A New Efficient Robustness Evaluation Approach for Video Watermarking based on Crowdsourcing

Asma Kerbiche[1], Saoussen Ben Jabra[1], Ezzeddine Zagrouba[1] and Vincent Charvillat[2]
[1]*Lab. RIADI - Team of Research SIIVA, Higher Institute of Computer Science, University Tunis El Manar, Ariana, Tunisia*
[2]*Lab. IRIT - Team of Research VORTEX, ENSEEIHT - INP TOULOUSE, University of Toulouse, Toulouse, France*

Keywords: Watermarking, Crowdsourcing, Evaluation, Robustness, Attacks, Camcording, Attack's Game.

Abstract: Signature robustness is the most important criteria that must verify a watermarking approach. However, existing watermarking evaluation protocols always tested simple attacks like rotation, cropping, and compression but did not consider many dangerous attacks such as camcording which is more and more used for videos. In this paper, a new robustness evaluation approach for video watermarking is proposed. It is based on on-line attack's game using crowdsourcing technique. In fact, the proposed game is provided to different users who will try to destruct an embedded signature by applying one or many combined attacks on a given marked video. Switch the choice of the users, the most important attacks can be selected. In more, users must not destroy the visual quality of the marked video to evaluate the tested watermarking approach. Experimental results show that the proposed approach permits to evaluate efficiently the robustness of any video watermarking. In addition, obtained results verify that camcording attack is very important in video watermarking evaluation process.

1 INTRODUCTION

The fast networks development and the evolution of new compression standards have facilitated copying, transmission and distribution of digital data such as text, image and video. Therefore, piracy and illegal use of these data has become easier and can cause a significant economic impact. Different techniques are appeared like cryptography, steganography but they cant protect efficiently digital contents. Watermarking is then proposed to resolve these problems. It consists to embed a signature into data and to try to detect it after any manipulation done on marked data. Many watermarking approaches are developed for different types of media and especially for video where the protection researches attracted more and more scientific community. In fact, an efficient video watermarking must verify two main constraints: invisibility, it means that original and marked video must be identical and robustness against different attacks. This last one is evaluated by applying different attacks on marked video and then trying to detect the embedded signature. However, despite the evolution of watermarking algorithms and hacking techniques, their robustness is always evaluated only against classic and simple attacks. In fact, existing evaluation protocols use the usual attacks such us geometric transformations, noise addition and filtering but, nowadays, all watermarking approaches must resist to this type of attacks. With new technologies development, other types of attacks are appeared and observed in the real world. These attacks must be considered both at development of watermarking approach and at evaluation step. The most important and malicious attack is camcording which consists of recording movies in theaters with a Smartphone or a camera that can be followed by colorimetric transformations, a compression or deformation manipulation.

In this paper, a new robustness evaluation approach is proposed. It is based on crowdsourcing technique which allows using the collective intelligence of many users. In fact, this approach consists of an attacks game where different users will try to destroy a mark inserted into a given video by applying various combinations of available attacks, while maintaining a good visibility of the video. This interaction will allows evaluating the watermarking approach applied on the test video and selecting the most interesting attacks.

The remainder of this paper is organized as follows: in the next section, a state of the art of the existing evaluation protocols of video watermarking

Kerbiche, A., Jabra, S., Zagrouba, E. and Charvillat, V.
A New Efficient Robustness Evaluation Approach for Video Watermarking based on Crowdsourcing.
DOI: 10.5220/0005726201670173
In *Proceedings of the 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2016) - Volume 3: VISAPP*, pages 169-175
ISBN: 978-989-758-175-5

algorithms and crowdsourcing technique will be presented. The proposed approach will be detailed in the second section. The selected attacks will be descriped in the third section. Experimental results and evaluation will be provided in the fourth section. Finally, conclusion and perspectives are drawn in Section 5.

2 STATE OF ART

The goal of the proposed work is to select the most important attacks which can be applied on a marked video to evaluate any watermarking approach. This selection is based on crowdsourcing technique.

2.1 Existing Evaluation Protocols

Several protocols have been proposed to evaluate video watermarking algorithms. However, these protocols generally use the same traditional attacks for robustness evaluation. The European project Certimark (Rollin,) is proposed to realize generic tests to evaluate image and video watermarking methods. In the case of a video watermarking, this protocol tested different attacks which are: compression, digital to analog and analog to digital conversion (D / A and A / D), lossy storage formats conversion, logos or captions adding, geometric transformations like rotation, translation, Cropping and scaling, multiple watermarks, noise and collusion. Several other protocols have been proposed for image watermarking algorithms and can be applied to video watermarking such as StirMark benchmark project (Petitcolas, 2000) and "BOWS" project (Break Our Watermarking System) (Bas and Furon,) which is based on multiple constraints like capacity, invisibility, speed and robustness. In spite of the efficiency of the existing protocols, they test only simple attacks where a classic watermarking approach can resist and they didn't integrate the most dangerous and real attacks which can easily destruct the embedded signature.

2.2 Crowdsourcing Technique

Crowdsourcing technique has become a widely applied practice in the context of innovation and problem solving (Stanoevska-Slabeva, 2011), that's why researches related to this technique have become a dynamic and vibrant research area. Howe (J., 2006), classifies crowdsourcing in three main categories based on type of task outsourced to the crowd. The first class presents the idea game which is essentially just a massive call for ideas such as IBM Jam. In fact, in 2006, IBM initiated a global idea jam related to the question how to best use and efficiently commercialize existing technological developments in the company, the task of the crowd was to brainstorm about potential new ways how technology developed at IBM might be applied to enhance existing or develop new products. The second category is crowdsourced problem solving where the problem is broadcasted to a large undefined network of potential solvers. The goal is to create a complete solution by integrating complementary contributions from the crowd by defining of clear interfaces. Xie et al. (Xie et al., 2005) propose new method to detect user interest maps and extract user attention objects from the image browsing log using crowdsourcing. A smart image viewer was developed based on user interest analysis and a second experiment was carried out to study how users behave with such a viewer. This approach is more efficient than image-analysis based methods and can better represent users' actual interest. Based on the fact that the viewing experience on the mobile devices can be improved by determining important and interesting regions within the video (regions of interest, or ROIs) and displaying only the ROIs to the viewer, Carlier et al (Carlier et al., 2010) propose an alternative paradigm to infer ROIs from a video by crowdsourcing from a large number of users through their implicit viewing behavior using a zoom and pan interface, and infer the ROIs from their collective wisdom. A retargeted video, consisting of relevant shots determined from historical users' behavior, can be automatically generated and replayed to subsequent users who would prefer a less interactive viewing experience. A user study shows that this automatically retargeted video is of comparable quality to one handcrafted by an expert user. Finally the last category is prediction markets in which investors from the crowd buy and sell futures related to some expected outcome.

3 PROPOSED EVALUATION APPROACH

The main originality of the proposed approach is to use crowdsourcing technique for evaluation. In fact, it consists of an attacks' game which is based on users' actions when they try to destroy signature from marked videos. This game makes users free to choice one or a combination of attacks and to apply them on videos. This allows detecting the most important manipulations which can be dangerous for a watermarking algorithm. In more, thanks to using real users, this permits to simulate the behavior of a pirate when he wants to destroy a signature contrary to the use

of a robot where we cannot know the type of manipulations which can be applied in reality. The proposed approach allows also applying different attacks without damaging visual quality of the marked and attacked video. In fact, a visual threshold is defined to oblige the users to reserve the visual contents of the video to be attacked. General architecture of the proposed approach is presented in the figure 1.

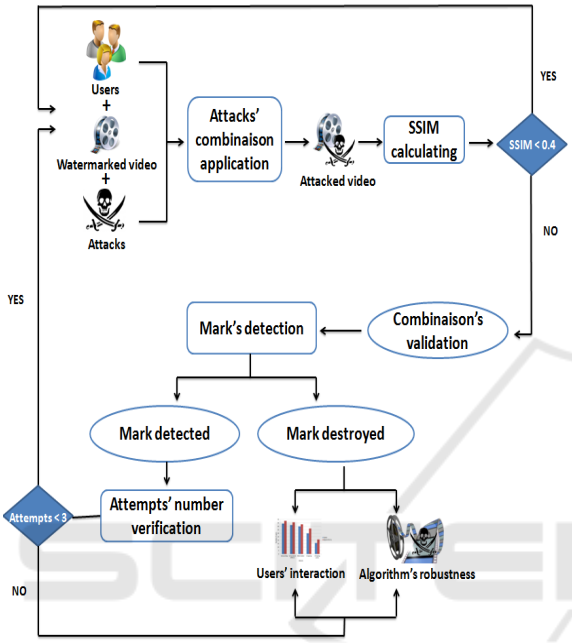

Figure 1: General architecture of the proposed approach.

The second originality of the proposed approach is to use camcording attack to evaluate the robustness of a given watermarking approach. In fact, camcording is an important and much applied attack for video applications but it is not considered in other evaluation protocols. This attack consists of filming the video projected or displayed using a Smartphone or a camera and then broadcast it after having applied some transformations to destroy the watermark that has been inserted. Due to camcording attack, illegal copies of movies have become an important concern of the film industry and technology development in recent years. Some works were then proposed, these last years, to guarantee robustness against this attack such as the algorithm developed by the research and development unit of Kodak (CHANDRAMOULI et al., 2001) that showed its worth against the camcording by embedding a signature containing the movie theater where the screening took place and the time and release date. In more, for helping researchers to develop watermarking approaches robust to camcording attack, Philipp Schaber et al. (Schaber et al., 2014) have developed a tool that simulates a reacquisition of content with a camcorder.

The proposed attack's game consists of an interface containing a fun challenge: "Find the best attacks that removes the watermark without radically degrading video." This interface is available to users and it allows them to apply to the watermarked videos a combination of attacks that we have identified as most important and dangerous. The proposed interface is shown in Figure 2 and is decomposed in three main parts: the first one contains a preview of the watermarked video, the second contains the list of selected attacks and the last part shows a view of the attacked watermarked video. Each user has three attempts to destroy the signature. Firstly, he must choice the type of test video which can be camcordered or not. Then, he can apply a compression on chosen video by choosing a compression rate. Finally, he can apply other types of attacks. After every attack application, the visual quality of attacked video will be calculated and if it is lower than a defined threshold, the user must choice other attacks.

4 CHOSEN ATTACKS

Based on investigations made with film experts, five attacks are chosen to be tested in the proposed interface. The first attack is camcording which is realized with four different camera positions: in front of the screen, then right, then left and finally down of the screen as shown in Figure 3.

The second chosen attack is MPEG 4 compression which is the most popular compression standard and presents the better method for high definition broadcasting. Due to the importance of this compression system, any efficient watermarking algorithm must be able to resist to this attack at least in the low compression ratio. For this reason the second step in our game of attacks is to allow users to choose to work with the compressed or not compressed watermarked video and to choose one of three compression rates 1000 kbit/s, 500 kbit/s and 200 kbit/s (Figure4).

The third attack is the deformation that users can apply, in the case of camcording videos. It consists to change videos reframing (Figure 5) by selecting area coordinates they want to rectify.

The fourth attack is cropping that consists of extracting a region from the video's frame by cutting horizontally or vertically images from the video. This attack can completely destroy the watermark. In our proposed game, users can select the video area they wish to preserve on condition to guarantee the good visual quality of the cropped video (Figure 6).

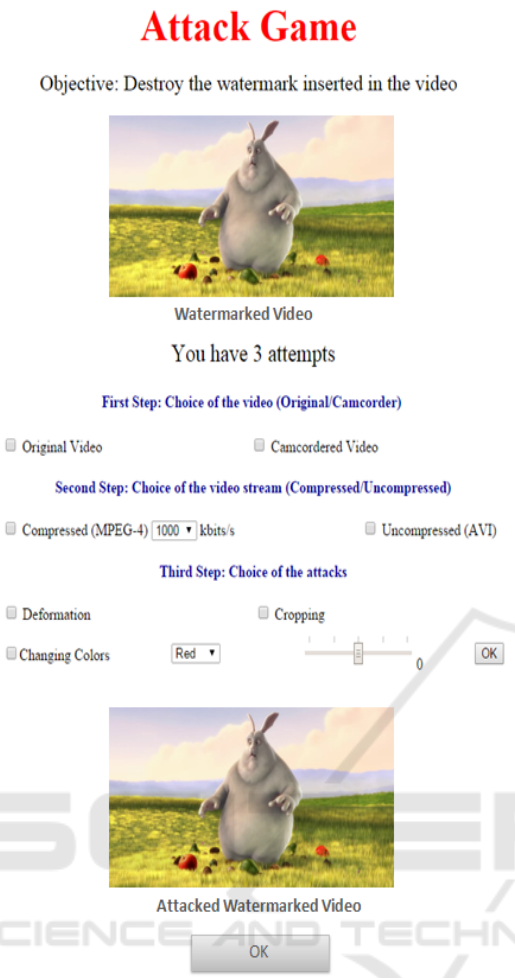

Figure 2: Attacks game interface.

Finally, the latest attack available in the proposed game is changing color of the video by adding red, green or blue color to the original video frames (Figure 7).

5 EXPERIMENTAL RESULTS

To test the proposed robustness protocol and to study and analyze the choice of the different users, we choose to evaluate and compare two existing video watermarking schemes: the first one is based on multi-frequency insertion in feature regions proposed in our previous work (Kerbiche et al., 2012) and the second is based on wavelet transform (Chan and Lyu, 2003). These two algorithms presented good robustness against the usual video watermarking attacks such as rotation, noise addition, frame deleting and compression... These algorithms were applied to the two colors video Stefan and Big Buck Bunny. We

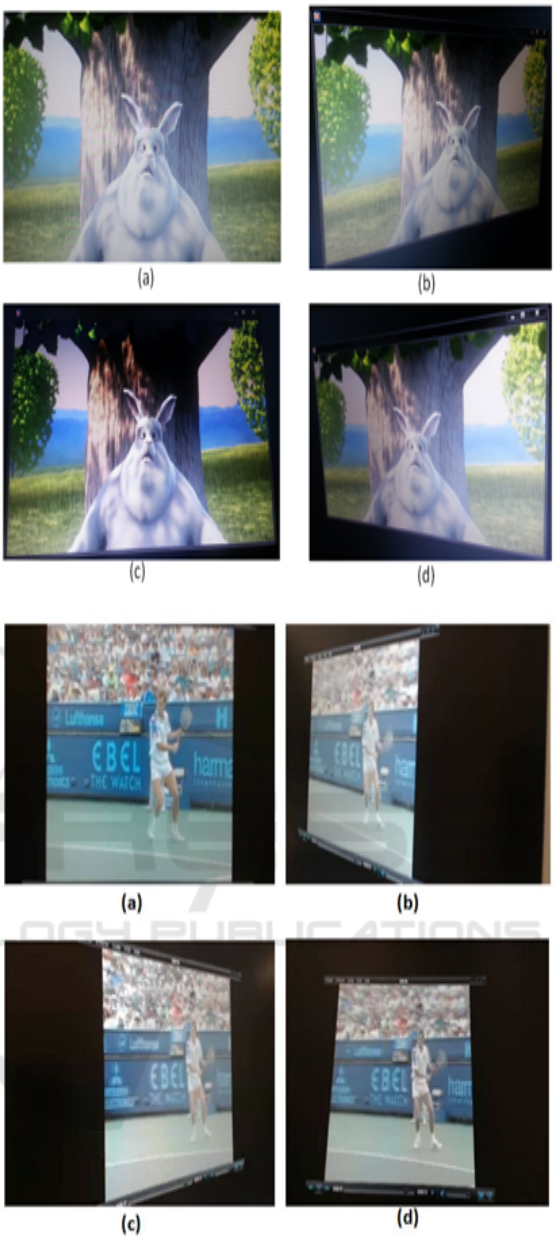

Figure 3: Camcording attack: (a) camera in front of the screen, (b) camera in the left of the screen, (c) camera down of the screen, (d) camera in the left of the screen.

have exposed the proposed game to 50 users who have 3 attempts to destroy the mark by combining attacks while keeping a good visibility of the video. In fact, after each attempt a measure of the quality was calculated and compared to a threshold before the validation of the user's attempt.

We choose to use the structural similarity (SSIM) as a quality's measure. It is a method for measuring the similarity between two images. The SSIM index is a full reference metric and it is designed to im-

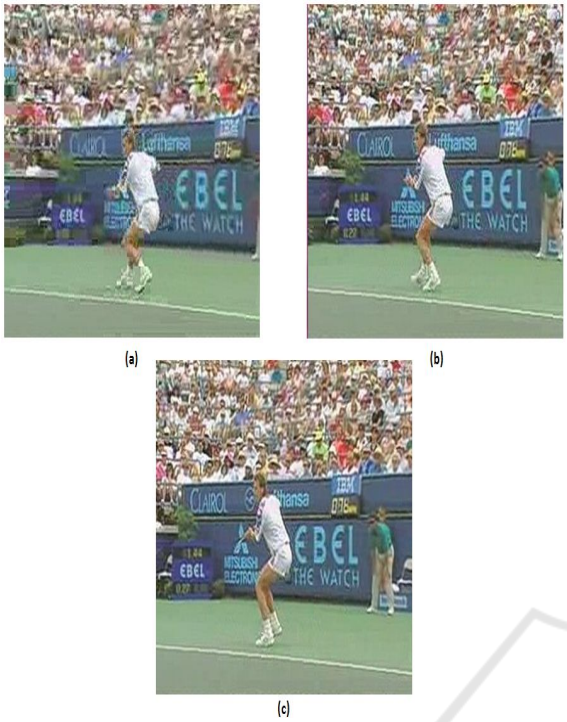

Figure 4: Compression MPEG 4 : (a) 200 kbit/s, (b) 500 kbit/s, (c) 1000 kbit/s.

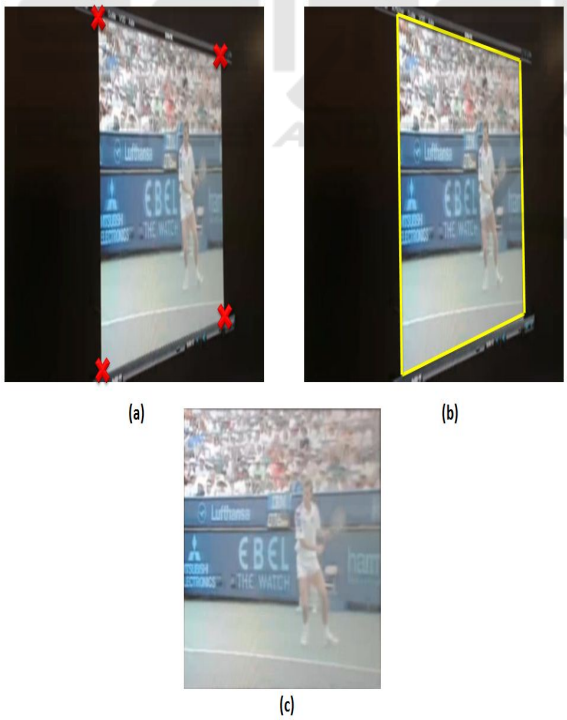

Figure 5: Deformation of camcordered watermarked video: (a) Selection of the coordinates of the region, (b) The selected region, (c) Rectified region.

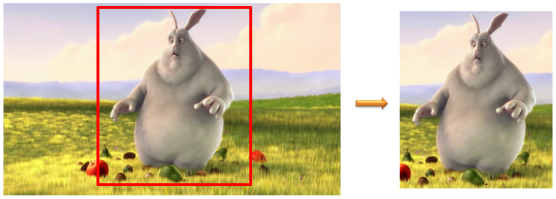

Figure 6: Cropping attack.

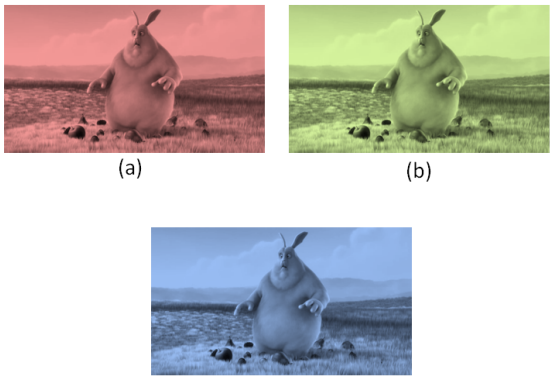

Figure 7: Colors changing of the watermarked video: (a) Red adding, (b) Green adding, (c) Blue adding.

prove on traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception. The difference with other techniques such as MSE or PSNR is that these approaches estimate perceived errors, but SSIM considers image degradation as perceived change in structural information. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The SSIM metric is calculated on various windows of an image. The measure between two windows $\boldsymbol{x}$ and $\boldsymbol{y}$ of common size N $\times$ N is:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (1)$$

Where μ_x presents the average of $\boldsymbol{x}$; μ_y the average of $\boldsymbol{y}$; σ_x^2 the variance of $\boldsymbol{x}$; σ_y^2 the variance of $\boldsymbol{y}$ and σ_{xy} the covariance of $\boldsymbol{x}$ and $\boldsymbol{y}$. The two variables c_1=$(k_1L)^2$ and c_2=$(k_2L)^2$ permit to stabilize the division with weak denominator. Finally, L is the dynamic range of the pixel-values (typically this is $2^{\sharp bits\ per\ pixel}$-1) and the values of k_1 and k_2 are respectively 0.01 and 0.03 by default.

This similarity study will be applied before each validation of user. Indeed, if SSIM value is less than 0.4, user attempt will not be validated and the combination he applied will not be considered.

5.1 Users Interaction

To identify the most used and important attacks we have registered the different choices of each user. We observed that users have attempted to test all the attacks in order to see their impacts on the video, after that, most of them have chosen the camcordered video (44 have chosen the Stefan camcordered video and 48 have chosen the Big Buck Bunny camcordered video). The users which have chosen the camcordered video with camera in the left, in right and down of the screen they have all applied the deformation to adjust the crop of the video. For compression, most users have chosen this attack with a 500 kbit/s compression rate in order to avoid degradation of the video visual quality. Figure 8 shows for each rate, the number of users which have chosen it.

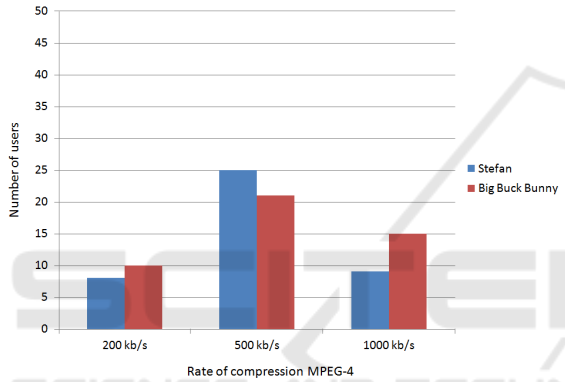

Figure 8: Number of choice for each rate of compression.

Finally, for the last two attacks, users have been careful to not degrade the visibility of the video and especially the visibility of the moving objects. Figure 9 shows for each attack the number of choice. According to this curve, we can notice that the most common attacks are camcording, compression, deformation and cropping.

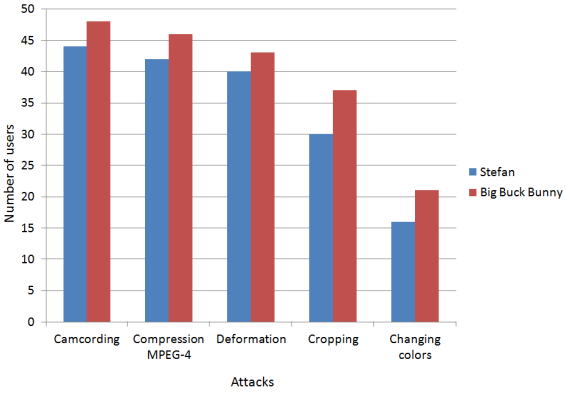

Figure 9: Number of choice for each attack.

5.2 Video Watermarking Algorithm Robustness

The video watermarking algorithm based on multifrequency insertion in the region of interests (Kerbiche et al., 2012), showed a high performance against all the combinations of attacks. In fact, this algorithm could always detect the presence of the mark in the video after each test. Figure 10 shows the result of some combinations of attacks applied on the watermarked video.

Figure 10: Attacked video watermarked (Kerbiche et al., 2012): (a) camcordered video with camera in front of the screen + MPEG-4 Compression 200 kb/s + cropping, (b) camcordered video with camera in the left of the screen + MPEG-4 Compression 200 kb/s + cropping + red color adding +15.

For video watermarking algorithm based on wavelet transform (Chan and Lyu, 2003), despite its robustness against common attacks, 17 users have destroy the mark inserted in the video while maintaining good visibility. Table 1 shows some combinations applied by those users who have succeeded to destroy the signature and SSIM values for each combination where (1) is camcordered video with camera in front of the screen + compression 500 kbit/s + Cropping, (2) camcordered video with camera in the right of the screen + deformation + compression 500 kbit/s + Cropping, (3) camcordered video with camera in the left of the screen + deformation + compression 500 kbit/s, (4) camcordered video with camera in the left of the screen + deformation + compression 500 kbit/s + Cropping + changing colors, (5) camcordered video with camera in the left of the screen + deformation + compression 500 kbit/s + Cropping and finally (6) camcordered video with camera down of the screen + deformation + compression 500 kbit/s + Cropping. Figure 10 shows the result of two combinations of attacks applied on the watermarked video.

Table 1: SSIM values of the watermarked video which users have destroy the mark.

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

(a) (b)

Figure 11: Attacked video watermarked (Chan and Lyu, 2003): (a) camcordered video with camera in the left of the screen + deformation + compression 500 kbit/s, (b) camcordered video with camera down of the screen + deformation + compression 500 kbit/s + Cropping.

6 CONCLUSION

In this paper we proposed a new robustness evaluation approach based on crowdsourcing in order to improve the evaluation protocols of video watermarking algorithms. This approach consists of a game which allows users to apply different combinations of important and most used attacks as camcording, deformation, adding color and MPEG-4 compression on watermarked videos in order to destroy the embedded mark. This game permits to evaluate existing video watermarking algorithms and also to identify the most important attacks based on the choices of different users. In fact, experimental tests have shown that the proposed evaluation approach is more efficient than other existing methods. In fact, it allowed us to compare two video watermarking algorithms which were ranked as two robust methods but only one of them have resisted to the combinations of attacks applied in the proposed game. In addition, it has proved the importance of the camcording attack which is very dangerous for video watermarking algorithms and is often not considered in existing evaluation protocols. As a perspective for this work, we will complete it in order to develop a new evaluation protocol of video watermarking techniques. In fact, other attacks that may present a risk can be added to the proposed game and also visibility evaluation must be included. The game will be beneficial to both sides. Indeed, it will evaluate the watermarking algorithms; in addition, the study of different users' choices as well as the reaction of the watermarking algorithm against their destruction attempts could be used to improve the watermarking algorithms to resist against these attacks.

REFERENCES

Bas, P. and Furon, T. Project bows2, www.http://bows2.ec-lille.fr/.

Carlier, A., Charvillata, V., Ooi, W., and Morin., R. G. G. (2010). Crowdsourced automatic zoom and scroll for video retargeting, in acm multimedia.

Chan, P. P.-W. and Lyu, M. R. (2003). A dwt-based digital video watermarking scheme with error correcting code, in icics'03. volume 2836.

CHANDRAMOULI, R., MEMON, N., and RABBANI, M. (2001). Invisible watermarking for digital cinema, in digital watermarking.

J., H. (2006). The rise of crowdsourcing, wired magazine. volume 14.

Kerbiche, A., Jabra, S. B., and Zagrouba, E. (2012). A robust video watermarking based on image mosacing and multi-frequential embedding, in ieee international conference on intelligent computer communication and processing.

Petitcolas, F. A. P. (2000). Watermarking schemes evaluation, in i.e.e.e. signal processing. volume 17.

Rollin, C. Certimark. www.certimark.org.

Schaber, P., Kopf, S., Wesch, C., and Effelsberg, W. (2014). A camcorder copy simulation as watermarking benchmark for digital video, in acm multimedia systems conference.

Stanoevska-Slabeva, K. (2011). Enabled innovation: Instruments and methods of internet-based collaborative innovation, in the 1st berlin symposium on internet and society.

Xie, X., Liu, H., Goumaz, S., and ying Ma., W. (2005). Learning user interest for image browsing on small-formfactor devices, in sigchi conference on human factors in computing systems.