Student's Video Clip Collusion Detection: the next generation of collusion detection

ANTHONY HERBLAND University of Hertfordshire
JOHANN SIAU University of Hertfordshire

Abstract This paper describes how an offline software tool identifies collusion on assessed video clips. The collusion detection processing is independent of the length, format, frame rate, compression and content of the video clips. The process consists of extracting prominent features from individual frames for each student's video clip and passing these through a rigorous comparison process. Collusion is identified when the software detects similar features when comparing these clips. A summary of results will be presented and the application will then allow users to view the colluded video via a graphical user interface. This paper also explains how this tool can enhance the learning and teaching when used as a deterrence tool. A software demonstration will be presented to multimedia students at the start of the academic year. Statistics have shown that students who are aware of the capability of modern collusion detection software will normally be driven to complete their coursework on their own. The collusion detection tool can also be used in research, where further investigations could be carried out to report on the performance of the detection process.

Introduction

Student plagiarism and collusion is prominent in the higher education sector. The existing plagiarism and collusion detection solutions are text-based detection. The detection process carries out electronic comparison of students' work against electronic text sources from the internet and other students only. With the growing demand of multimedia courses, it becomes necessary to verify that students' work is genuine and therefore to create appropriate tools to detect any form of plagiarism.

Description

Collusion is a specific type of plagiarism and falls within the definition of academic misconduct which is provided under the University Policies and Regulations (UPRs). It is defined as "evidence of the representation by an individual of work which he or she has undertaken jointly with another person as having been undertaken independently of that person".

Student plagiarism and collusion are a long-lasting problem in higher education. Existing plagiarism and collusion detection tools are based on

textual information only. The text-based detection process carries out electronic comparison of students' work against electronic text sources from the internet and other students. With the growing demand of multimedia courses, it becomes necessary to detect plagiarism on the students' multimedia coursework. This project developed a software tool for identifying collusion on assessed video clips. The detection method which is described here addresses only collusion, in which student A submits an assessed video clip wholly or partly copied by student B, and submits it as his/her own. For this reason, the underlying assumption is that all of the source material that need be examined is directly available in the form of the students' submissions.

Video Collusion Detection

The software project has been divided into three distinctive parts: file preparation, processing of the detection algorithm and display as shown in Figure 1.

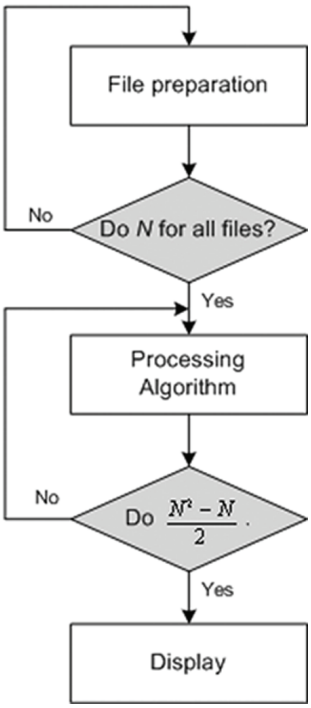

Figure 1 Software flowchart

File Preparation
The first part, file preparation, consists of counting the number of video clip submissions in a file pool folder and extracting information from the header of each video clip such as the length and resolution.

Processing Algorithm
Due to the large amount of data contained in a video clip, it is essential to retain a fraction of the information for each frame, also called *features*.

Feature Extraction
Before performing frame comparison between frames from different sources, the block preparation is carried out. This process consists of dividing a frame into a set of B $\times$ B blocks. The initial approach is to retain the average for each block in the frame by applying (1).

$$F(a,b) = \frac{1}{B^2} \sum_{x=1}^{B} \sum_{y=1}^{B} f(x,y) \tag{1}$$

Once the process above is completed, the results are contained in a matrix *F(a,b)* and this process is replicated for all the other frames of the clips. After the feature extraction process, the comparison process on a frame-by-frame basis is carried out on all the video clips.

Comparison process
The initial approach consists of comparing individual frames by measuring the absolute difference between the corresponding blocks as shown in Figure 2.

100	110	120	…
159	148	137	…
160	170	180	…
…	…	…	…

$F_1(a,b)$

-

101	112	123	…
160	150	140	…
161	172	183	…
…	…	…	…

$F_2(a,b)$

=

1	2	3	…
1	2	3	…
1	2	3	…
…	…	….	…

$D(a,b)$

Figure 2 Frame feature comparison process

Once all the absolute difference values are calculated between two frames of two different video clips, the mean of the resulting matrix is computed using (2).

$$\text{Mean of the absolute difference block} = \frac{1}{A \times B} \sum_{a=1}^{A} \sum_{b=1}^{B} D(a,b) \qquad (2)$$

Where: A is the number of blocks on the x-axis and
B is the number of blocks on the y-axis

Equation 2 is then computed to all the absolute difference blocks and the resultant is shown Figure 3.

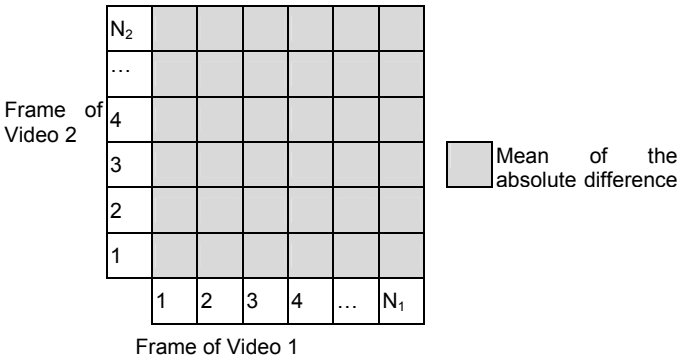

Figure 3 Matrix containing the mean of the |difference| between 2 frames

The lowest these values are, the most likely collusion is. The matrix values are then formatted into percentage values.

A thresholding transformation (3) is applied on the resulting matrix as follows.

$$t(i,j) = \begin{cases} 1, & \text{for } d(i,j) \geq T \\ 0, & \text{for } d(i,j) < T \end{cases} \qquad (3)$$

Where T is the threshold, $t(i,j) = 1$ for colluded video and $t(i,j) = 0$ for non-colluded video

If the values in the resulting matrix are above a predefined threshold value *T*, this means that two frames from different sources are identical. Therefore, video clip collusion can be detected using this detection process. The result of the comparison process is contained in a log table. For every collusion detected the timecode of the two video clips is recorded.

Display

Table 1 shows an example of a collusion log table. It is noted that each video clip is used as reference. A video clip can be colluded with several video clips

(i.e. VC1 with VC3 and VC5). There may be many incidences of collusions such as the Timecode1 and the Timecode2 between VC1 and VC3. Each timecode is recorded with its start and end points; and also the confidence level of collusion (1: low confidence to 5: strong confidence).

Table 1 Collusion log table

Reference clip			Comparison clip				
VC1	Timecode11-S	Timecode11-E	VC3	Timecode31-S	Timecode31-E	2	►
	Timecode12-S	Timecode12-E		Timecode32-S	Timecode32-E	4	►
	Timecode13-S	Timecode13-E	VC5	Timecode51-S	Timecode51-E	3	►
	Timecode14-S	Timecode14-E		Timecode52-S	Timecode52-E	5	►
	Timecode15-S	Timecode15-E		Timecode53-S	Timecode53-E	5	►
VC3	Timecode31-S	Timecode31-E	VC1	Timecode11-S	Timecode11-E	1	►
	Timecode32-S	Timecode32-E		Timecode12-S	Timecode12-E	1	►
VC5	Timecode51-S	Timecode51-E	VC1	Timecode13-S	Timecode13-E	5	►
	Timecode52-S	Timecode52-E		Timecode14-S	Timecode14-E	5	►
	Timecode53-S	Timecode53-E		Timecode15-S	Timecode15-E	3	►
	Timecode54-S	Timecode54-E	VC7	Timecode71-S	Timecode71-E	5	►

The ► symbol indicates that the user can play simultaneously two colluded videos from two different sources as shown Figure 4.

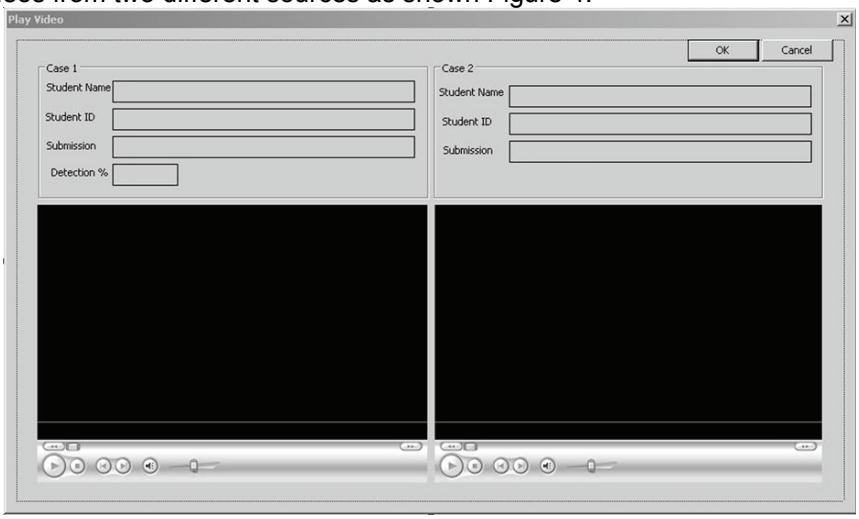

Figure 4 Graphical interface with dual display

Experimental results

For experimental purposes, two video clips are used with a resolution of 320 by 240. The block size is experimentally set to 32. The first clip is manipulated in such way that a part of the second clip is inserted as shown in Figure 5. The video part from frame 200 to frame 335 is identical for both clips.

Figure 5 Video sequences for both experimental video clips

After computing the detection algorithm, the matrix containing the mean of the absolute difference between 2 frames is obtained. The corresponding graph of the matrix is shown Figure 6.

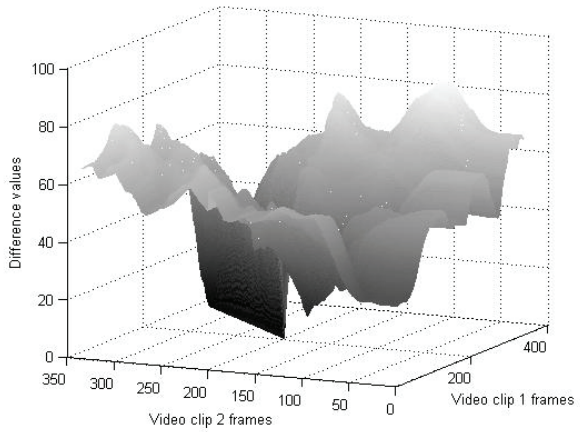

Figure 6 Mean of the absolute difference between both clips

In Figure 6, it can be seen that the darkest line is shown between the frame range [200, 335] for both video clips. This line indicates that both videos are identical for this particular range.

Figure 7 shows the graph of the same matrix after converting into a percentage scale. This graph confirms that there is 100% confidence that the video 1 frames are identical with the video 2 frames for the interval [200, 335]. Figure 8 shows the graph (Figure 7) in 2 dimensions stressing the identical frames between both video clips.

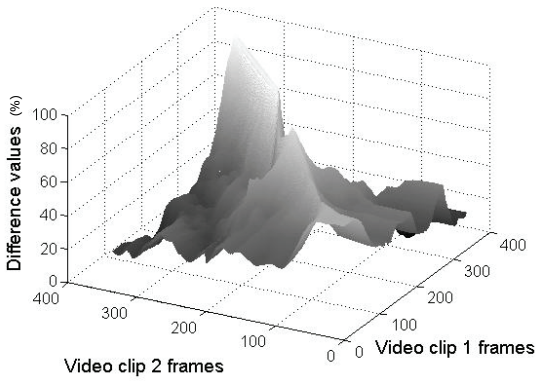

Figure 7 Mean of the absolute difference between both clips in percentage

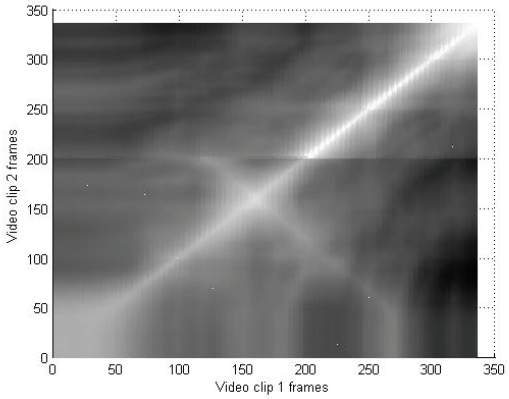

Figure 8 Mean of the absolute difference between both clips in 2-D

With an experimental binary threshold T set to 95%, the matrix shown in Figure 9 becomes a 2-D B&W matrix results. As expected from the clear white line (Figure 8), the segmentation between colluded and non-colluded parts is very effective.

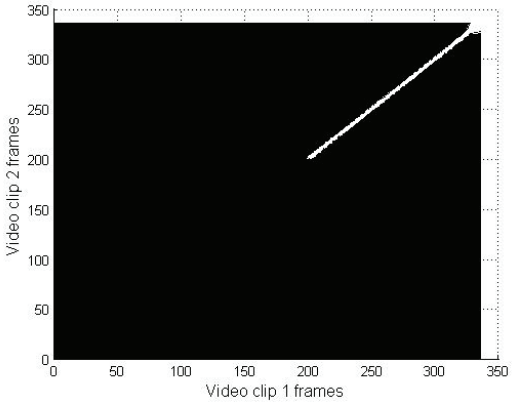

Figure 9 Resulting matrix after a 95% thresholding

The colluded timecode is simply extracted from Figure 8 by determining the x and y axis coordinates of the white line. The final result is stored in the log collusion table as shown Table 2.

Table 2 Log table

Reference clip			Comparison clip			
VC1	00:08:00	00:13:10	VC2	00:08:00	00:13:10	►
VC2	00:08:00	00:13:10	VC1	00:08:00	00:13:10	►

The same process must be ran $\frac{N^2 - N}{2}$ times with N being the number of submitted video clips.

Deterrence

Deterring will always be more effective than detecting once it occurs (Carroll). To deal with student plagiarism, the Joint Information Systems Committee (JISC) was launched and funded by the Plagiarism Advisory Service in 2001 (Carroll 2004). Electronic detection is probably the most suitable response to a problem caused by technology. The UK HE and FE institutions have adapted Turnitin UK software. The main advantage from the use of Turnitin is a significant increase in student awareness of plagiarism issues. A study conducted by Savage (2004) concluded that Turnitin is thought to be most useful as a deterrent rather than as a solution to Internet-assisted plagiarism. She also added that students considered fear of detection to be a significant deterrent. Like Turnitin, this project also had the intention of deterring the students from plagiarising.

Conclusion

The video clip detection process has been discussed in detail. The frame-based detection algorithm has produced good results. Further research is required to measure the effectiveness of the collusion detection on videos with different parameters (i.e. encoding type, resolution and frame rate). The primary objective of this software tool is not only to detect and punish. It will be also used to deter this type of plagiarism.

References

Carroll, J. (2004) Institutional issues in deterring, detecting and dealing with student plagiarism, JISC, Available: http://www.jisc.ac.uk [Accessed 23 May 2007]

Carroll, J (2005) Deterring, Detecting and Dealing with Student Plagiarism, JISC, Available: http://www.jisc.ac.uk [Accessed 23 May 2007]

Savage S. (2004) Staff and Student Responses to a Trial of Turnitin Plagiarism Detection Software in *Proceedings of the Australian Universities Quality Forum*.

UPR ASAS/C/6.2 - Appendix I (2006) Assessment and Examinations – Regulations, University of Hertfordshire. (Internal document)

Biographies

Anthony Herbland is a lecturer at University of Hertfordshire. He has interest in applied technology in learning and teaching. Email: a.j.m.herbland@herts.ac.uk.

Johann Siau is a Senior Lecturer and Faculty Blended Learning Champion at the University of Hertfordshire. He has been developing web applications and applying the technology in learning and teaching.