Forensic approach for detecting the region of Copy-Create video forgery by applying frame similarity approach

Govindraj Chittapur[1*], S. Murali[2] and Basavaraj S. Anami[3]
[1]Department of Computer Applications, Basaveshwar Engineering College, Bagalkot, India
[2]Department of Computer Science & Engineering, Maharaja Institute of Technology, Mysore, India
[3]Department of Computer science & Engineering, KLE Institute of Technology, Hubli, India
gbchittapur@gmail.com

Available online at: www.isca.in
Received 28th August 2019, revised 24th November 2019, accepted 12th December 2019

Abstract

Now a day's videos are living in the heart of the modern communication world. Every one socio living being in this world uses videos are parts of social media like Whats-app, Facebook, Instagram, and Twitter. However, the problem persists the trustworthiness of those video published in the media world. Due to high-end open source free video editing software are readily available for editing the source video and modifying the content of the video becomes simpler. In forensically a part of media information copied and pasted in the same or another footage without changing the source of information is called it as copy-create forgery techniques. At presently some researcher found the methods in both active and passive forgery techniques those are all focusing on hardware embedded and high processing detection with the lowest accuracy and executed by considering minimal parameters which are becoming a bottleneck for the unique solution. Now we are proposing techniques with the help of necessary video vision processing to identify the forged region with extracting necessary information and applying the backtrack methods for investigation method to detect the forged part and authenticating the source of the video. We are proposing concepts and implementation by considering the region of interest parameter by visualizing and analyzing the very basic pixel mapping along with block matching of a group of pictures converted by forged video along with source information. We are taking the statistical mean frame of each forged frame along with color channels and deducing and mapping with each block and generating a forged region of copy-create forged video. We are using forensically standard forgery data set created by Surrey University as SULPA and its parser dataset REWIND with customizing with the help of visionary parameter for testing the result. We succeeded 96% for accuracy and precession of the result. We also got the excellent accuracy in other standard dataset YTD and SYSU-OBJ-FORGE dataset.

Keywords: Copy-create forgery, pixel mapping, block- matching, frame-similarity, standard data, set.

Introduction

With the availability of advanced video editing tool creates socio-living problem., due to such software, digital media communication becomes untrustworthiness where we are living with the social media world. In social media, every day we are getting massive fake video transactions with the advancement of technology over modification and alter of the video information becomes more straightforward, but identification and publication of such video become a bottleneck for currently available of the technology. All forged media editors create such video for targeting high profile personalities to create embarrassment situations for them and creates media hype for publication impact factor. Recently words top newspaper Times of India identify popular actor Amitabachhans fake video published on June 28, 2019, in digital publications as shown in Figure-1[1]. Various television media starts telecasting with forgery video in the console and making entertainment program, as shown in Figure-2[2].

Many passive approaches are available with limited parameter based identification; now we are proposing a forensic approach for detecting the region of Copy-Create Video Forgery By applying frame similarity approach using generic solution by using standard video forgery dataset.

Literature Survey on Recent Video Forgery Detection

From the literature survey, several researchers have developed and proposed different video forensic approaches: Omar Ismael Al-Sanjary[1] proposed a method related to cloning object in a video, Shania et al.[2] proposed copy-move using coarse-to-fine approach, general copy-move forgery techniques[3-10] are presented based on specific forgery techniques. Later frame duplication related work and copy -create video forgery related work submitted by Chittapur and Murali S[11-13]. Automatic detection of object forgery along with the sysu-obj-forge dataset given by S, Chen[14].

From the above literature survey, it identifies that mentioned achievable results are by considering a few numbers of input customized video, now we are proposing a method which supports standard video forensic dataset like SULFA[15], REWIND[16] and VTD[17] dataset. All results and their contributions applicable to customized video dataset and few parts of standard data set. Now we are proposing the methodology for the generic dataset and identify the forgery region.

Method and Implementation

In this proposed algorithm, first illustrates designing the dataset by referencing standard forged and authentic video gallery. In next section described copy create video forgery detection by applying a frame similarity approach for standard forgery data set used for scene created by adding, subtracting, or modifying the information about the original video. Second Section illustrate regarding frame similarity algorithm, and last section discussed the result differed frame different data set.

Designing the dataset: From considering the SULFA[15], REWIND[16] and VTD[17] data set around 300 authenticate and forged video data, we are created customized video dataset by considering invariant frame features with the discontinuity of the object in a preferred video. SULFA[15] contains unique just as forged video documents. Every video is around ten seconds in length with the resolution of 320x240 and 30 frames for each second. Thus, The VTD[17], concentrated on video altering recognition on videos gathered from the YouTube, is made out of 33 downloaded videos, 16-s in length, at 30 fps with an HD goal. The first dataset is subdivided into four subsets: one containing unaltered videos; one with videos made by joining; one with videos controlled by copy-move; and one with videos altered by swapping frames essential. SYSU-OBJFORG[4] dataset contains 100 essential and comparing 100 object-based forged video cuts, which are all 3 Mbit/s, 1280x720 (720p) H.264/MPEG-4 encoded video streams.

Copy-Create video Forgery By Frame Similarity approach: We are proposing an approach by considering each suspected video is converting into several groups of picture frames as blocks, now we each block is consist of a group of pixels with a defined set of picture element properties. Now by considering those properties set it as mapping frame-block as **Ω**.

Each **Ω** block is a summation of video which is represented by video model representation

$$\Omega z = [I(1), B(1), B(2), P(3), B(4), B(5), P(6), B(7), B(8) \qquad (1)$$

Ωz is a typical time sequence with a variant set of relative group of video model with a different colligative sequence of flow frames with Interleaving(I), Bidirectional(B) and Predictive(P). Now, with reference video, each block Ωz is having feature group of sequence with directional components and correlative features between a set of frames.

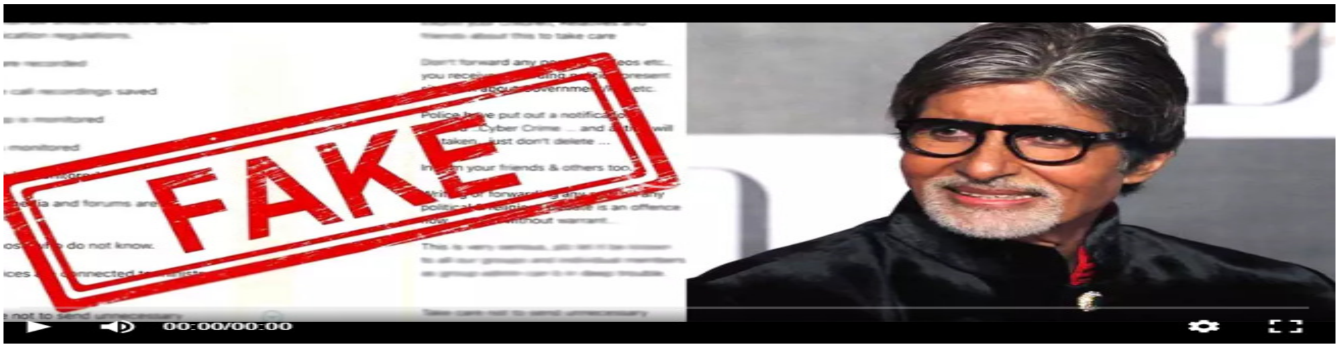
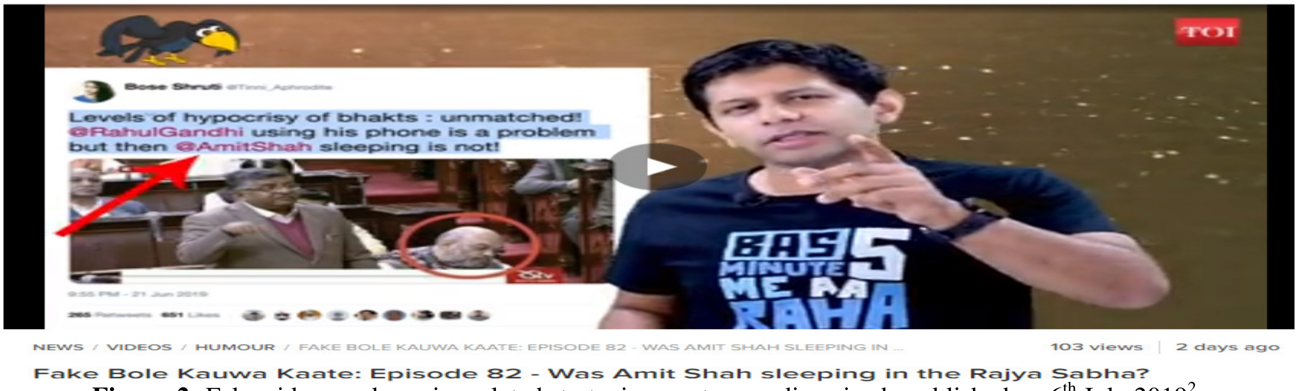


Figure-1: Amitabh Bachchan falls prey to fake news via web-based networking media distributed in Times of India on June 28, 2019[1].



Bose Shruti

Levels of hypocrisy of bhakts : unmatched! @RahulGandhi using his phone is a problem but then @AmitShah sleeping is not!

NEWS / VIDEOS / HUMOUR / FAKE BOLE KAUWA KAATE: EPISODE 82 - WAS AMIT SHAH SLEEPING IN ... 103 views | 2 days ago

Fake Bole Kauwa Kaate: Episode 82 - Was Amit Shah sleeping in the Rajya Sabha?

Figure-2: Fake videos and gossips related strategies create a media episode published on 6th July 2019[2].

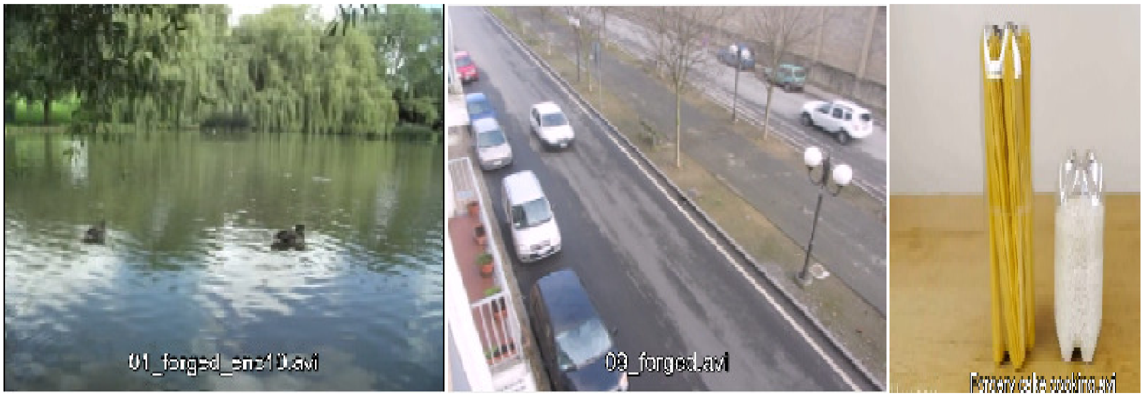
Now each block is consist of set frames as:

$$z(\Omega) = \sum_{1}^{n} xi \cong \sum_{1}^{m} yi \qquad (2)$$

Z (Ω) is the resultant identified forged region and ∑ xi over the set of converted group of frames from 1 to last identified frame as ***n*** is the set of frame feature compared with each block along with a set of sequence, those are block mapped by comparing each block by a group of pixels to ∑yi along with 1st frame of feature set to last colligative sequence as *m.* Each resultant compared features stored in the z(Ω), which has forged region of suspected video.

Result and discussion

Dataset designed and proposed algorithms are implemented in matlab14 using computer vision and image processing toolbox. We considered all the video specified in dataset standards and achieved good precession and accuracy result shown in table1 for different operations performed in a video.



(a) SULFA Data set (b) REWIND Dataset (c) VTD Data Set

Figure-3: Forged Videos from different standard Dataset.

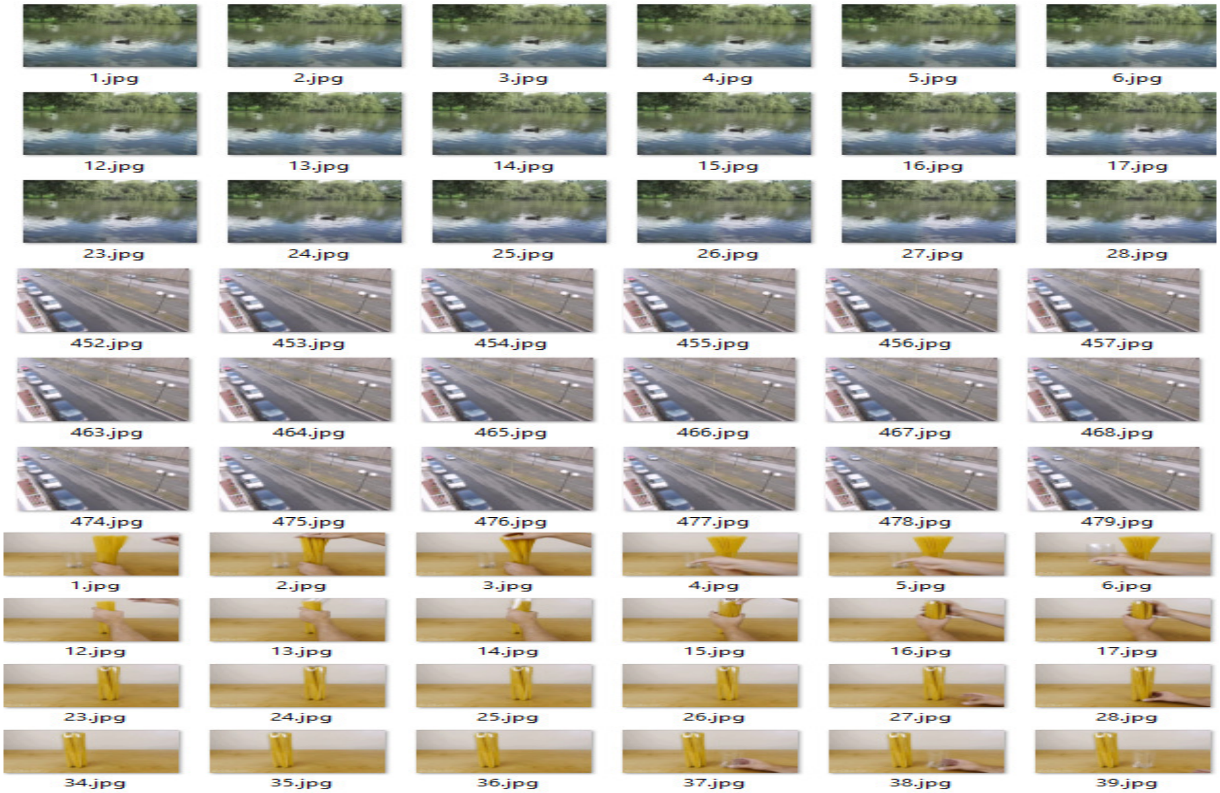
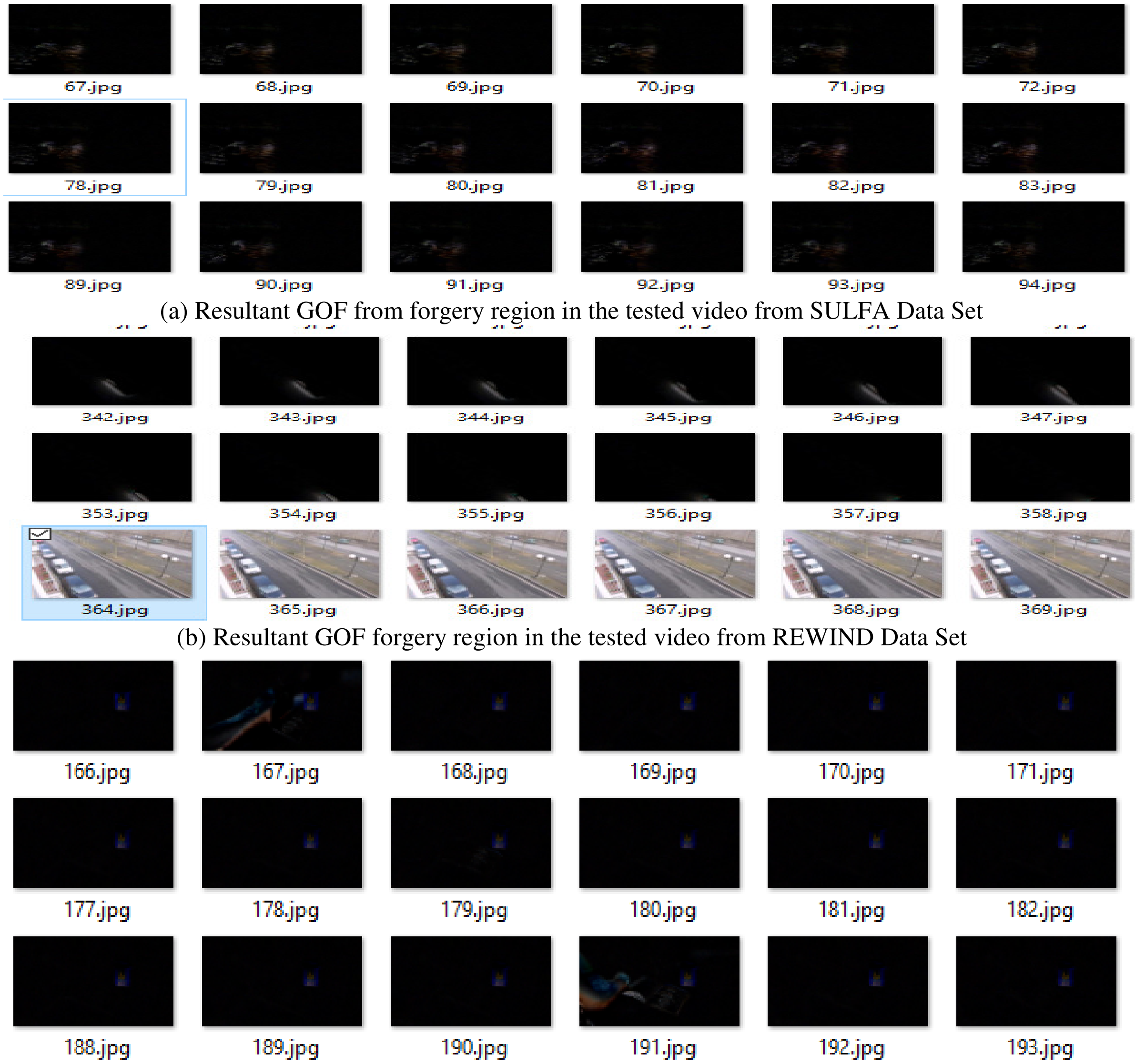


Figure-4: Group of pictures from different standard Dataset.

Figure-3 demonstrated the sample videos from the different standard dataset; we extracted a group of frames (GOF) is shown in Figure-4 the resultant forgery regions are shown in Figure-5 and Figure-6 by referring proposed copy create forgery detection using similarity approach algorithm.



(a) Resultant GOF from forgery region in the tested video from SULFA Data Set

(b) Resultant GOF forgery region in the tested video from REWIND Data Set

(C) Resultant GOF forgery region in the tested video from VTD Data Set

Figure-5: copy creates forgery detection using similarity approach algorithm.

(a) Sulfa dataset (b) Rewind dataset (c) VTD dataset

Figure-6: Forgery region identified by proposed frame similar approach.

Following Table-1 illustrate the result among different standard data set for different operation performing on copy-create video forgery detection using a frame similarity approach.

Table-1: Forgery frame detection among different dataset samples using a frame similarity approach.

Data set	Resultant forgery GOF extracted from tested video	Resultant Original GOF extracted from tested video	Total Number of Group of Frames tested in each video.
SULFA Dataset	210	40	250
REWIND Dataset	348	206	554
VTD Dataset	184	267	451

Conclusion

Copy creates video forgery is a common problem in video authenticity because freely available sophisticated video editing software's. Research community working on finding a solution for this classical problem, they are all success in identifying the solution with backtrack techniques. We are proposing a unique solution by refereeing standard and forgery video dataset, which helps to identify the challenging problem exist in copy create video forgery detection. We proposed a forensic approach for detecting video forgery detection using a frame similarity approach.

We use SULFA[15], REWIND[16] and VTD[17] dataset for the different forged dataset and tested around 300 videos. In this paper, we use each video from the said dataset as identified. We successfully identified the forgery region with frame comparison with similarity approach. We use forensic back-track approach that suggests us to identify forgery anomalies by referring intensity differences by mapping the block comparison techniques. Source mapping is the bottleneck of this approach.

References

1. Al-Sanjary O.I., Ahmed A.A., Jaharadak A.A.B., Ali M.A. and Zangana H.M. (2018). Detection clone an object movement using an optical flow approach. In 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 388-394. IEEE. doi: 10.1109/ISCAIE.2018.8405504

2. Jia S., Xu Z., Wang H., Feng C. and Wang T. (2018). Coarse-to-fine copy-move forgery detection for video forensics. *IEEE* Access, 6, 25323-25335. doi: 1109/ACCESS.2018.2819624

3. Üstübıoğlu B., Ulutaş G., Nabıyev V.V., Ulutas M. and Üstübıoğlu A. (2018). Using correlation matrix to detect frame duplication forgery in videos. *26th Signal Processing and Communications Applications Conference (SIU)*, Izmir, 1-4. doi: 10.1109/SIU.2018.840436 4

4. Su L., Li C., Lai Y. and Yang J. (2017). A fast forgery detection algorithm based on exponential-Fourier moments for video region duplication. *IEEE Transactions on Multimedia*, 20(4), 825-840. April 2018 doi: 10.1109/TMM.2017.2760098.

5. Verde S., Bondi L., Bestagini P., Milani S., Calvagno G. and Tubaro S. (2018). Video Codec Forensics Based on Convolutional Neural Networks. *2018 25th IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, 2018, 530-534. doi: 10.1109/ICIP.2018.8451143

6. Feng C., Xu Z., Jia S., Zhang W. and Xu Y. (2016). Motion-Adaptive Frame Deletion Detection for Digital Video Forensics. in *IEEE Transactions on Circuits and Systems for Video Technology*, 27(12), 2543-2554, Dec. 2017. doi: 10.1109/TCSVT.2016.2593612 .

7. Huang C.C., Zhang Y. and Thing V.L. (2017). Inter-frame video forgery detection based on multi-level subtraction approach for realistic video forensic applications. *IEEE 2nd International Conference on Signal and Image Processing (ICSIP)*, Singapore, 2017, 20-24. doi: 10.1109/SIPROCESS.2017.8124498.

8. Sitara K. and Mehtre B.M. (2017). A comprehensive approach for exposing inter-frame video forgeries. In 2017 IEEE 13th International Colloquium on Signal Processing & its Applications (CSPA), 73-78. IEEE. doi:1109/CSPA.2017.8064927.

9. Xu J., Liang Y., Tian X. and Xie A. (2016). A novel video inter-frame forgery detection method based on histogram intersection. In 2016 IEEE/CIC international conference on communications in China (ICCC), 1-6. IEEE. doi: 10.1109/ICCChina.2016.7636851

10. Mathai M., Rajan D. and Emmanuel S. (2016). Video forgery detection and localization using normalized cross-correlation of moment features. 2016 IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), Santa Fe, NM, 149-152. doi: 10.1109/SSIAI.2016.7459197.

11. Chittapur G.B., Murali S., Prabhakara H.S. and Anami B.S. (2014). Exposing Digital Forgery in Video by Mean Frame Comparison Techniques. In: Sridhar V., Sheshadri H., Padma M. (eds) Emerging Research in Electronics, Computer Science and Technology. Lecture Notes in Electrical Engineering, 248. Springer, New Delhi

12. Murali S., Chittapur G.B. and Prabhakara H.S. (2013). Detection of Digital Photo Image Forgery Using Copy-Create Techniques. In: S M., Kumar S. (eds) Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012). Lecture Notes in Electrical

Engineering, 221. Springer, India doi: 10.1007/978-81-322-0997-3_26.

13. Murali S., Chittapur Govindraj S., Prabhakara H. and Anami Basavaraj (2013). Comparison and analysis of photo. image forgery detection techniques. doi:10.5121/ijcsa.2012.2605.

14. Chen S., Tan S., Li B. and Huang J. (2015). Automatic detection of object-based forgery in advanced video. *IEEE Transactions on Circuits and Systems for Video Technology*, 26(11), 2138-2151.. 26.1-1.10.1109/TCSVT. 2015.2473436.

15. Qadir G., Yahaya S. and Ho A.T. (2012). Surrey university library for forensic analysis (SULFA) of video content. Insert Name of Site in Italics. N.p., n.d. Web. 21 Jul. 2019 http://sulfa.cs.surrey.ac.uk/.

16. REWIND Video: Copy-move Forgeries Dataset - Rewind Project. (2019). Retrieved from https:// sites.google.com/ site/rewindpolimi/downloads/datasets/video-copy-move-fo

17. Al-Sanjary O.I., Ahmed A.A. and Sulong G. (2016). Development of a video tampering dataset for forensic investigation. *Forensic science international*, 266, 565-572. 10.1016/j.forsciint.2016.07.013.

18. Andy S. and Haikal A. (2017). Simple duplicate frame detection of MJPEG codec for video forensic. 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, 321-324. doi: 10.1109/ ICITISEE.2017.8285520