculé et comparé à un seuil afin de valider ou non l'ensemble d'attaques choisies par l'utilisateur. Pour ce faire, nous avons utilisé la mesure de qualité SSIM (Structural SIMilarity) [WBSS04] qui permet de déterminer la similarité structurelle entre les images de la vidéo tatouée et les images de la vidéo tatouée après l'application des différentes combinaisons d'attaques par un utilisateur. Cette mesure a été choisie puisqu'elle calcule la similarité de structure entre ces images et pas la différence pixel à pixel comme c'est le cas pour les autres critères tels que le PSNR partant de l'hypothèse que l'œil humain est plus sensible aux changements dans la structure de l'image. Cette étude de similarité sera appliquée après chaque validation de choix d'un utilisateur. En effet, si la valeur du SSIM est inférieure à 0.4 l'essai de l'utilisateur ne sera pas validé et les combinaisons qu'il a appliquées ne seront pas considérées.

5.1. Interaction des utilisateurs

Nous avons enregistré les différents choix d'attaques de chaque utilisateur afin de dégager les attaques les plus utilisées et plus importantes. Nous avons alors remarqué que les utilisateurs ont essayé de tester toutes les attaques afin de voir leurs impacts sur la vidéo. En fait, ils ont tous choisi les vidéos camcordées : 3 utilisateurs ont sélectionné la vidéo camcordée avec une caméra en face de l'écran, 9 ont sélectionné la vidéo camcordée avec une caméra à gauche de l'écran, 6 ont sélectionné la vidéo camcordée avec une caméra à droite de l'écran et 2 ont sélectionné la vidéo camcorder avec une caméra en dessous de l'écran. Pour la compression la plupart des utilisateurs (13 utilisateurs) ont choisi la compression MPEG-4 avec un débit de compression de 500 kbit/s afin d'éviter la dégradation de la qualité visuelle de la vidéo. La figure 7 présente pour chaque débit, le nombre d'utilisateurs qui l'ont choisi. Les utilisateurs qui ont choisi la vidéo camcordée avec une caméra à gauche, à droite ou en dessous de l'écran ont tous choisi d'appliquer la déformation afin de recadrer la vidéo. Enfin, pour les deux dernières attaques, les utilisateurs qui les ont choisi, ont bien veillé à ne pas trop dégrader la visibilité de la vidéo et surtout la visibilité de l'objet en mouvement Stefan. La figure 8 montre pour chaque attaque le nombre d'utilisateurs qui l'a choisi. D'après cette courbe, nous pouvons remarquer que les attaques les plus utilisées sont le camcording, la compression, la déformation et le cropping.

5.2. Robustesse des l'algorithmes de tatouage

L'algorithme de tatouage vidéo basé sur l'insertion multifréquentielle dans les régions d'intérêts [KJZ12], a montré

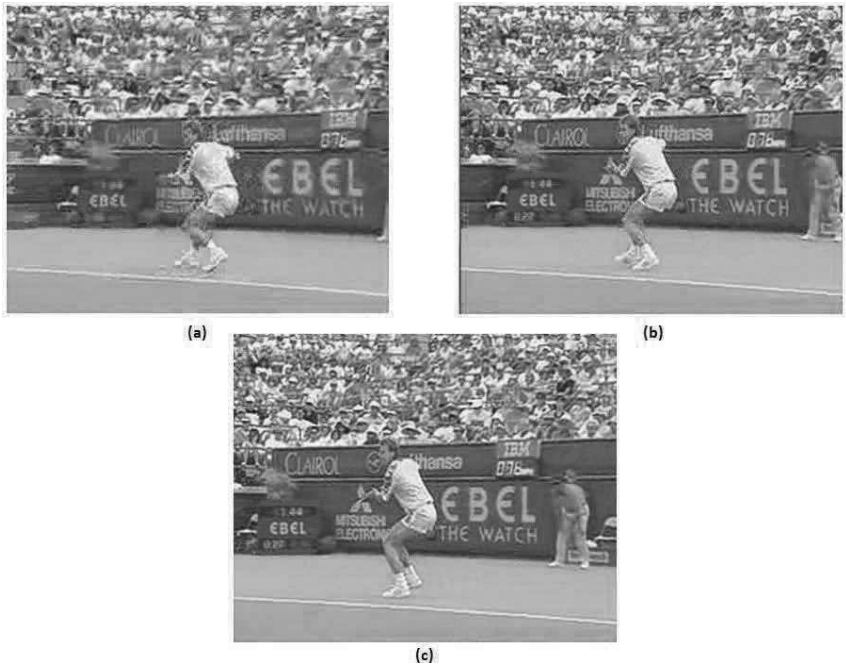

Figure 3: *Vidéo compressée : (a) Débit 200 kbit/s, (b) 500 kbit/s, (c) 1000 kbit/s.*

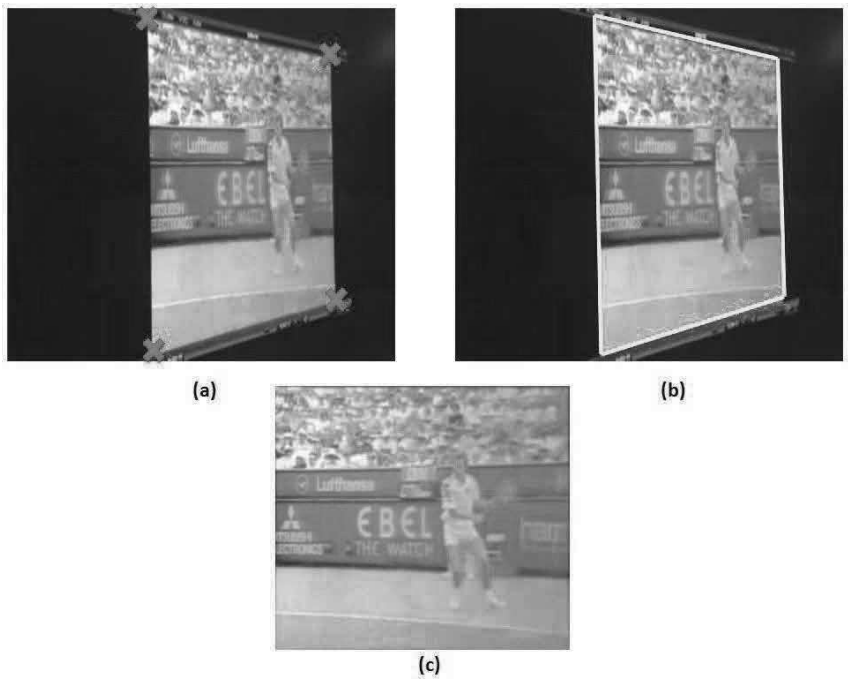

Figure 4: *Déformation des vidéos camcordées : (a) Sélection des coordonnées de la region à rectifier, (b) La région sélectionnée, (c) La région rectifiée.*

une haute performance face à toutes les combinaisons d'attaques possibles. En effet, on arrivait toujours à détecter la présence de la marque dans la vidéo après chaque test. La figure 9 présente le résultat de certaines combinaisons d'attaques appliquées sur la vidéo tatoué.

Pour l'algorithme de tatouage vidéo basé sur la transformée en ondelette [CL03], malgré sa robustesse face aux attaques usuelles, 6 utilisateurs ont réussi à détruire la marque insérée dans la vidéo tout en conservant une bonne visibilité, le tableau 1 présente les combinaisons appliquées par ces utilisateurs qui ont réussi à détruire la marque et les valeurs SSIM pour chaque combinaison et la figure 10 présente

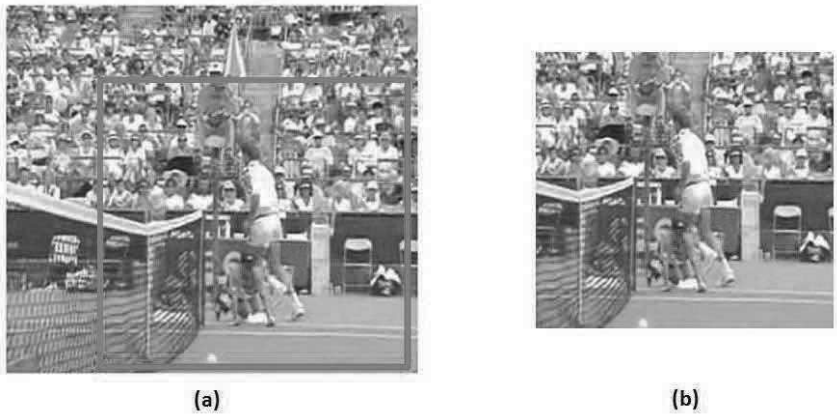

Figure 5: *Cropping de la vidéo : (a) sélection de la région par l'utilisateur, (b) vidéo croppée.*

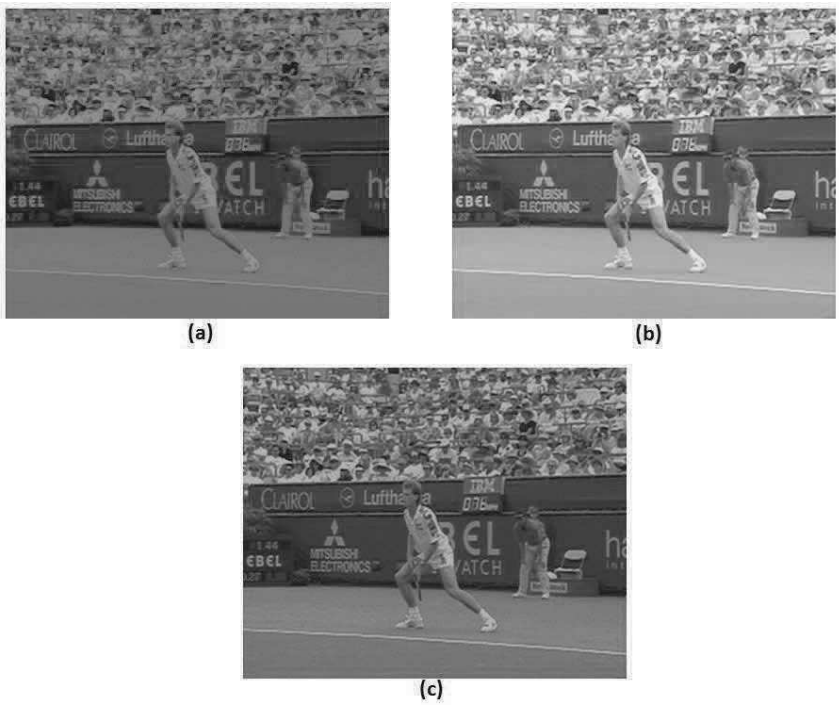

Figure 6: *Modification des couleurs de la vidéo : (a) Ajout de rouge, (b) Ajout de vert, (c) Ajout de bleu.*

le résultat de deux combinaisons d'attaques appliquées sur la vidéo tatoué.

6. Conclusion

Dans ce papier nous avons proposé un nouveau jeu d'attaques basé sur le crowdsourcing dans le but d'améliorer l'évaluation des algorithmes de tatouage vidéo. Ce jeu permet aux différents utilisateurs d'appliquer sur une vidéo tatouée des combinaisons d'attaques importantes et réelles telle que le camcording, la déformation, l'ajout de couleur et la compression dans le but de détruire la marque qui a été insérée. Ce jeu a permis non seulement d'évaluer les algorithmes d'insertion utilisés pour tatouer la vidéo test, mais aussi de dégager l'ensemble d'attaque les plus importantes en se basant sur les choix des différents utilisateurs. En effet, les tests réalisés ont montré que notre méthode d'évaluation est bien meilleure que les autres méthodes usuelles vue que ça nous a permis de comparer deux algorithmes de tatouage vidéo qui ont déjà fait leurs preuves face aux attaques usuelles et ont été classés parmis les méthodes robuste de tataouge vidéo alors que un seul a résisté aux combinaisons d'attaques appliquées dans notre jeu. En plus, ça a montré l'importance de l'attaque du camcording qui présente un grand risque pour les algorithmes de tatouage et qui est souvent négligée dans l'évaluation de robustesse de la plupart des algorithmes de tatouage vidéo. Comme perspective pour ce travail, nous allons le compléter afin d'élaborer un nouveau protocole d'évaluation des techniques de tatouage vi-

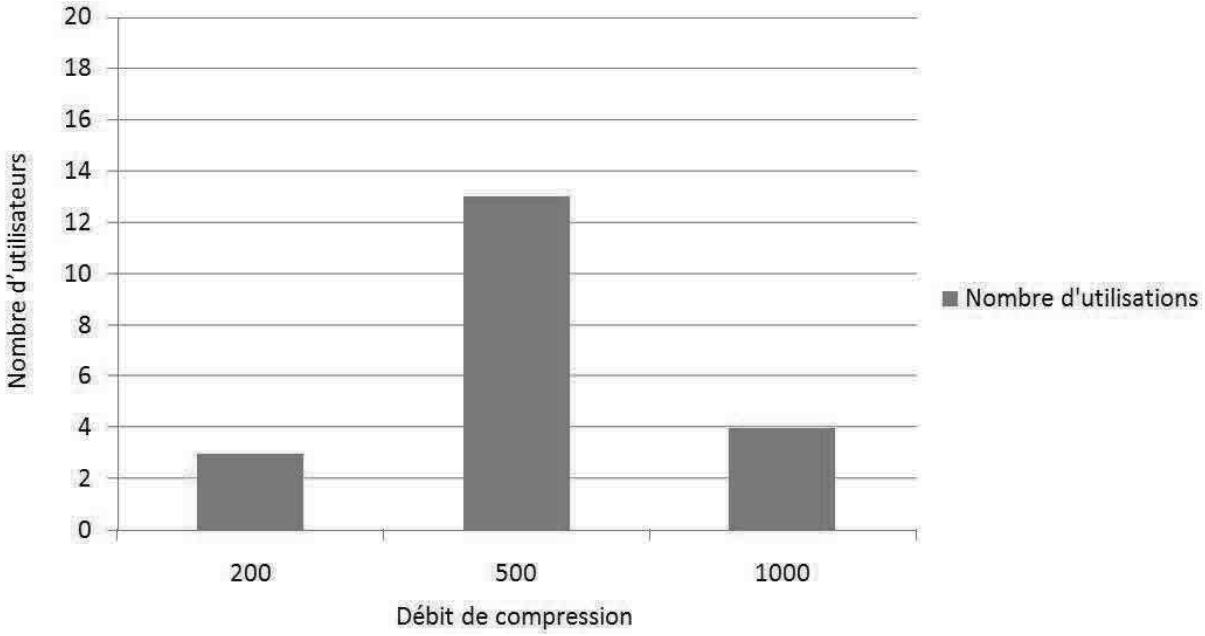

Figure 7: *Nombre d'utilisation pour chaque débit de compression.*

	(1)	(2)	(3)	(4)	(5)	(6)
SSIM	0.57	0.51	0.53	0.437	0.431	0.47

Table 1: *Valeurs de SSIM pour les vidéos tatouées dont la marque à été détruite : (1) Vidéo camcordée en face + compression 500 kbit/s + Cropping,(2) Vidéo camcordée à droite + déformation + compression 500 kbit/s + Cropping,(3) Vidéo camcordée à gauche + déformation + compression 500 kbit/s,(4) Vidéo camcordée à gauche + déformation + compression 500 kbit/s + Cropping + modification de couleurs,(5) Vidéo camcordée à gauche + déformation + compression 500 kbit/s + Cropping,(6) Vidéo camcordée en bas + déformation + compression 500 kbit/s + Cropping*

déo et ceci en ajoutant d'autres attaques qui peuvent présenter un danger sur la marque en la combinant avec d'autres attaques et aussi en intégrant l'évaluation de la visibilité de la vidéo après l'application des attaques. Ce jeu sera bénéfique sur deux côtés. En effet, il permettra d'évaluer l'algorithme de tatouage à tester en se basant sur un ensemble d'attaques les plus importantes. En plus, l'étude des choix des différents utilisateurs ainsi que la réaction de l'algorithme de tatouage face aux tentatives de sa destruction pourra servir pour l'amélioration du principe de l'algorithme afin de résister à ces attaques.

Références

[A.P99] A.P.PETITCOLAS F. : Attaques et évaluation des filigranes numériques. *CORSEA*, Num. 14-15 (1999).

[BF] BAS P., FURON T. : Project bows2. *www.http ://bows2.ec-lille.fr/.*

[C.08] C. B. D. : Crowdsourcing as a model for problem solving : an introduction and cases. *The International Journal of Research into New Media Technologies. Vol. 14*, Num. 1 (2008).

[C.10] C. B. D. : Moving the crowd at threadless : motivations for participation in a crowdsourcing application. *Information, Communication & Society. Vol. 13*, Num. 8 (2010).

[CCOM10] CARLIER A., CHARVILLATA V., OOI W., MORIN. R. G. G. : Crowdsourced automatic zoom and scroll for video retargeting. *ACM Multimedia* (2010).

[CL03] CHAN P. P.-W., LYU M. R. : A dwt-based digital video watermarking scheme with error correcting code. *ICICS'03* (2003).

[CMR01] CHANDRAMOULI R., MEMON N., RABBANI M. : Invisible watermarking for digital cinema. *DIGITAL WATERMARKING* (2001).

[FJB99] F.HARTUNG, J.K.SU, B.GIROD : Spread spectrum watermarking : Malcious attacks and counter-attacks. *SPIE : Security and watermarking of Multimedia Contents. Vol. 3657*, Num. 147-158 (janvier 1999).

[GF11] GREENGARD, FOLLOWING S. : the crowd. *Communications of the ACM. Vol. 54*, Num. 2 (2011).

[J.06] J. H. : The rise of crowdsourcing. *Wired Magazine. Vol. 14*, Num. 6 (2006).

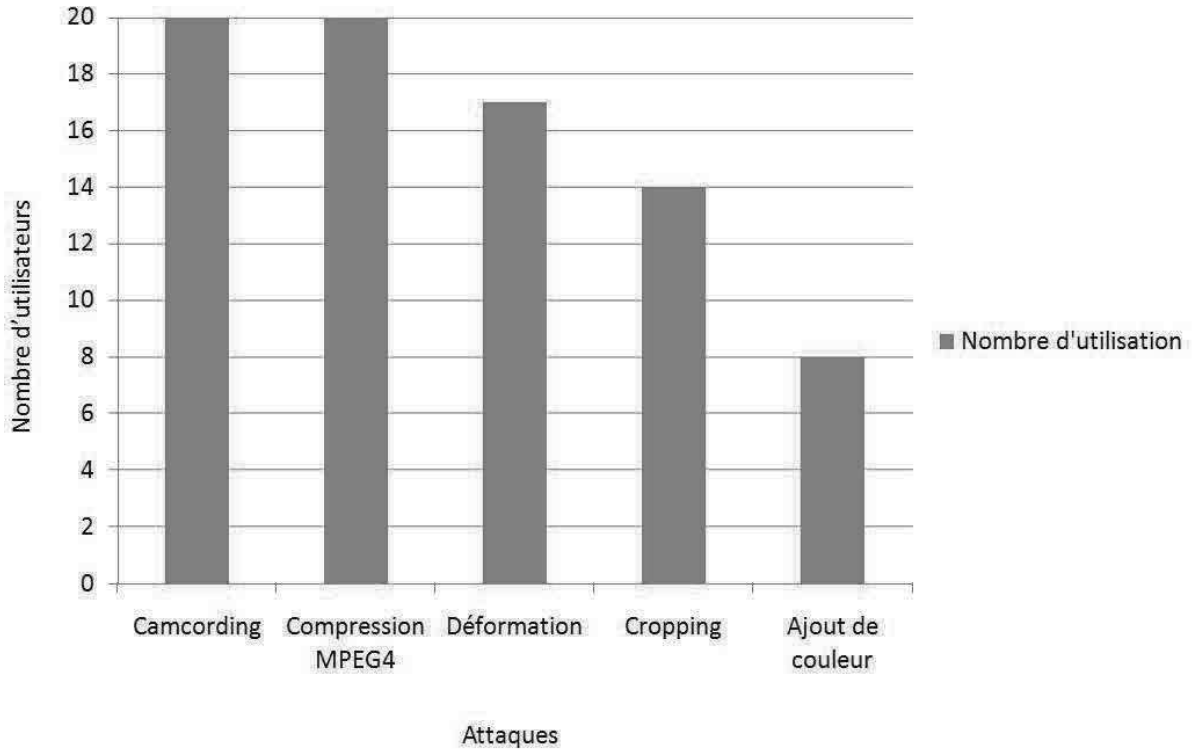

Figure 8: *Nombre d'utilisation pour chaque attaque*

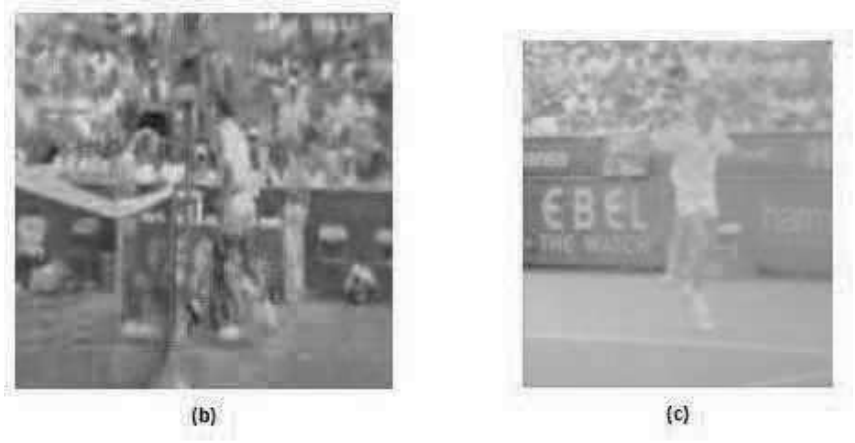

Figure 9: *Vidéo attaquée, tatoué par l'algorithme [KJZ12] :(b) vidéo camcorder en face + compression MPEG-4 200kbit/s + cropping, (c) vidéo camcorder à gauche + compression 500 kbit/s + cropping + ajout de couleur bleu +10.*

[J.08] J. B. : Hack, mash and peer : Crowdsourcing government transparency. *The Columbia Science and Technology Law Review. Vol. 9* (2008).

[KJZ12] KERBICHE A., JABRA S. B., ZAGROUBA E. : A robust video watermarking based on image mosacing and multi-frequential embedding. *IEEE International Conference on Intelligent Computer Communication and Processing* (2012).

[Pet00] PETITCOLAS. F. A. P. : Watermarking schemes evaluation. *I.E.E.E. Signal Processing. Vol. 17*, Num. 5 (2000).

[Rol] ROLLIN C. : Certimark. *www.certimark.org/.*

[SKWE14] SCHABER P., KOPF S., WESCH C., EFFELSBERG W. : A camcorder copy simulation as watermarking benchmark for digital video. *ACM Multimedia Systems Conference* (2014).

[WBSS04] WANG Z., BOVIK A. C., SHEIKH H. R., SI-

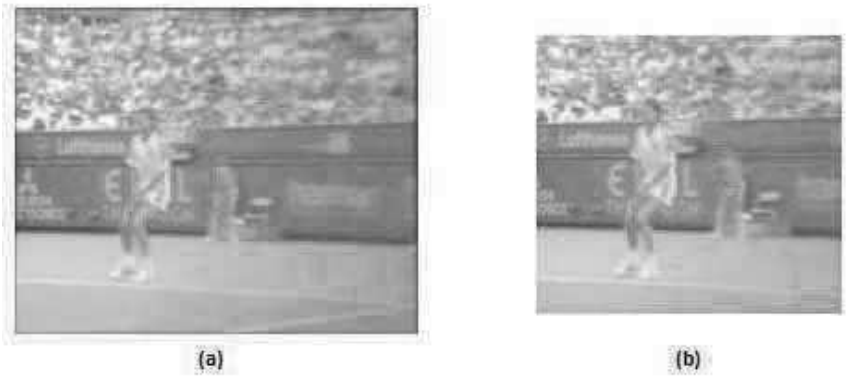

Figure 10: *Vidéo attaquée, tatoué par l'algorithme [CL03] : (a) Vidéo camcordée à gauche + déformation + compression 500 kbit/s(b) Vidéo camcordée à gauche + déformation + compression 500 kbit/s + Cropping*

MONCELLI E. P. : Image quality assessment : From error measurement to structural similarity. *IEEE Trans. Image Processing* (2004).

[XLGyM05] XIE X., LIU H., GOUMAZ S., YING MA. W. : Learning user interest for image browsing on small-formfactor devices. *SIGCHI Conference on Human Factors in Computing Systems* (2005).