# Development of a Video Tampering Dataset for Forensic Investigation

**Article** *in* Forensic science international · July 2016

DOI: 10.1016/j.forsciint.2016.07.013

Ahmed Abdullah Ahmed

Kurdistan Technical Institute

**2** PUBLICATIONS **1** CITATION

SEE PROFILE

Ghazali Sulong

Universiti Teknologi Malaysia

**137** PUBLICATIONS **384** CITATIONS

SEE PROFILE

Forensic Science International 266 (2016) 565–572

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

# Development of a video tampering dataset for forensic investigation

Omar Ismael Al-Sanjary[a,*], Ahmed Abdullah Ahmed[b], Ghazali Sulong[a]

[a] MaGIC-X (Media and Games Innovation Centre of Excellent), Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310 Johor Bahru, Malaysia
[b] Department of Computer Science, Kurdistan Technical Institute, Sulaimani Heights Sulaymaniyah/Kurdistan Region, Iraq

ARTICLE INFO

*Article history:*
Received 4 November 2015
Received in revised form 25 June 2016
Accepted 9 July 2016
Available online 25 July 2016

*Keywords:*
VTD
Video investigation
Forgery
Splicing
Swapping-frame
Copy–move

ABSTRACT

Forgery is an act of modifying a document, product, image or video, among other media. Video tampering detection research requires an inclusive database of video modification. This paper aims to discuss a comprehensive proposal to create a dataset composed of modified videos for forensic investigation, in order to standardize existing techniques for detecting video tampering. The primary purpose of developing and designing this new video library is for usage in video forensics, which can be consciously associated with reliable verification using dynamic and static camera recognition. To the best of the author's knowledge, there exists no similar library among the research community. Videos were sourced from YouTube and by exploring social networking sites extensively by observing posted videos and rating their feedback. The video tampering dataset (VTD) comprises a total of 33 videos, divided among three categories in video tampering: (1) copy–move, (2) splicing, and (3) swapping-frames. Compared to existing datasets, this is a higher number of tampered videos, and with longer durations. The duration of every video is 16 s, with a 1280 × 720 resolution, and a frame rate of 30 frames per second. Moreover, all videos possess the same formatting quality (720p$^{HD}$.avi). Both temporal and spatial video features were considered carefully during selection of the videos, and there exists complete information related to the doctored regions in every modified video in the VTD dataset. This database has been made publically available for research on splicing, Swapping frames, and copy–move tampering, and, as such, various video tampering detection issues with ground truth. The database has been utilised by many international researchers and groups of researchers.

## 1. Introduction

Often causing indignation on social media networks, including Facebook, Twitter, Yahoo, and YouTube, there are an infinite number of communities throughout the world who continuously manipulate daily media and other sites they want you to visit. There is a multitude of videos online being continuously uploaded or downloaded to and from YouTube at the rate of about 65,000 videos per day [1]. Our daily lives are now mostly dominated by digital media, and consequently, this has led to exposure to digital forgery attacks [2]. Advanced and cost-effective camcorders and digital cameras, along with upgraded high-quality tools for data processing algorithms, are now readily available to simplify video acquisition and forgery procedures. Moreover, a forger's primary aim is to develop a manipulated, doctored, or copied video of an original one.

With numerous sophisticated video editing tools readily available, this has provided an easy platform for forgers to manipulate real videos and create perceptually indistinguishable fake ones. This great assistance from video editing tools makes the manipulation process easier for forgers, and at the same time, it has become difficult to detect modified videos. Moreover, a single video (single source), or multiple videos (various sources), can be tampered [3]. This has consequently led to the requirement to verify online videos. Furthermore, media societies have been greatly impacted by the incessant growth of the video tampering business. To date, very few forgeries of digital videos have been fully exposed to the public; resulting in public trust drifting a long way because of such videos. Therefore, it is a good time for scientists to rapidly develop an effective approach to distinguish non-modified videos from their fake counterparts.

Videos are usually tampered with using two techniques: passive-blind video tampering detection and active video tampering detection [3]. Passive-blind methods are effective on three types of forgery, including cloning (such as duplicated region and

[*] Corresponding author.
*E-mail addresses:* alsanjaryomar@gmail.com, omis.golden.oasis2@gmail.com (O. Ismael Al-Sanjary), Ahmed.Abdullah@kti.edu.krd (A.A. Ahmed), ghazali@utmspace.edu.my (G. Sulong).

http://dx.doi.org/10.1016/j.forsciint.2016.07.013
0379-0738/© 2016 Elsevier Ireland Ltd. All rights reserved.

copy–move tampering) of framed objects, swapping frames, and splicing [4,5]. As previously mentioned in the literature on digital forensics, passive-blind methods play a significant role in independently verifying and guarding original digital content, and relative complexity lies in yielding a generic series of test data sufficing acceptable parameters with regards to each digital forensics task [6]. Data from various sources can only efficaciously test particular algorithms associated with device identification. Similarly, both original, untouched data and tampered test data play important roles in detecting authorized algorithms. Utilization of an anomaly identification associated task can assist other forensic tasks when applied to both untainted and tampered data.

Therefore, every type of digital image tampering process is encompassed by a forged image dataset so that researchers are able to obtain the opportunity of assessing the applied detection methods, and, subsequently, three standard image sets have become freely available: (1) Dresden image database [6], concentrating mainly on integrity substantiation and camera identification; (2) CASIA [7], an image dataset with rendering of forged images; and (3) Uncompressed Image Database (UCID) [8], which contains 1338 uncompressed images.

More challenges lie in digital video forensics than in digital image forensics. Presently, there are numerous algorithms to deal with various types of forgeries, as reported in the literature [2,9,10]. However, dependable test data falls short as all types of video modification are not encompassed by the existing datasets, such as SULFA [10]; the design and development of the database is on the basis of the movement of one object, and only copy–move tampering is covered by it, since a static camera captured this dataset. Additionally, to the best of the author's knowledge, splicing forensics are not available in any of the existing datasets. Lastly, good quality data are acquired by most researchers with regards to a particular task. However, in terms of a standardized dataset, this has not yet been compiled.

This shortage of reliable data for video investigation of forensic algorithms has made the design and development of a new video library crucial. The main objective of developing the VTD dataset isto help researchers by providing them with the opportunity to use a database in this field, and to prepare a comparative study on the outcome of video forensic detection algorithms. YouTube is the main source from which the new video dataset was compiled. Moreover, in the selection of the videos considered, the scenario was that the actual videos contain significant spatial and temporal features found in typical videos. There are a total of 33 videos in the VTD dataset, and only seven among the total have not been tampered with so that they can be used to verify the ability of systems to identify original videos. The three tampered categories consist of a group of 10 videos that have been manipulated by copy–move methods, a group of six videos by the swapping frame methods, and a group of 10 videos by the applied splicing methods.

The structure of this paper comprises Sections 2–5, containing a literature review in association with building databases on video tampering, types of video tampering, outline of the process of video tampering, the ground truth of the composed dataset, and conclusions, respectively.

## 2. Related work

Any research work essentially requires the availability of datasets. Unfortunately, there are limited resources in the statistics of available digital video datasets [10–15]. The majority of researchers have evaluated their methods by recording and gathering videos individually. A new video tampering dataset has been created since relatively few videos are included in most of the existing datasets. These datasets do not include video splicing examples, and, as such, all types of video tampering containing objects copied and pasted from various sources, as well as the use of a static camera, which is easily recognized compared to a dynamic camera for malicious tampering. The number of frames, video duration, camera type, video source, and tampering type are limited in the present modified videos dataset. Table 1 summarises several important video tampering databases, as well as their important features.

**Table 1**
Summary of notable video forgery databases.

| Author's | Number of video | Video length | Video source | Static/dynamic camera | Type of video | Remark |
|---|---|---|---|---|---|---|
| [10] | 10 video = 30 fps | 10 s shot | 1—Canon SX220<br>2—Nikon S3000<br>3—Fujifilm S2800HD | Static camera | Copy–move | SULFA dataset does not cover all the kind of video tampering utilizing just a fixed camera |
| [12] | 7 video = 25 fps | N/A | SONY DSCP10 | Static camera | Copy–move object | Video tampering of this dataset has been done based on one objects movement and has a little video source. There is no ground truth of this dataset to show the important information such as video length and number of frames |
| [13] | 5 video = N/A | N/A | N/A | Static camera | Swapping frames | No gold standard and no camera type have been mentioned. Few numbers of videos and does not contained all the type of video forgery |
| [14] | 10 video = 30 fps and 25 fps | N/A | 1—Canon IXUS<br>2—SONY DSC-PIO | Static camera | Swapping frames | This dataset has no ground truth to show the significant information such as video length and number of frames. Video tampering has been done just for swapping frames |
| [15] | 18 video = N/A | N/A | Canon IXUS 750 | Static camera | Copy–move object | This dataset focused only one type of video tamper (copy–move object) using static camera |
| Proposed MTVFD | 30 video = 30 fps | 16 s shot | YouTube | Static & dynamic camera | 1—Copy–move<br>2—Swapping frames<br>3—Splicing | MTVFD dataset covered different types of video tampering with biggest number of video and long duration of video forgery time compared with the existing datasets. This dataset used static and dynamic camera which has been collected from YouTube. MTVFD dataset provided ground-truth which contains significant information such as number of video frames tampering and length of video |

## 3. Video tampering domain

Digital forensics confronts great challenges with regards to forgery or tampering of digital content. Recently, hackers have found numerous techniques to modify digital content, among these techniques are copy-moving and cloning. Video tampering can be categorized into three areas: temporal domain, spatial domain, and spatio-temporal domain [3,12,16–20]. Tampering with videos spatially (spatial tampering) is possible by forgers as pixels inside a video frame or neighbouring video frames are manipulated by them. Fig. 1(a) illustrates an authentic video out of which a tampered video in Fig. 1(b) is created. Moreover, as Fig. 1(c) depicts, the source video in terms of time (temporal tampering) can be tampered with by forgers if the frame sequence is disrupted by replacing, adding and removing frames, and recording frame sequences. Finally, as Fig. 1(d) illustrates, a combined domain of spatial and temporal (spatio-temporal tampering) videos can be altered by forgers in the case pixels inside a video frame or neighbouring video frames are manipulated by disrupting the frame sequence.

Splicing and copy–move techniques are applied to manipulate video frames in the spatial domain, but those techniques are also applicable to still images. The basis of forged regions is post-processes, and their true value can be maintained. A macro-block structure is a preferable choice for its ability to cross the boundary of identical or considerable extraction of frames out of the comparison region. The perfect method is to overlap blocks in the strategic region of block matching because of the characteristics of the extraction on the basis of the blocks that are contrasted by recognizing resemblances among them. Spaces adjacent to the pixel enable the video data to connect to the blocks with a motion vector of 8 × 8 overlapping blocks used in the luminance sample. A particular finite precision is responsible for the quantization of each value of the pixel. MPEG algorithms implement coding methods of discrete cosine transform (DCT), and each 16 × 16 frame region (macro blocks) inevitably requires vectors. Two copied frames of manipulated video inform about spatial domains [14].

The manipulation of two videos in the VTD dataset by applying the copy–move method is illustrated in Fig. 2. YouTube is the source of all of these videos on the basis of a complicated scene in which animated objects and entities that reflect realistic situations are included. The frame rate ranges between 1 and 189 frames per second. This rate has been used to manipulate where the object is focused, and the surrounding background was not disrupted. The tampering frames at 1–111 per second are illustrated in Fig. 2(b).

Copying a portion of a video sequence into another by splicing can produce another type of spatial domain tampering. Furthermore, splicing tampering becomes difficult if the directions and lighting conditions vary during recording the video using a dynamic camera. Additionally, maintaining consistency in the frame rate to produce the video is another difficulty associated with splicing tampering. Examples of the splicing method used for the manipulation of video samples from the VTD dataset can be seen in Fig. 3(a) and (b). Fragments of video frames are combined through a process called video splicing from different videos, or from the same video, where no more boundary smoothing of various fragments or post-processing is carried out. The artefacts that the video splicing introduces tend to be imperceptible, and are without post-processing. Such scenarios often make people overlook the involved splicing upon inspection.

Frames are swapped through the average of frames, insertion, and deletion, to tamper with video frames in the temporal domain

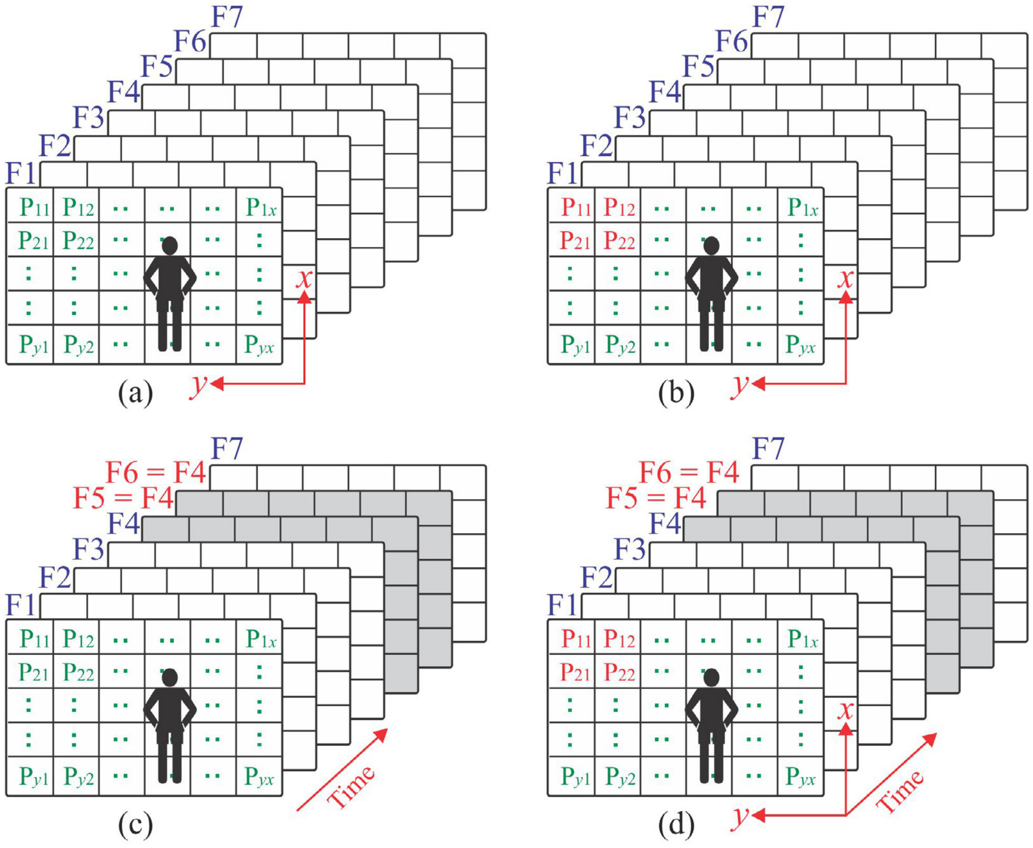


**Fig. 1.** (a) Original video; (b) spatially tampered video; (c) temporally tampered video; and (d) spatio-temporal tampered video. Here, *Fi* and *Pij* denote the *i*th frame and pixel intensity respectively. Height and width are constituted by *x* and *y* respectively. The manipulated versions of the *i*th frame and pixel intensity are *Fi′ and Pij′* respectively.

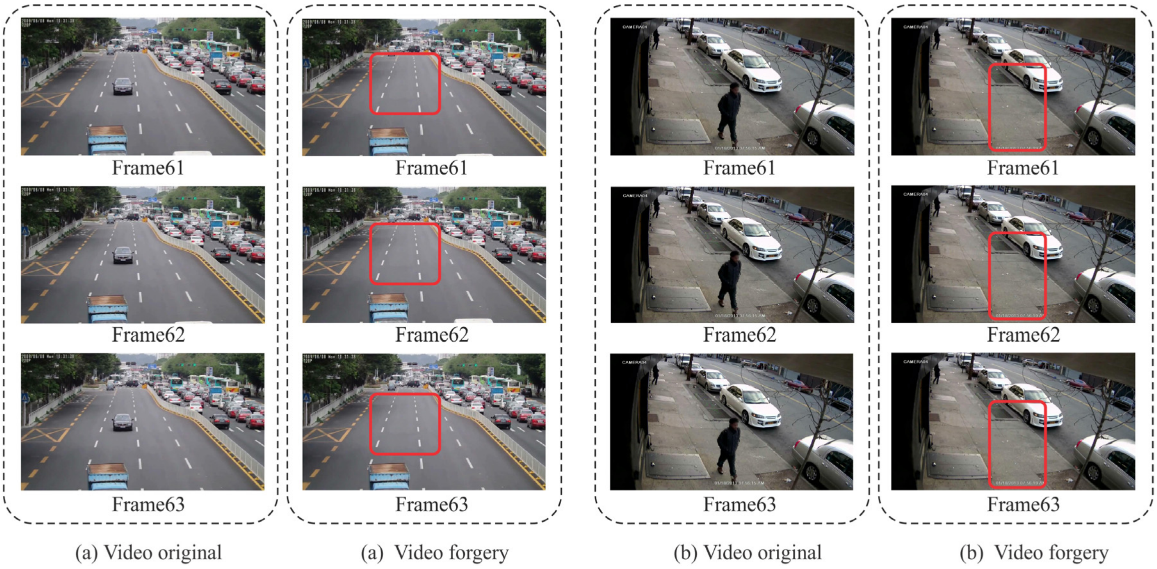


**Fig. 2.** The process of copy–move tampering.

[14]. Three levels are involved in conducting video temporal tampering, namely, frame level, shot/scene level, and video level. Deletion of frames from a video, which may not be from the same scene, or removal of middle frames from the video, can be carried out at the frame level. Manipulation of a whole scene is achieved through deleting a video scene (such as shot cut or scene), or duplicating a video scene into another place, is performed at the scene level. Lastly, duplicating a video is a method of manipulation at the video level [3,19,21]. However, the temporary manipulation of video can be carried out at the video level; a few temporal manipulations cannot be realized at the video level, and sometimes an entire video can be an attempt to delete frames at the video level.

An example of duplicating frames at the frame level is shown in Fig. 4(b). There is a chance for those copied frames to function as middle frames of a video scene at the frame level. Duplicating and pasting an entire scene is possible at the scene level. In fact, at the video level, duplicating is also possible; another video can be produced as a copy of the source video by duplicating and pasting each frame of the video sequence. At the frame level, a frame drop is illustrated in Fig. 4(c). Moreover, items can also be deleted at the scene level. The deletion of each frame in a scene leads to the removal of an entire scene. Deletion is expressed as a shot of a scene cut at the scene level. In the case video frames are swapped (or reordered as per frame sequence) to yield a doctored video from a source one, the frame count is unaltered, as occurs in frame drop. A few video frames in one or two scenes can be those swapped frames at the frame level, while an entire scene is swapped at the scene level, meaning the interchange will occur among all frames of two different scenes. Frame swapping at the frame level is demonstrated in Fig. 4(d). The manipulation of the source video through duplicating video frames and placing them in a different location of the source video increases the frame count.

An actual example of frame swapping from the VTD dataset at frame level is shown in Fig. 5. The yellow car is observed only once in the video scene of the original video. Repetition of the appearance of the yellow car frames was carried out to manipulate it in the forged video, as a specific number of frames containing the

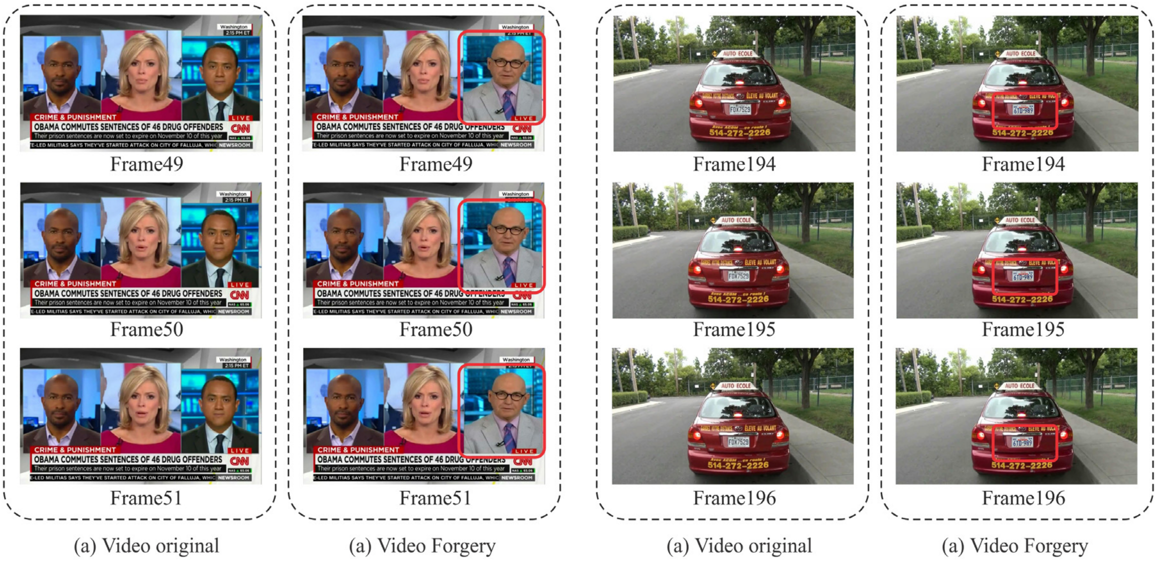


**Fig. 3.** Splicing tampering in video frames.

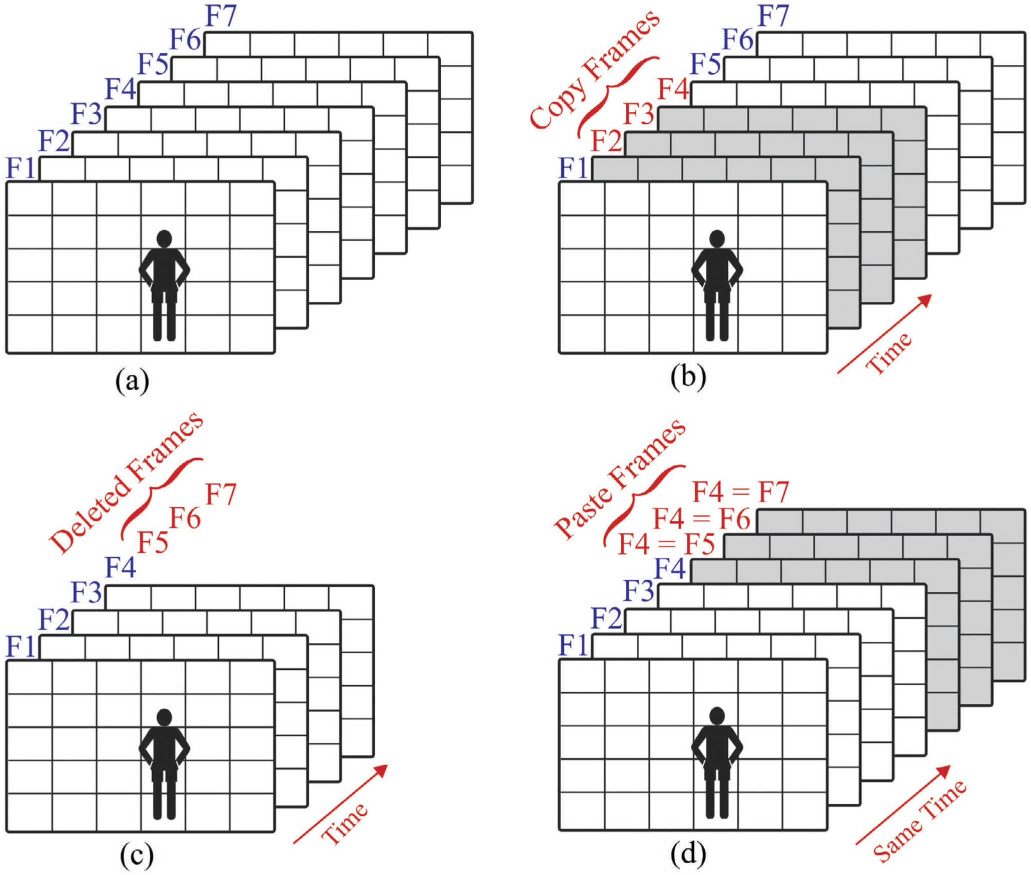


**Fig. 4.** An example of temporal domain: (a) original frames; (b) frame copying; (c) frame drop; and (d) frame swapping.

yellow car have been copied to different locations of the source video, while keeping the original number of frames intact.

## 4. Framework of video tampering process

There are three main types of video modification in the VTD dataset: splicing frames, swapping frames, and copy–move. The manipulation procedure consists of five stages: (1) select and download original videos with the same file type (.avi) from YouTube; (2) trim a specific video part with the use of Video Editor and Video Pad; (3) transform into frames from the video with the use of software such as Matlab; (4) doctor a particular number of frames with the use of Adobe Photoshop CS; and (5) give back forged video along with frames of the video using software such as Matlab.

A generic block diagram through a video tampering process is demonstrated in Fig. 6. First, videos are imported into Photoshop

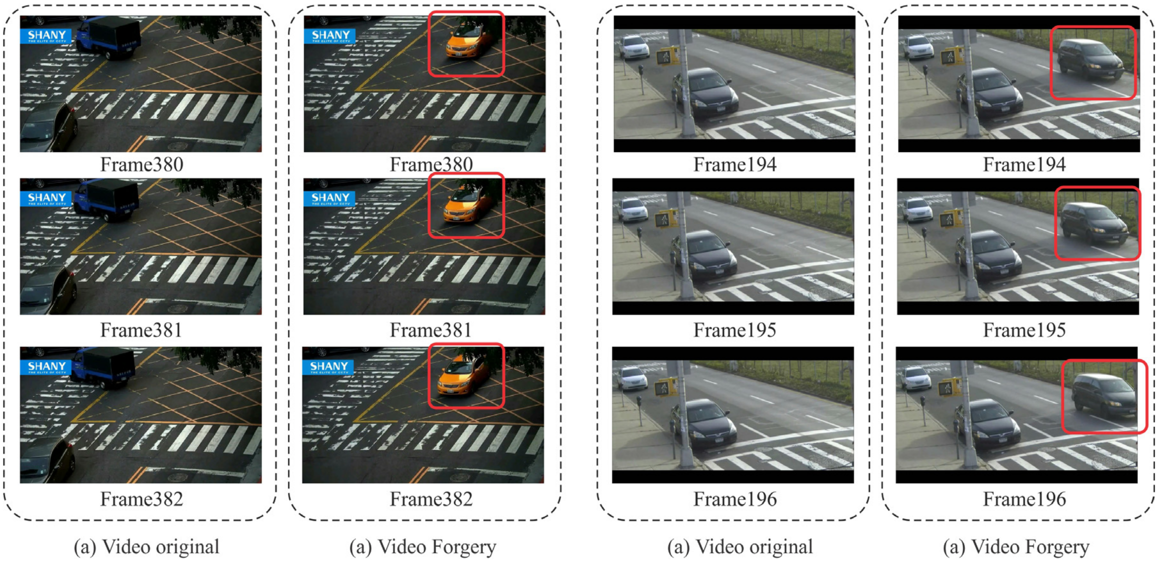


**Fig. 5.** Swapping frames (drop and add). (For interpretation of the references to colour in the text, the reader is referred to the web version of this article.)

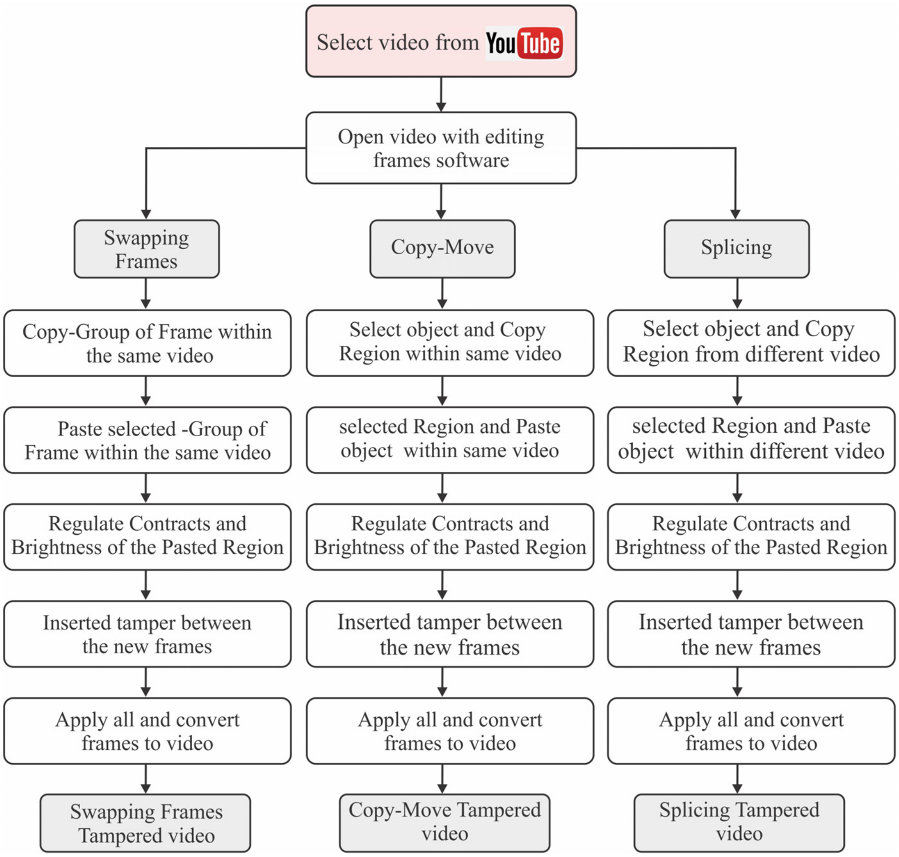

Select video from YouTube
Open video with editing frames software
Swapping Frames
Copy-Move
Splicing
Copy-Group of Frame within the same video
Select object and Copy Region within same video
Select object and Copy Region from different video
Paste selected -Group of Frame within the same video
selected Region and Paste object within same video
selected Region and Paste object within different video
Regulate Contracts and Brightness of the Pasted Region
Regulate Contracts and Brightness of the Pasted Region
Regulate Contracts and Brightness of the Pasted Region
Inserted tamper between the new frames
Inserted tamper between the new frames
Inserted tamper between the new frames
Apply all and convert frames to video
Apply all and convert frames to video
Apply all and convert frames to video
Swapping Frames Tampered video
Copy-Move Tampered video
Splicing Tampered video

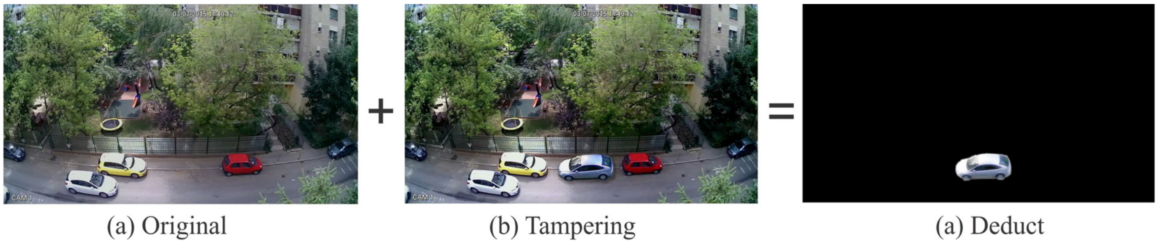
**Fig. 6.** Framework of the video tampering process.

for the animation in the process. The appearance consists of a 16 s timeline and a single layer in the animation window. Frame by frame browsing of the video is possible via the animation timeline, and a simple frame with an unwanted object was picked out. Next, the Clone Stamp tool was used to remove the object as pixels were copied from an alike adjacent area and pasted onto the object. The similarity of the pixels including their neighbours was improved by adjusting the contrast and brightness. After its completion, duplicating the newly modified area, and then copying it into a new video layer tampering was carried out. After that, some adjustments were carried out with regards to how the pasted region appeared between the timeline and synchronies of the original video. An amalgamation of subtractive masking, including the previously stated process, was implemented, followed by using After Effect Photoshop CS for the unwanted objects. Unwanted objects are concealed by this process, while keeping the remaining regions untouched. Lastly, this full tampered video exported, including lossless compression.

The ground truth of this dataset is described in the proceeding section following the explanation of video tampering.

## 5. Ground truth

Developing the ground truth of the dataset is aimed at providing complete information and details regarding each type of video tampering found in the proposed dataset. A new dataset of standard video modification has been created so that researchers have the opportunity of a forensic area for video tampering detection by assessing the performance of their method with a sturdy dataset. Various types of tools for video tampering have been encompassed in the present dataset, which has the largest number videos, and with the longest duration (14–16 s). There are also a set of tampered frames in the VTD dataset that are obtained from manipulating the original footage. There are two videos (i.e. original and tampered) in each scene, which comprise identical file names, duration, length, and number of frames. The researcher is



(a) Original (b) Tampering (a) Deduct

**Fig. 7.** Deducted ground-truth frame of figures (a) and (b).

**Table 2**
Ground-truth video details.

| Video name | Length video = 30 frame per second (fps) | Frames number | Type of video | Number of frame tamper | Percentage | Static/dynamic camera |
|---|---|---|---|---|---|---|
| car_number_plate | 00:15.249 | 457 | Splicing | Frame182–Frame213 | 3.8% | Dynamic camera |
| car_parking | 00:15.051 | 452 | Splicing | All frames tampering | 6.5% | Static camera |
| cake_cooking | 00:15.049 | 451 | Splicing | Frame163–Frame300 | 5.4% | Static camera |
| passport | 00:14.849 | 445 | Splicing | Frame60–Frame297 | 4.2% | Dynamic camera |
| pepper_cooking | 00:15.049 | 451 | Splicing | Frame1–Frame95 | 8.2% | Static camera |
| plane_airport | 00:15.049 | 451 | Splicing | Frame1–Frame39 | 7.1% | Static camera |
| highway_signboard | 00:15.049 | 451 | Splicing | Frame48–Frame236 | 9.4% | Static camera |
| Studio | 00:15.049 | 451 | Splicing | Frame1–Frame69 | 4.2% | Static camera |
| Billiards | 00:14.048 | 421 | Splicing | All frames tampering | 4.7% | Static camera |
| Bowling | 00:14.782 | 435 | Splicing | All frames tampering | 7.3% | Static camera |
| Basketball | 00:15.049 | 451 | Copy–move | All frames tampering | 2.3% | Dynamic camera |
| Football | 00:15.016 | 450 | Copy–move | Frame1–Frame197 | 3.6% | Dynamic camera |
| Clarity_Sample | 00:15.850 | 475 | Copy–move | Frame371–Frame451 | 8.7% | Dynamic camera |
| Archery of 16 | 00:15.049 | 451 | Copy–move | Frame237–Frame279 | 5.4% | Dynamic camera |
| 100 m swimming | 00:15.049 | 451 | Copy–move | Frame362–Frame423 | 3.9% | Static camera |
| Camera_Demo | 00:16.017 | 480 | Copy–move | Frame1–Frame189 | 7.8% | Static camera |
| CCTV_London_Str. | 00:14.048 | 421 | Copy–move | Frame120–Frame244 | 8% | Static camera |
| man _street | 00:15.049 | 451 | Copy–move | Frame1–Frame111 | 7.4% | Static camera |
| white_Car | 00:15.049 | 451 | Copy–move | Frame243–Frame334 | 8.7% | Static camera |
| Dahua_HDCVI | 00:14.048 | 421 | Copy–move | All frames tampering | 4.8% | Static camera |
| AudiRS7 | 00:15.182 | 455 | Swapping frame | Repeat Frame27–Frame81 | – | Dynamic camera |
| yellow_car | 00:15.049 | 451 | Swapping frame | Repeat Frame359–Frame434 | – | Static camera |
| Pong_Trick_Shots | 00:15.049 | 421 | Swapping frame | Repeat Frame289–Frame421 | – | Static camera |
| Awesome_Cuponk | 00:15.049 | 451 | Swapping frame | Repeat Frame51–Frame100 | – | Static camera |
| Varifocal Bullet | 00:15.051 | 452 | Swapping frame | Repeat Frame225–Frame301 | – | Static camera |
| SWANN_HD820 | 00:16.017 | 480 | Swapping frame | Repeat Frame1–Frame123 | – | Static camera |
| Ball_Bowling | 00:15.049 | 451 | Original frame | – | – | Dynamic camera |
| Manchester vsChel. | 00:14.749 | 442 | Original frame | – | – | Dynamic camera |
| Car_move | 00:15.783 | 473 | Original frame | – | – | Static camera |
| Parking a Vehicle | 00:16.017 | 456 | Original frame | – | – | Static camera |
| High_way | 00:15.316 | 460 | Original frame | – | – | Static camera |
| man_street | 00:15.049 | 451 | Original frame | – | – | Static camera |
| Stop_car | 00:15.916 | 477 | Original frame | – | – | Static camera |

able to obtain an apt tampered assessment, expressed as a percentage of the video frames, yielded by the ground truth. The computation of tampering percentage depends on the tampered area size of each frame. Fig. 7 illustrates a 6.5% tampering percentage of the entire frame size.

Moreover, the VTD dataset comprises 33 videos (both original and tampered), the first seven of which are not manipulated, as the capability of recognizing original videos by a method can be evaluated. The rest are distributed among three forgery categories: (1) 10 videos with copy–move, (2) six videos with swapped frames, and (3) 10 videos with splicing. Both the original and forged videos are shown in Table 2. Information related to the number of forged frames, video length, total number of frames, video type, camera type, and size of tampered region, are all provided in the ground truth. With this dataset, researchers are able to make a better assessment of the methods involved in their work.

## 6. Conclusions

A public forensic library of modified videos available in the VTD dataset was comprehensively presented in this paper. All 33 videos in the current dataset were gathered from YouTube, currently making it the largest dataset. The purpose of developing the VTD dataset is to provide test data to standardize video forensic algorithms for the identification of three tampering types, namely, splicing, swapping frames, and copy–move. The duration and frame size of each video is about 16 s and 1280 × 720 respectively, along with a frame rate of 30 frames per second. Both dynamic and static cameras have been used for shooting these videos in various lighting conditions. This dataset can be found on the YouTube video channel reached using the following URL https://www.youtube.com/channel/UCZuuu-iyZvPptbIUHT9tMrA. This library will be consistently enhanced with the addition of more videos of various sources. Footage from digital camcorders and smart phones will be included as well. Researchers will greatly benefit from such a library, as they will be provided with a general demonstration video to build a standard for their forensics algorithms.

## Acknowledgements

The authors would like to acknowledge the support provided by Perbadanan Kemajuan Filem Nasional Malaysia (FINAS) to evaluate and validate the quality of creating video tampering the VTD dataset and verify the ground truth that has been provided by the authors for benchmarking reason. We also thank the anonymous reviewers whose comments have improved this paper.

## Appendix A. Supplementary data

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.forsciint.2016.07.013.

## References

[1] S.A. Chowdhury, D. Makaroff, Characterizing videos and users in YouTube: a survey, 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA) (2012) 244–251 IEEE.

[2] F.N. Dezfoli, A. Dehghantanha, R. Mahmoud, N.F.B.M. Sani, F. Daryabar, Digital forensic trends and future, Int. J. Cybersecur. Digit. Forensics 2 (2013) 48–76.

[3] M.K. Thakur, Tampered Videos: Detection and Quality Assessment, Jaypee Institute of Information Technology, 2013.

[4] O.I. Al-Sanjary, G. Sulong, Detection of video forgery: a review of literature, J. Theor. Appl. Inf. Technol. 74 (2015) 207–220.

[5] W. Wang, H. Farid, Exposing digital forgeries in video by detecting double quantization, Proceedings of the 11th ACM Workshop on Multimedia and Security (2009) 39–48 ACM.

[6] T. Gloe, R. Böhme, The dresden image database for benchmarking digital image forensics, J. Digit. Forensic Pract. 3 (2010) 150–159.

[7] J. Dong, W. Wang, T. Tan, Casia image tampering detection evaluation database, 2013 IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP) (2013) 422–426 IEEE.

[8] G. Schaefer, M. Stich, UCID: an uncompressed color image database, Electronic Imaging 2004, International Society for Optics and Photonics, 2003, pp. 472–480.

[9] D. Tralic, I. Zupancic, S. Grgic, M. Grgic, CoMoFoD—new database for copy–move forgery detection, ELMAR, 2013 55th International Symposium (2013) 49–54 IEEE.

[10] G. Qadir, S. Yahaya, A.T. Ho, Surrey university library for forensic analysis (SULFA) of video content, IET Conference on Image Processing (IPR 2012) (2012) 1–6 IET.

[11] J. Chao, X. Jiang, T. Sun, A novel video inter-frame forgery model detection scheme based on optical flow consistency, International Workshop on Digital Watermarking (2012) 267–281 Springer.

[12] L. Su, T. Huang, J. Yang, A video forgery detection algorithm based on compressive sensing, Multimed. Tools Appl. 74 (2015) 6641–6656.

[13] Q. Wang, Z. Li, Z. Zhang, Q. Ma, Video inter-frame forgery identification based on consistency of correlation coefficients of gray values, J. Comput. Commun. 2 (2014) 51.

[14] S.-Y. Liao, T.-Q. Huang, Video copy–move forgery detection and localization based on Tamura texture features, 2013 6th International Congress on Image and Signal Processing (CISP) (2013) 864–868 IEEE.

[15] D. Conte, P. Foggia, G. Percannella, M. Vento, Performance evaluation of a people tracking system on PETS2009 database, 2010 Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (2010) 119–126 IEEE.

[16] P.K. Atrey, W.-Q. Yan, M.S. Kankanhalli, A scalable signature scheme for video authentication, Multimed. Tools Appl. 34 (2007) 107–135.

[17] S. Upadhyay, S.K. Singh, Video authentication: issues and challenges, Int. J. Comput. Sci. Issues 9 (2012).

[18] A. Subramanyam, S. Emmanuel, Video forgery detection using HOG features and compression properties, 2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP) (2012) 89–94 IEEE.

[19] S. Upadhyay, S.K. Singh, Learning based video authentication using statistical local information, 2011 International Conference on Image Information Processing (ICIIP) (2011) 1–6 IEEE.

[20] J. Zhang, Y. Su, M. Zhang, Exposing digital video forgery by ghost shadow artifact, Proceedings of the First ACM Workshop on Multimedia in Forensics (2009) 49–54 ACM.

[21] G.-S. Lin, J.-F. Chang, Detection of frame duplication forgery in videos based on spatial and temporal analysis, Int. J. Pattern Recognit. Artif. Intell. 26 (2012) 1250017.