ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse53842019.pdf
https://doi.org/10.30534/ijatcse/2019/53842019

Detection of Video Spam In Social Network Based Neural Network Convolution

Fatna EL MENDILI[1], Younès EL BOUZEKRI EL IDRISSI[2]
[1] Systems Engineering Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, f.elmendili@gmail.com
[2] Systems Engineering Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, y.elbouzekri@gmail.com

ABSTRACT

Today's Social networks are very popular, millions of people use various forms of social networks because they allow individuals to connect with friends and family, and share private information, users have the ability to communicate easily without constraints by providing them with free and open platforms. However, problems related to maintaining the confidentiality and security of a user's information may arise, particularly when the content downloaded by the user is multimedia, such as photos, videos and audio. The downloaded multimedia content transports information that can be transmitted virally and almost instantly to a social networking site and beyond. In this article, we have proposed a new approach to limit the dissemination and dissemination of spam videos on social networks, both when they are downloaded as an opening publication and when they are published as a video response. Since using online social networking services, users trust that they will be protected against all types of malicious content, including spam videos, which could compromise patient and user satisfaction with these platforms. This is why it is necessary not to neglect the security and confidentiality of profiles and systems, but rather to make a series of changes to improve protection and security on these platforms. Our work is based on one of the most popular deep learning algorithms, which are convolutional neural networks. Experience shows that the proposed solution is capable of providing excellent performance on 98% Accuracy, which shows that the proposed method is very effective.

Key words : Social network, Spam videos, convolutional neural network, Deep learning, Security.

1. INTRODUCTION

Recently, online social networking services such as Twitter, Facebook and YouTube have grown dramatically in popularity. The internet goes starting with the email social media or posts such as twitter, Gmail, face book, etc. This information may be called as the BIG DATA[11]. People are now getting all kinds of information in different areas on social media. It is an age where people live their social lives online, [1] use social sites for countless activities including creating an online presence, developing friendships and searching information.

Except that people often tend to forget, the security problems associated with the increasing use of these sites. Users share personal data on social networks without being fully aware of the consequences, whereas the context of an individual in these platforms can be used to extract sensitive information [2].

Since video permeates the Internet and supports new types of interaction among users, including political debates, video chats, video mail and video blogs, and that online social network allow users to publish and share their generated content independently, social video sharing systems can become vulnerable to various types of opportunistic and malicious actions such as spam videos. We define a video spam response as a video posted in response to an opening video, but whose content is completely independent of the opening video. Video spammers are motivated to use spam to promote specific content, advertise to generate sales, distribute pornography (often in the form of an advertisement) or compromise the reputation of the system [3].

In many social networks, such as Facebook, mainly multimedia data is produced and shared. According to a report from Zephoria Digital Marketing (ZDM) , approximately 136,000 photos are uploaded every 60 s on Facebook. A set of statistics from SocialMediaToday show that the average viewing and sharing rate of videos on Facebook is increasing day by day. Currently, approximately 8 billion videos per day are viewed on Facebook, which is double the amount viewed in 2015.

After all, users cannot easily identify video spam before watching at least one segment, thereby consuming system resources, especially bandwidth, and compromise users' patience and satisfaction. Thus, identifying video spam is a difficult problem in social video sharing systems [4].

The rest of the paper is divided into eight sections. Section 2 will be dedicated to discuss the issue of security in social networks. Then, in section 3, we will discuss the work that deals with the preservation of privacy in social networks.

After that, we will propose in section 4 a new approach to limit the spread of spam videos in these platforms in order to preserve the security of users and ensure better protection against the spread of spam contents in these platforms. In section 5, several experiments will be presented using our system, to prove its effectiveness when detecting spam videos at the social network level, while in section 6 we present our prototype of proposed solution "SpamVideosDetector" in section 7 we will compared our method with those presented in section 3 .In Section 8, we presented our motivations behind this article. Finally, we will quote a conclusion and future work in section 9.

2. PROBLEMATIC

A social network R consists of X communities G (U, E), where U represent the users of a community of this social network, while E represent the unidirectional connections between U, each community contains {P1, P2, P3 ..Pn} user profile. Among the N users of this social network where N = X * U, there are N1 honest users in the social network called honest nodes. Where each of these nodes has a unique identity that characterizes him, and N2 malicious users who also have a unique identity, but in most cases usurping an identity of one of the N users of the R in order to lead several attacks like the dissemination of spam videos. The problem of detecting these spam videos consists in the possibility of preventing a video V_i from being a spam video using a classifier,

$$C : U\_i \rightarrow \{\text{Spam video, legitimate video}\} \quad (1)$$

These spam videos can be sent to users using the social network's messaging services, or even posted as a comment in one of a user's posts. Figure 1 below illustrates the reception of a user of a spam video.

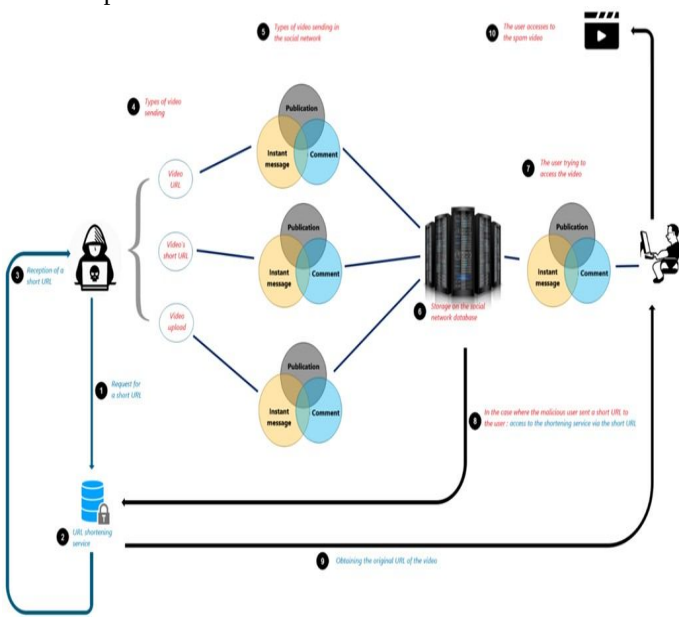


Figure 1: Methods of sending a spam video to a user in a social network

3. RELATED WORK

Nowadays, Applications such as Internet telephony, video response or video streaming have experienced spectacular growth in terms of popularity, which explains their importance in social networks. For example, a video conferencing system allows real-time discussions with colleagues from different agencies, without having to travel. However, unfortunately, different forms of unsolicited communication disturb users of social networking services [5]. Unsolicited communication opens a large gray area, where videos can be considered as spam or promotion. The simplest form of spam occurs when users submit a video with a long list of misleading tags to describe its content in order to deceive the video search mechanisms [6]. Another form of video spam occurs when a video is published as a response to an opening video, but whose content is completely independent of the opening video [7]. On the other hand, the promotion is that when users try to boost the ranking of their videos to make them very visible in social networks. Due to its intrinsic nature, the video response seems to be an attractive feature for spam users who exploit it for several actions, among which are the dissemination of pornography (often as advertising), promotion of specific content, compromise the reputation of the system etc..., disseminate pornography (often as advertising) or simply compromise reputation of the system.

Several methods are proposed to ensure and protect the privacy and confidentiality of users within social networks, among which we find the method proposed by (Fabricio Benevenuto et al [7] , which is based on the characterization of the users' behavior. The inter-reference distance (IRD) has been defined on users' sequence who download video responses to video V_i as the total number of responses that appear between two video responses from the same user. They considered that a user who downloads many video responses by video, one after the other, as a mechanical process, could be a candidate for further investigation. Thus, combining a large number of video-to-video responses and small IRDs suggests that the user has some type of antisocial behavior.

Another method called "UserRank" proposed by the same group based on the rank of the user, which allows capturing the importance of users in terms of views' number. They consider that high-ranking users are among the most visited and viewed, while lower-ranked users have few views and receive few or no video responses from the video community. This method has been proposed for the users' detection who boost a video ranking (i.e. promoted videos).

Priyanka Thakur et al. [12] examine the sentiment expression to classify the polarity of the text review on a scale of negative to positive and perform feature extraction and ranking and use these features to train our classifier to classify the text data into its correct label.

Another method has been proposed (by Margaret M. Flecket al. [8] which is based on a cutaneous filter. Since the

appearance of the skin is narrowly limited, and the color of a human's skin is created by a combination of blood (red) and melanin (yellow, brown), human skin has a range restricted hue. This method consists in extracting the images from a video and applying a classification description and approach based on these images, that if an image is considered as inappropriate, this means that the color characterizing the human skin covers the entire image, the video that corresponds to it will also be considered as inappropriate.

Researchers [10] proposals to improve the security of users are still limited and many spammers still publishing the spam videos in these platforms, the thing that motivated us to propose a new approach to limit the publication of these spam videos.

4. PROPOSED FRAMEWORK

We human beings; we constantly analyze the world around us. Without conscious effort, we make predictions about everything we see, and act on them. When we see something, for example a video, we label each image in that video based on what we have learned in the past and then we can deduce its context. However, how do we do that? How can we interpret everything we see? How can we use the way our brain processes data to provide a method for filtering spam videos in an efficient way?

As shown in Figure 2, the collaboration between the eyes and the brain, called the primary visual pathway, is the reason why we can make sense of the world around us as vision begins in the eyes, the actual interpretation of what we see occurs in the brain, in the primary visual cortex.

When seeing an object, the light receptors in the eyes send signals through the optic nerve to the primary visual cortex, where the input is being processed. The primary visual cortex gives meaning to what the eye sees.

All this seems very natural. We hardly think how special it is that we are able to recognize all the objects and people we see in our lives. The deeply complex hierarchical structure of neurons and connections in the brain plays a major role in this process of memorizing and labeling objects.

To better understand this, let us think of how we learned about a car, a computer, a dog, etc. In the beginning, our parents or our family told us the names of the objects in our direct environment. We have learned from examples that have been given to us. Slowly but surely, we started to recognize some things more and more often in our environment. They have become so common that the next time we see them; we will know instantly what the name of this object was. They have become part of our model on the world.

It is the same way that convolutional neural networks (CNN) work and on which we will rely for the detection of spam videos "that means a video representing inappropriate content, or even a video posted as response to an opening video.

However, whose content is completely independent of the opening video " during their publications on social networks, our method is based on 3 steps:

4.1. Step 1: Extracting images from a video

As mentioned earlier, video has become one of the most widely used media in online social networks, playing a big role in how audiences get content on these platforms, but what represent a video from a technical point of view? In a simple way, a video is only a combination of images, accompanied or not by sound, to form a moving image that means that we have the possibility to extract all the images who composes a given video. During this step, as shown in Figure 3. We assumed that the extraction of an image from a video every second is largely sufficient to have good results during the following steps.

Algorithm for extracting images from a video

```
Input: video
Output:images[sequences]
# Importing all necessary libraries
import cv2
import os
# Read the video from specified path
cam =
cv2.VideoCapture("C:\\Users\\Admin\\video
spam\\project_1\\openCV.mp4")
try:
    # creating a folder named data
    if not os.path.exists('data'):
        os.makedirs('data')
# if not created then raise error
except OSError:
    print ('Error: Creating directory of
data')
# frame
currentframe = 0
while(True):
    # reading from frame
    ret,frame = cam.read()
    if ret:
        # if video is still left continue
creating images
        name = './data/frame' +
str(currentframe) + '.jpg'
        print ('Creating...' + name)
        # writing the extracted images
        cv2.imwrite(name, frame)
        # increasing counter so that it will
        # show how many frames are created
        currentframe += 1
    else:
        break
# Release all space and windows once done
cam.release()
cv2.destroyAllWindows()
```

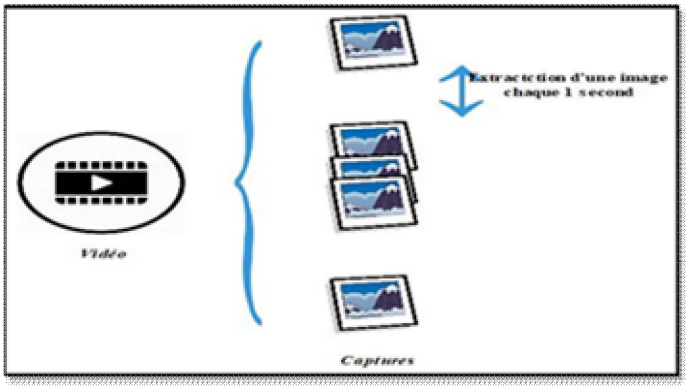


Figure 2: Extracting images from a video

4.2. Step 2: Context extraction of images

Nowadays, among the most efficient models for classifying images, there is what is called; the convolutional neural networks. Designated by the acronym CNN, they have two distinct parts. In input, an image is provided in the form of a matrix of pixels. It has 2 dimensions for a grayscale image. The color is represented by a third dimension of depth to represent the fundamental colors [Red, Green, and Blue]. In addition, the neurons of a layer connect only to a small region of the next layer, and not to all his neurons. Finally, the result will be reduced to a single probability score vector, organized according to the depth dimension.

a. Characteristics extraction

One of the main building blocks of a CNN is convolution, that means, the mathematical combination of two functions to produce a third function (it merges two sets of information).

In the case of a CNN, convolution is performed on the input data using a filter or kernel, where it will slide across the entire image creating new values.

As shown in Figure 3, at the beginning of the convolution, the convolution filter will be positioned at the top left of the image and then shifted by a certain number of boxes (this is what the we call the step) to the right and when it arrives at the end of the image, it will shift one step down and so on until the convolution filter goes through the whole image.

Some intermediate filters reduce the resolution of the image by a local maximum operation. In the end, the convolution maps are laid flat and concatenated into a feature vector, called the CNN code.

The steps for detecting the contexts of the images in a video is represented as follows:

1. The convolution layer (CONV) that processes the data of a receiver field.

2. The pooling layer (POOL), which compresses information by reducing the size of the pool by the intermediate image (often by sub-sampling).

3. The correction layer (ReLU), often abusely called'ReLU' in reference to the function activation (Linear grinding unit).

4. The "fully connected" (FC) layer, which is a perceptron type layer.

5. The loss layer (LOSS).

The convolution filter will be positioned at the very top left of the image, then it will shift a number of squares (this is called the step) to the right and when it reaches the end of the image, it will shift one step down and so on until the convolution filter is scanned the entire image.

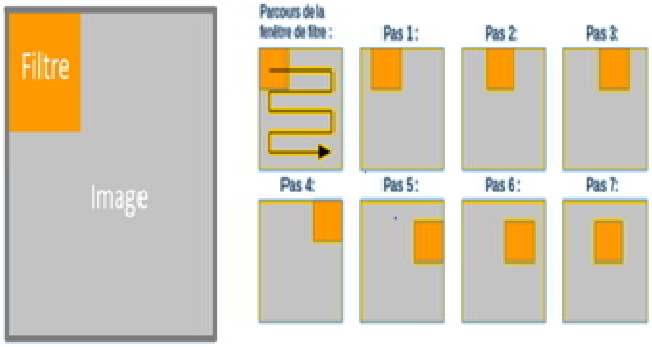


Figure 3: Example of a filter

For each filter position, the values of the two overlapping matrices (filter and image to be processed) are multiplied. Each value thus inferred is projected into a new matrix. This matrix represents a new image that highlights the characteristics sought through the filter. The image in Figure 4 below shows an example of a calculation. The values of the image to be processed are abnormally small, but this is just to understand more easily the calculation made.

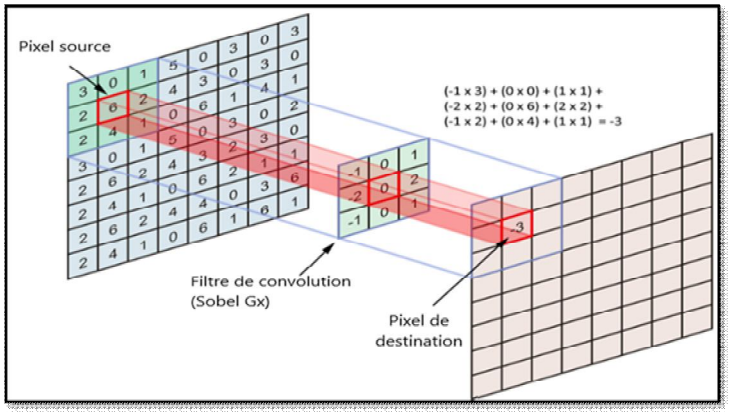


Figure 4: Convolution example

Some intermediate filters reduce the image resolution by a local maximum operation. In the end, the convolution cards are flattened and concatenated into a vector of characteristics. Two of the most common pooling operations are maximum and average pooling. Max-pooling selects the maximum of values in the region of the input characteristics map of each step and pools the average value of the values in the region. The result of each step is therefore a single scalar, which results in a significant reduction in the size of the output.

Pooling is an important process in a convolution network. By extracting important values from pixels, it allows to reduce an image while keeping the relevant characteristics. The most commonly used method is "Max Pooling". It consists in reducing the image by keeping the largest values of the pixels. To do this, we have a tile that moves (like a filter)

on the surface of our image. At each position of the tile, the highest value is extracted and retained only that one. This produces a new
image with only the remarkable values of the image. The image in figure 5. below shows an example of Pooling. The tile here has dimensions of 3 by 3. The 9 by 9 pixel image is reduced to a 7 by 7 pixel image.

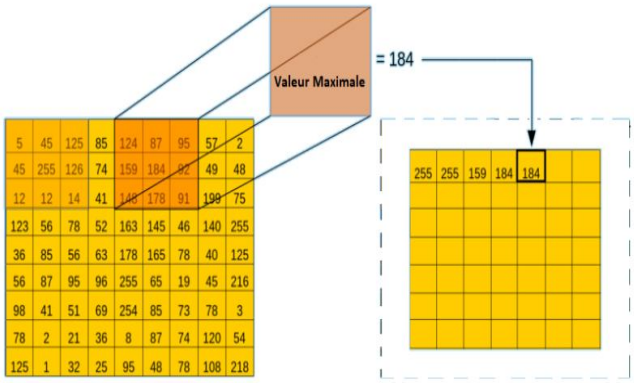
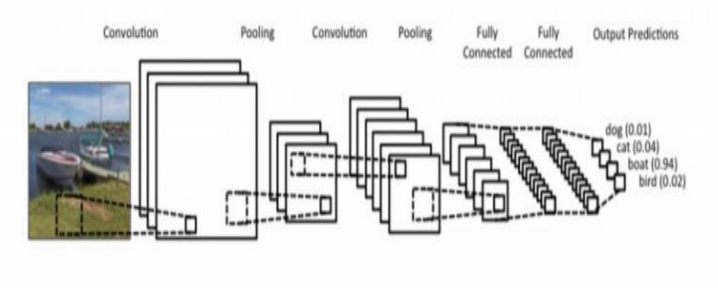


Figure 5: Example of the pooling step

b. *Classification*

This CNN code at the output of the convolutional portion is then connected to the input of a second portion, consisting of fully connected layers (multilayer perceptron) which will serve as a classifier for this CNN code. In another way, the role of this part is to combine the characteristics of the CNN code to classify the image and to deduce its context. The output is a final layer with one neuron per category. The numerical values obtained are generally normalized between zero and one, of sum 1, to produce a probability distribution on the categories.

During this step, we will keep the category with more



probability that represents the context of the image.
As shown in Figure 6 convolutional neural networks

Figure 6: Standard architecture of a convolutional neuron network

4.3. Step 3: Video classification

During this method, we are based on the image's context extracted from the video to deduce if it represents a spam video or not and finally prohibit the user from publishing it if this is the case.

Since online social network users, as the case for Facebook, have the opportunity to publish their videos either by sharing it in their profile page or even as a response to a publication of a friend or others, so the 3rd step which represents the classification, will be done according to the context that characterizes the publication of this video.

a) Sharing a video

When a user tries to publish a video using online social networks, that means sharing it with his friends or others from his profile page, all the contexts of the images extracted in the first 2 steps will be filtered, so that as soon as we detect that a context of one of the images in this video is sensitive "that means representing a pornographic video", the whole video will be considered as spam.

The figure 7 show when a video published as an opening publication.
the contexts of the images in a video must be approximately similar to designate a legitimate video. if this is not the case, the probability of contexts is less than 50% and the video will define spam.

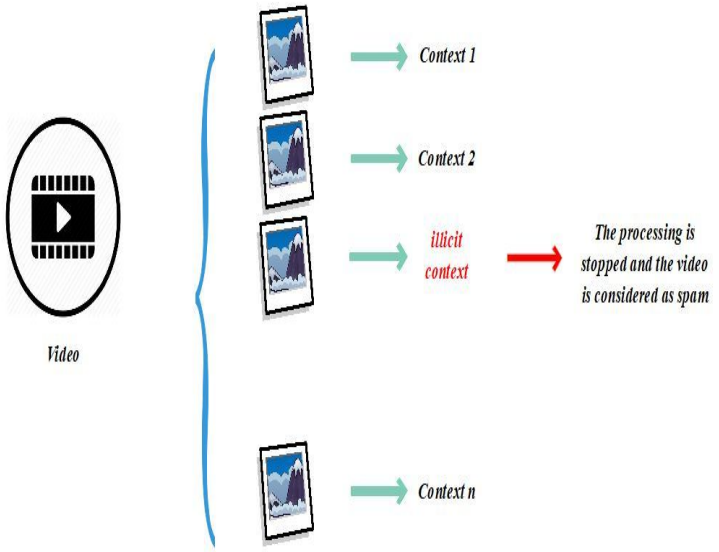


Figure 7: Filtering a video when it is published as an opening publication.

b) Video response

As shown in Figure 7, when a user attempts to publish a video as a response to a publication "whether it is a text paragraph, image or a video", the contexts of the images extracted in the first two steps will be used to filter this video following 2 steps:

- **Step 1: Researching an illicit context**

As illustrated in Figure 8, as soon as it is detected that a context of one of the images of the video that the user wishes to publish as an answer is sensitive "that means representing a pornographic video", the whole video will be considered as spam.

Step 2: Comparison with the opening publication context

As soon as the video surpasses the first step, that means that this video is not a sensitive content, it will be in front of a second test. The purpose of this test is to verify if there is a

match between the content of the video that the user wishes to publish as a response with the opening publication.

We consider that if the context of the opening publication represents more than 50% of the content of the response video, the response video will not be considered as spam unless if they are similar (the user tries to publish the opening video as video response).

Figure 9 shows the steps and the execution process of our system to detect spam videos.

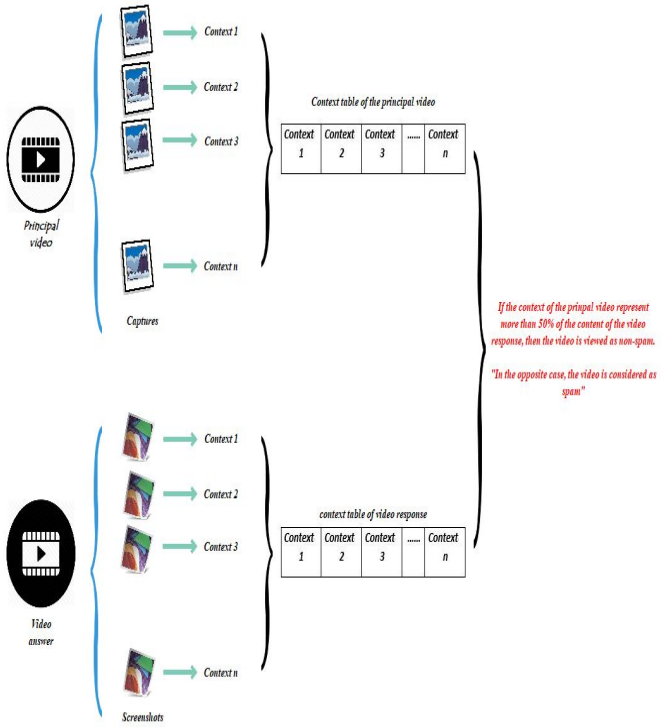


Figure 8: Filtering a video when it is published as a video response.

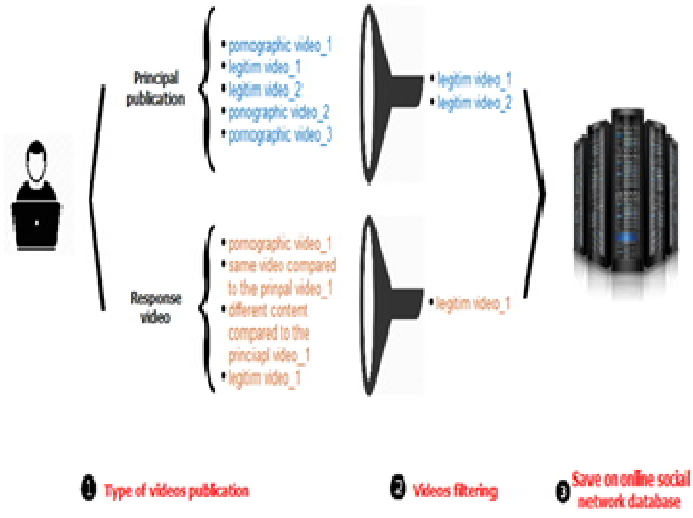


Figure 9 : Architecture of the proposed system

5. EXPERIENCES AND RESULTS

The submitting author is responsible for obtaining agreement of all coauthors and any consent required from sponsors before submitting a paper. It is the obligation of the authors to cite relevant prior work.

Authors of rejected papers may revise and resubmit them to the journal again.

a) Data and protocol

In the test phase, we used the Tensorflow framework which allows us to use the GoogLeNet Inception API to learn images.

the application of our contribution on a GoogLeNet Inception dataset allows training and context detection of images between publishing videos and response videos.

the GoogLeNet Inception database contains almost all types of images.

As shown in the table 1 below, the performance of our system has been tested based on 2 experiments, where each of these experiences represents a category:

• **Experience 1:** Comparison of opening publications (text paragraphs, images and videos) with the response videos, where their contents are the same.

• **Experience 2:** Compare each of the opening publications (text paragraphs, images and videos) with the response videos, where their content is not the same.

Table 1: Summary of collected data

<table>
<tr><th colspan="2">Experiences</th><th colspan="2">Number of videos</th><th>Feature</th></tr>
<tr><td colspan="2">Sensitive content</td><td colspan="2">7000 sensitive videos</td><td rowspan="8">GoogLeNet Inception</td></tr>
<tr><td rowspan="4">Experience 1</td><td rowspan="4">Principal publications and response videos share the same content</td><td>Principal publication</td><td>Video answer</td></tr>
<tr><td>30 text paragraphs</td><td rowspan="3">80 videos</td></tr>
<tr><td>30 images</td></tr>
<tr><td>30 videos</td></tr>
<tr><td rowspan="4">Experience 2</td><td rowspan="4">Principal publications and response videos do not share the same content</td><td>Principal publication</td><td>Video answer</td></tr>
<tr><td>30 text paragraphs</td><td rowspan="3">80 videos</td></tr>
<tr><td>30 images</td></tr>
<tr><td>30 videos</td></tr>
</table>

b) Results

Experience 1 : As shown in the result of one of the first experiment in Table 2, during this experiment, we relied on 3 categories of media that represents the opening publication (i.e. text paragraphs, images and videos) and whose content of these 3 categories is the same "use of flowers".

Regarding the videos database that we considered as an answer, it contains 80 videos whose content is also the same "use of flowers as context" whereas these videos are distinct (this means that there is no duplication of any of the videos at this database level)

Each type of the opening publication will be compared with the answer videos, this means that during this experiment, we will do 7200 tests (30 text_paragraphs * 80 videos_response + 30 images * 80 videos_response + 30 videos * 80 videos_response = 7200 tests) to get the result.

The results of this experiment are illustrated in figure 10.

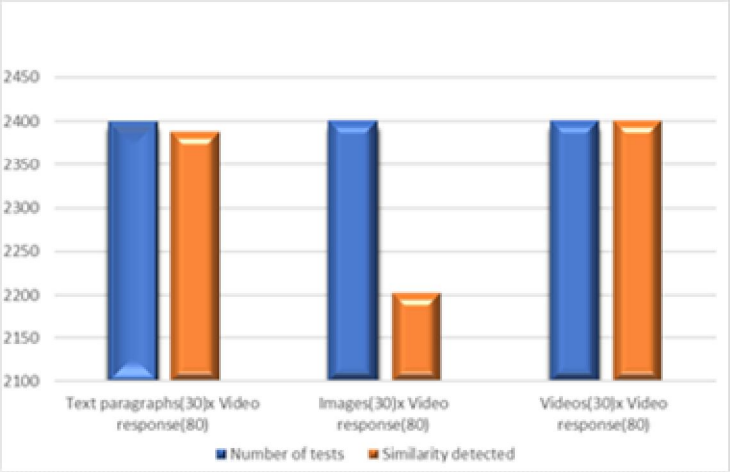


Figure 10: Resultat of experience 1

Experience 2: As shown in the result of one of the second experiment in Table 2, during this experiment, we also relied on three categories of media that represents the opening publication (i.e. text paragraphs, images and videos) and whose content of these three categories is the same "use of flowers". Regarding the videos database that we considered as an answer, it contains 80 videos whose content is not the same as the opening publication content.

Each type of the opening publication will be compared with the answer videos, this means that during this experiment, we will do 7200 tests (30 text_paragraphs * 80 videos_response + 30 images * 80 videos_response + 30 videos * 80 videos_response = 7200 tests) to get the result. The results of this experiment are illustrated in Figure 11.

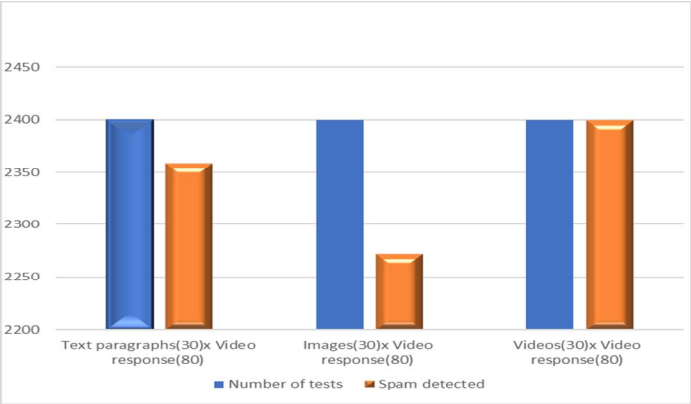


Figure 11: Result of experience 2

The Table 2 represents the results of the experiments performed by our proposal to detect videos according to their image context.

We tested two cases, when the contexts are similar and when the contexts of the videos are not similar. Our contribution shows that the detection of image contexts in a video gives good results on both cases. The proposal considered all videos that share similar content as legitimate videos, and videos with a different context as spam videos.

A spam video is a video that contains a context far from the context of opening publication, even if there are no pornography videos, videos with a context that does not have a relationship with the opening publication that can be a text, image, link or video publication.

Our proposal approach detects videos with a similar context according to the probability of similarity which must be 50%>, and in the case of non-similarity the system considers videos as non-spam according to the calculated probability which equals 0%.

Table 3 shows the performance of our system, which focuses on the detection of spam videos in social networks. Through this experience, we have concluded that we can achieve an accuracy of 0.99% when detecting spam videos, whether during their upload as an opening publication or their publications as video response.

Table 3: Detection accuracy of each experiment

Experience	*Accuracy*
1	*0,98%*
2	*0,99%*

6. PROTOTYPE OF PROPOSED SOLUTION "SPAMVIDEOSDETECTOR"

At this stage, after having described the main lines and steps of the proposed approach in the security side, it was necessary to develop it in the form of an application. It is true that it is difficult to decide on the effectiveness of our approach without exploring this part, which is decisive in the validation and approval of the subject, hence the importance of properly describing the work environment. In this section, we discuss the various details related to the implementation and development of our approach. We illustrate, by screenshots, the description of the work done. We developed our solution while using java language in the eclipse environment. In addition, the Tensor Flow framework which' is an open source automatic learning tool developed by Google

Figure. 12 Prototype of proposed solution "SpamVideosDetector

Our proposed solution "SpamVidéosDetector" allows you to check if a video represents spam video. The figure 12 shows the interface that makes the extraction of images and context detection of a video. This interface allows you to compare the two opening and response videos to detect the context of each video. The figure 12 shows the prototype of proposed solution for detecting spam video in social network.

The user has the possibility to compare all types of video including pornographic videos that are considered as spam in social networks. When the opening video has a context for example "flowers" and the response video contains 50% context probability of the opening video, our solution considered this video as non-spam. Moreover, in the case where the response video has a 50% lower probability of context of the opening video our solution treats the video as spam.

This solution is based on context comparison while using the convolutional neural network algorithm. However, the application of our proposal "SpamVideosDetector" has given good results on videos. The following figure 13 shows the percentage of correspondence between two videos.

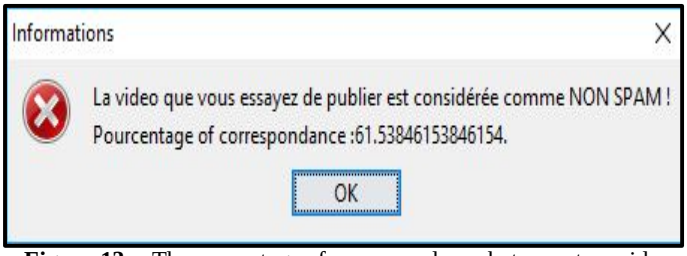


Figure 13 : The percentage of correspondence between two videos

7. COMPARISON WITH OTHER PROPOSALS

Researchers to find out spam videos in various online social networks have used different techniques. In this section, we compare our method to three existing techniques already presented in the third section of this article allowing the detection of spam videos, whether during their upload as an opening publication or their publications as video response. Table 3 is showing the summary of the papers presented in the third section « Related work » as well as ours.

Table 3 : Outline of techniques used for the detection of spam videos

Title	Metrics based on	Data used	Accuracy
Understanding Video Interactions in YouTube.	User behavior	3,436,139 of top 100 videos in the social network YouTube.	80%
Identifying Video Spammers in Online Social Networks	User rank	3,436,139 of top 100 videos in the social network YouTube.	87%
Spam videos detection in social network using deep learning.	Images extracted from video.	Experience 1: 110 videos, 30 photos and 30 text paragraphs. Experience 2: 110 videos, 30 photos and 30 text paragraphs.	98.75 %

Spam videos detection in social network using deep learning. Images extracted from video. Experience 1: 110 videos, 30 photos and 30 text paragraphs.

Experience 2: 110 videos, 30 photos and 30 text paragraphs.

98.75%

Our proposed method using convolutional neural networks performed better than all current works in terms of accuracy, it was about 98.75%, the first method was 13.8%, and the second one was 80% while the third one was 87%.

From the results obtained, we can point out that with the convolutional neural networks method; we have the chance to detect more video spammers than with other traditional methods, and why not trying in our future work to apply a combination of this method in order to improve the detection of spam videos.

Table. 2: Summary of the experiments results

Experiences	**Video's content context**			**Probability**	**Spam classification**
Principal publications and response videos share the same content	**Frames of principal video = 21**		Frames of video response = 13	61.538%	Legitimate
	• Nematode • Yellow • Yellow • Bee • Butterfly • Ear • Chambered • Candle • Cabbage • Daisy • Jellyfish • Ear	• Rapeseed • Bee • Cardoon • Cabbage • Daisy • Coral fungus • Matchstick • Cauliflower • Book jacket	• Nematode • Sea anemone • Daisy • Coral fungus • Brassiere • Velvet • Daisy • Hip • Bee • Daisy • Kimono • Daisy • Nematode		
• Principal publications and response videos do not share the same content	• Frames of principal video = 12		• Frames of video response = 13	0%	Spam
	• Hammerhead • Scuba diver • Triceratops • Hammerhead • Great white shark • Hammerhead • Killer whale • Hammerhead • Hammerhead • Scuba diver • Sea lion • Lotion		• Nematode • Sea anemone • Coral fungus • Brassiere • Velvet • Daisy • Hip • Bee • Daisy • Kimono • Daisy • Nematode		

8. CONCLUSION

Social networks provide easy-to-use user experience thanks to its architecture. The thing that attracts the attention of spammers who post contents « for example: spam videos ».

Since some social networks like Twitter, has unique characteristics from email services and websites, traditional spam-filtering methods are not able to detect all spam videos in these platforms. Thus, a more robust spam video detection approach, which is specially designed for these platforms, is needed in order to provide a spam-free environment.

CNNs are particularly useful for image classification and recognition. They have two main parts: a feature extraction part and a classification part. The main technique in CNN is convolution, where a filter slides over the input and merges the input value and the filter value on the feature map. Our goal is to use CNN to have a probability for the displayed object and that thanks to this description; we manage to filter the videos that represent spam. Our future work will be to apply a hybrid method, this means, a combination of our method and others to improve the detection of spam videos in online social networks.

REFERENCES

1. Radhika Bhagat et al,(2017)**Privacy and Security Issues in Social Online Networks**, International Journal for Innovative Research in Science & Technology, pp 130-134.
2. Prateek Joshi, C. –C. Jay Kuo, (2011) **security and privacy in online social networks: a survey**, 2011 IEEE International Conference on Multimedia and Expo, Barcelona, Spain. https://doi.org/10.1109/ICME.2011.6012166
3. P. Sai Kiran , (2015)**Detecting spammers in YouTube: A study to find spam content in a video platform, Journal of Engineering** (IOSRJEN), Vol. 05, Issue 07 PP 26-30.
4. Fabricio Benevenuto et al,(2008) **Identifying Video Spammers in Online Social Networks**, International Workshop on Adversarial Information Retrieval on the Web(AirWeb'08),Beijim, China. https://doi.org/10.1145/1451983.1451996
5. A. Zinman and J. Donath.(2007) **Is britney spears spam?** In Proc. of CEAS, The Fourth Conference on Email and Anti-Spam, Mountain View, California, USA.
6. P. Heymann, G. Koutrika, and H. Garcia-Molina (2007). **Fighting spam on social web sites: A survey of approaches and future challenges**. IEEE Internet Computing, 11(6):pp36–45, https://doi.org/10.1109/MIC.2007.125
7. Fabricio Benvenuto ,(2008) **Understanding Video Interactions in YouTube**, MM'08, Vancouver, British Columbia, Canada.
8. Margaret M. Fleck, David A. Forsyth and Chris Bregler,(2005) **Finding Naked People**, Lecture Notes in Computer Science, Berlin, Heidelberg.
9. Rossotti, Hazel (1983) Colour: **Why the World isn't Grey**, Princeton University Press, Princeton, NJ.
10. Shailendra Rathore et al,(2017), **Social network security: Issues, challenges, threats, and solutions, Information Sciences**,pp43–69. https://doi.org/10.1016/j.ins.2017.08.063
11. 1B. Manoj, K.V.K.Sasikanth, M.V.Subbarao, V Jyothi Prakash, **Analysis of Data Science with the use of Big Data,** International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No.6, Pp-87-90, 2018. https://doi.org/10.30534/ijatcse/2018/02762018
12. Priyanka Thakur, Dr. Rajiv Shrivastava, **A Review on Text Based Emotion Recognition System,** International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No.5, Pp-67-71, 2018. https://doi.org/10.30534/ijatcse/2018/01752018