Video Authentication using PLEXUS Method

Dr. Hala Bahjat Abdulwahab[1]
Computer Science Department
University of Technology
Baghdad, Iraq

Khaldoun L. Hameed[2]
Ibn Sina University for Medical and Pharmaceutical Sciences
Baghdad, Iraq

Nawaf Hazim Barnouti[3]
Al-Mansour University College
Baghdad, Iraq

***Abstract*—Digital Video authentication is very important issue in day to day life. A lot of devices have got the ability of recording or capturing digital videos and all these videos can be passed through the internet as well as many other non-secure channels. There is a problem of illegal updating or manipulation of digital video because of the development in video editing software. Therefore, video authentication techniques are required in order to ensure trustworthiness of the video. There are many techniques used to prevent this issue like Digital Signature and Watermarking, these solutions are successfully included in copyright purposes but it's still really difficult to implement in many other situations especially in video surveillance. In this paper, a new method called PLEXUS is proposed for digital video authentication on temporal attacks. In authentication process, the sender will generate a signature according to the method steps using a video and private key. In verification process, the receiver will also generate a signature using the same video and private key then each signature will be compared. If the two signatures are matched then the video is not tampered otherwise the video is tampered. This method is implemented using 10 different videos and proved to be an efficient method.**

Keywords*—PLEXUS; video authentication; video tampering; temporal attacks

I. Introduction

Video authentication continues to be an important subject with significant attraction to researchers in last few years. By definition, Digital video authentication represents the technique of deciding whether the taken video is original and has not happened to be tampered with or not. Information can be transmitted quickly to thousands of kilometers with a few seconds. This will make a powerful influence on the growth and development in public. However, the significant improvement in information technology taken us to a new generation of effective information, it also has additionally added a few challenges related to information [1].

In digital generation, communication and compression methods help learning to share multimedia data including images and videos. Although, multimedia editing resources and tools may often use successfully modify the material of digital data, then straining the integrity of information [2]. The developing of computer systems and the equipment are making digital manipulation of video very simple and so easy to accomplish. Digital video trustworthiness and credibility has become really difficult because the copy of digital multimedia data acts similar to the original data.

A video might possibly be modified in a certain process to defame someone. In last few years, a number of situations are actually reported where some well-known individuals in the society was detected against the law in different actions in the video recordings done by some journalists. But unless they use reliable methods to find that the video is not easy to believe on these kinds of incidents. Meanwhile, criminals escape from getting arrested simply because this video that is used as facts against them indicating their crime will not completely confirmed in the court of law [1][3]. When it comes to surveillance systems, it is hard to guarantee that the digital video provided as facts, is just like it had been in fact recorded by the camera. For this reason, you can find an interesting require for video authentication.

Standard data authentication technology for message credibility is developed fully, but video authentication remains as early development step and several essential questions are still in mind. As an example, several different authentication methods designed during the last few years, it is difficult to acknowledge which method appear to be appropriate choice to make sure of credibility adapted to videos. There is certainly a good reason to use synthesizing literature to figure out the type of the condition, discover the probability of research difficulties, standardize different research subjects and evaluate the relative performances of the various methods [3].

II. The Need for Video Authentication

In certain products the credibility of video data is major concern including video surveillance, law enforcement, and forensic investigations. As an example, in court of law, trustworthiness must be established in this case for any video that is used as evidence. It is simple and easy to clear away a specific activity, individuals through removing some frames from video sequences. Meanwhile, it is simple to place some objects into the same video [4].

For that reason, video authentication is a technique that make sure that the information in the video is original and similar when taken. For confirming that video content is original, check whether the video was modified or not, and avoid different types of forgeries, video authentication methods are utilized [5].

These methods also detect and recognize the form of modification. In point of fact, several powerful processing tools are available for digital video. Considering that different video recording devices become much more convenient and reasonably priced choice in the private and public sections.

In criminal investigations, video evidences receive an important role as a result of their ability to acquire complete information and additionally have significant possibilities to help with investigations. Therefore, it will be important to obtain highest attention to ensure that the provided video evidence is original [3].

III. Video Authentication Applications

Digital video applications have a large number of advantages compared with custom analog video, better image quality, better color reproduction, and sharper images. Additionally, with the development in digital technologies, a video is often simple to carried over the internet and it produces easy editing and cropping [6].

Today the world is a video world from standard television broadcasting to modern communication media. In public individuals are more likely being video recorded. If you are walking on street, riding a city bus, entered a government building, etc. you probably being video recorded by a camera. Some civilians have setup mobile CCTV systems in their home and even their cars just in case of anything happen and they need to secure themselves or discover a crime that can happen any time. In fact, the police originally setup cruiser video recording systems to protect themselves and also to protect the citizens [6][7].

Forensic professionals have got several tools to decide scientifically whether the video is original or has been modified. In particular, it is difficult with digital video to discover which way a video was edited. This is where forensic investigation will become the only way to decide the video evidence credibility.

There are actually a number of situations in our everyday life exactly where video authentication is apparently necessary. In a situation of a well-known person was involved in illegal activities, it is a major interest to be able to determine whether or not the video was modified. In other situation, criminals can be set free simply because the video displaying their crime is not proved definitely in the court of law [1][7].

IV. Video Tampering

Video Tampering is a process of maliciously modification to the information material that going to be made by a video sequence. This process will be done for the purpose to hide an object or event. The seriousness and importance of video tampering depends on how and where these tampered videos have to be put to use. Since many advanced and low-cost video editing software tools are presented in the market which will make it an easy task to modify the video information material maliciously, it gives a significant challenge to researchers to be solved [8][9].

There are lots of potential attacks which will performed to modify the video data material. Whenever a risky modification is done on a video sequence, it either attacks on the contents of the video or attacks on the temporal dependency between the frames [10]. A large number of authentication methods are actually proposed but the majority of them are actually mainly dedicated to still images. However, the primary activity of video authentication system is to confirm whether or not the given video is tampered. Although, in a number of applications, because the ability to access information in video sequences, it will become better if the authentication system can find exactly in which part the modifications occurred and exactly how the video is tampered. Taking into consideration where and how, the video tampering attacks offers different classifications [11][12].

According to video sequences regional property, video tampering attacks can be classified to three basic types: spatial tampering, temporal tampering and the combination of these two, spatio-temporal tampering attacks. However, each category can even further be classified into their subcategories [10].

A. Spatial Tampering

In spatial tampering risky modifications are carried out on frames content. The operations which can be performed as spatial tampering are different methods to modify the frame just like copy, move, splicing, object adding and removing etc. Spatial tampering can be divided into three categories as shown in Figure 1. These kinds of attacks can be successfully performed by using video editing software [13][14].

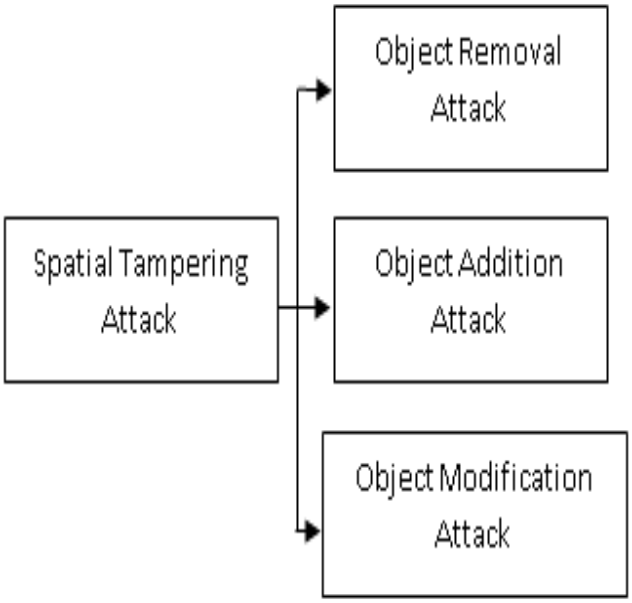

Fig. 1. Spatial Tampering Classification.

Object removal attack can be done with both foreground and background objects basically by hiding the occurrence of a person or object in a specific sequence of frames. Object addition attack can be done with both foreground and background objects basically by inserting any kind of objects in a frame or in a number of frames that belongs to a specific digital video that are available used as evidence fact. Additional object can easily paste in a frame or set of frames by using video editing software. Object modification attack can be done with both foreground and background objects basically by modifying any existing object of the frame in such a way that the actual identity of that object is misplaced, and a new object may occurred which is totally different from the original object [15][16].

B. Temporal Tampering

In temporal tampering malicious modifications is done on the video sequence of frames give attention to the temporal dependency. Time sequence of the frame that is recorded by a digital video camera generally influenced by Temporal tampering attacks [8][9]. Temporal tampering attacks can be divided into three types: frame addition, frame removal and frame shuffling as shown in Figure 2.

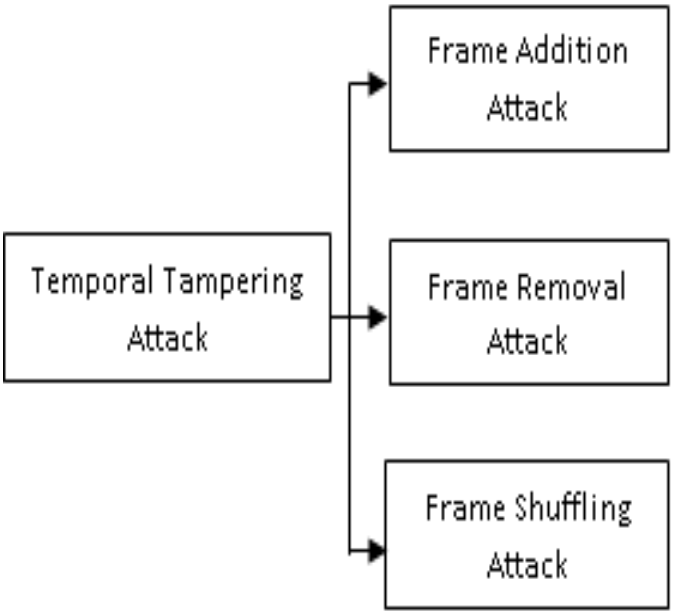

Fig. 2. Temporal Spatial Tampering Classification.

1) Frame Addition Attack

This kind of attack can be performed basically by adding additional frames from another video at some random locations in a video which has the same statistical properties as shown in Figure 3 [8][17].

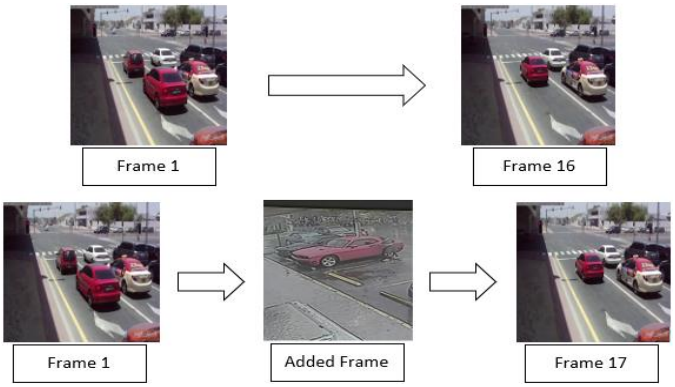

Fig. 3. frame addition attack example. In first row the original frame sequence from 1 to frame 16 has been shown. After attack, the second row of the frames shows the altered frame sequence in which a new frame is inserted between frame 1 and frame 16. And frame 16 become frame 17.

2) Frame Removal Attack

This kind of attack can be performed basically by removing one frame or a number of frames from the digital video at a certain location to a fixed location or removing set of frames from different locations as shown in Figure 4 [9][18].

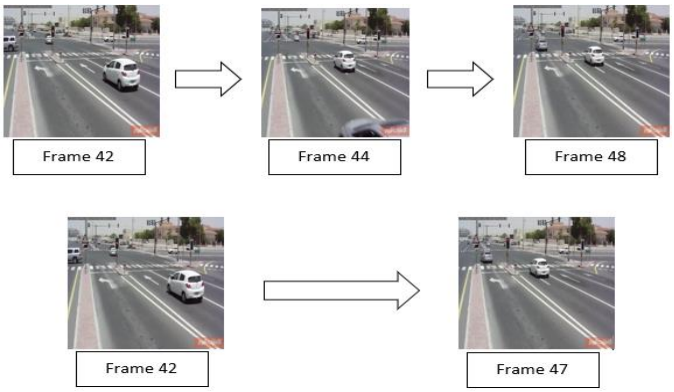

Fig. 4. frame removal attack example. In first row the original frame sequence with frame 42, frame 44, and frame 48. After attack, the second row of the frames shows the altered frame sequence with frame removal attack in which frame 44 is eliminated from the video and hence frame 48 become frame 47.

3) Frame Shuffling Attack

This kind of attack can be performed basically by shuffling the frame. The order of the frames will be changed and incorrect information is done by the digital video when compared with the original taken video as shown in Figure 5 [8][9].

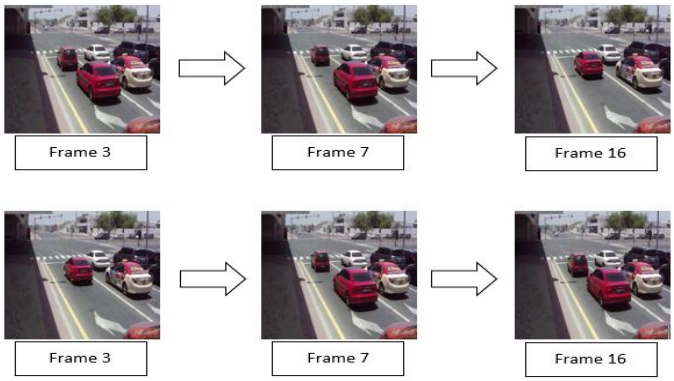

Fig. 5. Frame shuffling attack example. In first row the original frame sequence with frame 3, frame 7, and frame 16. After attack, the second row of the frames shows the altered frame sequence with frame shuffling attack in which the position of frame 3 and frame 16 have been changed.

V. Typical Video Authentication System

A video authentication system is consisting of two basic steps: Authentication process and verification process. Ideal and effective video authentication system have to follow the properties including sensitivity to changes, strength to benign operations, sensitivity against false alarm, self-recovery of modified regions, compactness of authentication data, localization and computational feasibility. In the authentication process, the authentication method processes the feature that taken out from the video and outputs the authentication data that is certainly encrypted by using the encryption key to form the signature [2][18].

In verification process, the video credibility is approved by determine the new authentication data through the use of the exact same authentication method. Then the new authentication data is compared with the original authentication data. The

video will be treated as authentic if both authentication data are matched otherwise it is construed to be tampered [4][17].

VI. Previous Related Work

Researchers have done some work in the area of video authentication and several methods are presented on the subject of digital video authentication. The methods that have been done to match specific requirements but their techniques have one or more weak points. Basically, two techniques have already been implemented: digital signature and digital watermarking. This paper focus on the digital signature video authentication.

In [11] proposed a new method for digital video authentication that depends on video statistical local information. In this method, SVM (Support Vector Machine) classifier has been not used. However, this method approved to be efficient and trusted. The proposed method was evaluated on the dataset of videos, eight different attacks in each video were completely inserted and the method can successfully detect the attacks with overall classification accuracy 96.77%.

In [12] proposed a signature-based video authentication method to improve the digital video authentication in surveillance system using histogram of oriented gradient of the selected DCT (discrete cosine transform) coefficients in three dimensions. In this method, the result depends on optimal threshold that need a high threshold to ignore all tampered. The experiment results show that video with modification is ignored when using high threshold.

In [13] presents an algorithm which helps to determine whether the video is tampered or not. The algorithm is divided in two steps: computing the repeated frames and computing the tampering attack. Local information is determined and SVM classifier is successfully applied to classify whether the digital video is tampered or not.

VII. The Proposed Plexus Method

In this work, a new method called PLEXUS is proposed to address digital video authentication challenges and proved to be an efficient and high accuracy method. In the authentication part that done by the sender, the method generates a signature by multiplying first frame with the private key $f_1 * K$ to generate a new authentication image i_1 then multiplying second frame with the private key and the authentication image $f_2 * K * i_1$ to generate a new authentication image i_2 and this process will continue until reaching the last frame f_n and the signature can be generated by multiplying the last frame with the private key and the last authentication image $f_n * K * i_{n-1}$.

The embedding process between the frames, private key, and authentication images actually done between the three images by adding each color pixel-by-pixel and then divide the result by three which represent the number of images except first stage when the first frame only adding with private key and then divide the result by two. Embedding process diagram between first frame and private key is shown in Figure 6. Embedding process diagram between second frame, private key, and authentication image is shown in Figure 7

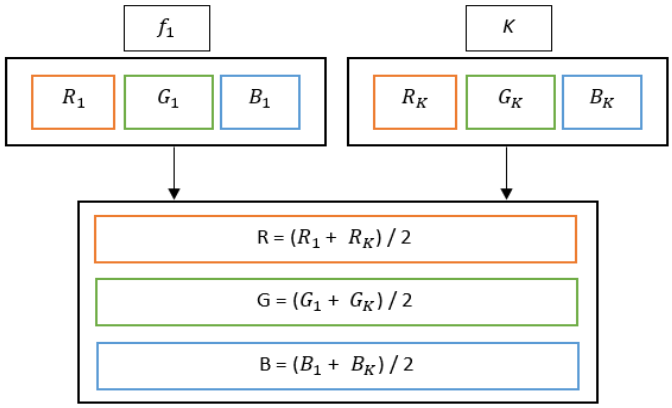

Fig. 6. Multiplication Process between First Frame and Private Key.

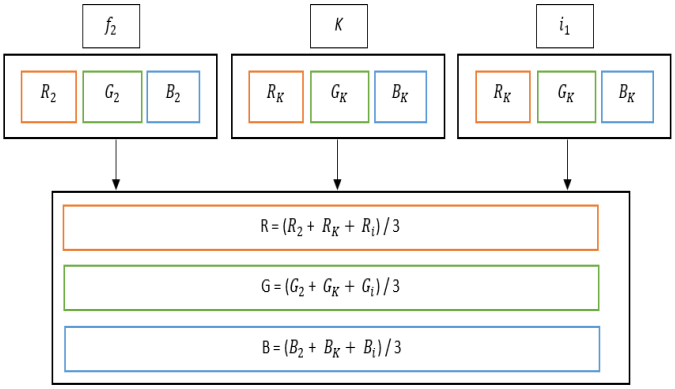

Fig. 7. Multiplication Process between Second Frame, Private Key, and Authentication Image.

In RGB color model, each pixel contains three colors which represent Red, Green, and Blue. The PLEXING process is the multiplication between these colors. This process will be divided into three steps: (1) Red color remains unchanged and the multiplication process will be done between green and blue colors (GB). The pixel three colors will be R GB GB. (2) Green color remains unchanged and the multiplication process will be done between red and blue colors (RB). The pixel three colors will be RB G RB. (3) Blue color remains unchanged and the multiplication process will be done between red and green colors (RB). The pixel three colors will be RG RG B. These steps will be applied to each pixel in the image while accessing the last pixel.

In verification part that done by the receiver, this process will be repeated to generate a signature. Each signature will be compared using image quality similarity measurement to determine whether the video is tampered or not. The authentication accuracy will be higher rate when increasing the number of frames. The overall PLEXUS method diagram is shown in Figure 8.

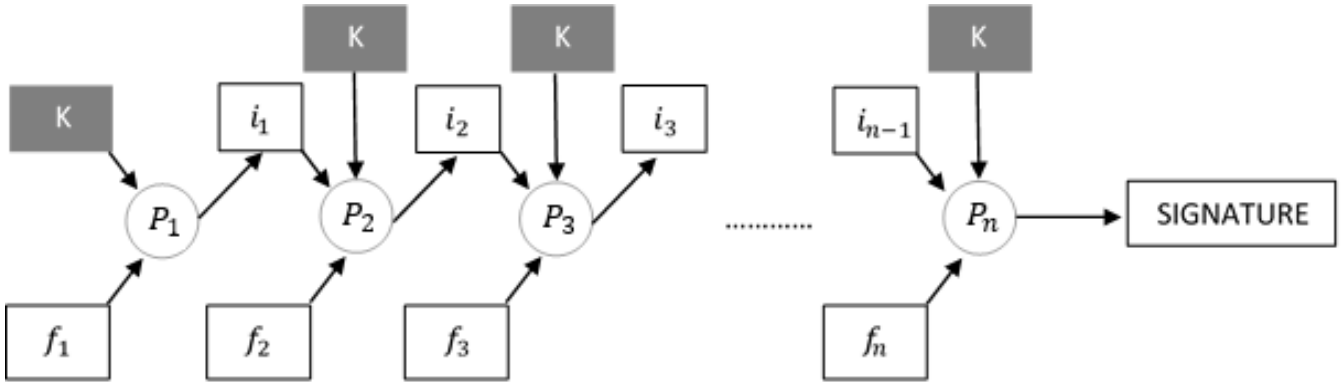

Fig. 8. Overall PLEXUS Method Diagram.

A. Frame Quality Measurement

The digital image can be affected by different types of distortions when passing through several processing stages. Image processing stages can lead to important loss of information or quality. Different metrics are utilized to estimate digital video quality. In image quality evaluation there are basically two methods: subjective and the objective methods. The subjective method quality evaluation being considered as time consuming because it is depending on human evaluation and work without references to specific considerations. The objective quality evaluation takes advantage of automatic algorithms to determine the quality of the image without human interfere [6][14].

The most popular are the objective methods: PSNR (peak signal-to-noise ratio) and MSE (mean-squared-error). The two measurements are based on pixel-by-pixel comparison and its parameters are frequently used for simple identification, but they do not reflect the perceptions of the recipient. To reach the best quality, PSNR should be the biggest and MSE should be the smallest [14][19].

1) MSE – Mean Squared Error

MSE is objective method represent the average of the squared differences between the luminance values of corresponding pixels in two different frames. It is possible to evaluate the degree of image reconstruction by a decoder and do not consider any peculiarity of HVS (human visual system) [14]. MSE is definitely non-negative, and should be as small as possible. Given a noise free $m * n$ monochrome image I and its noisy approximation I'. MSE mathematical representation can be shown in the equation bellow:

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} ([I(i,j) - I'(i,j)])^2 \qquad (1)$$

2) SNR (Signal-to-Noise-Ratio) AND PSNR (Peak Signal-to-Noise-Ratio)

SNR measure used in science and engineering that compares the level of a desired signal to the level of background noise. SNR ratio is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise [14][19].

PSNR is objective method that measure image quality based on the pixel difference between two different images. It is the most commonly used measurement metric describes the ratio of peak to noise [19]. The SNR measure is an estimation of quality of reconstructed image as compared with original image. PSNR mathematical representation can be shown in the equation below:

$$PSNR = 10. log_{10} \left(\frac{{MAX_I}^2}{MSE} \right) \qquad (2)$$

Where, MAX_I is the maximum possible pixel value of the image.

VIII. Result and Discussion

This work is done using a laptop with Intel(R) Core (TM) i5, CPU 2.40 GHz, 8 GB RAM. Visual Studio Community 2017 with Visual Basic programming language.

First, we would take the input video (37 second length) and then extract two frames per second (each frame 450x450 pixels with PNG format) as shown in Figure 9.

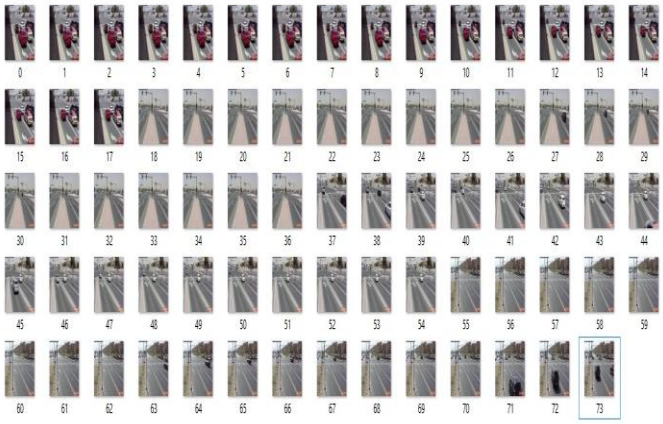

Fig. 9. Frame Extraction (74 Frames).

Second, the sender and receiver choose a private key. The private key is also an image (750x540 pixels with JPG format) as shown in Figure 10. Finally, PLEXUS method will work to generate a signature (sender signature) as shown in Figure 11.

The receiver should apply the previous steps for verification process. The receiver will generate a signature (receiver signature) and compare this signature with sender signature. The video is not tampered if both sender and receiver signatures are matched as shown in Figure 12. Otherwise, the video is tampered (Frame 70 is removed) as shown in Figure 13. This method achieves high accuracy and tested on 10 different digital videos. Then, this method evaluated using different evaluation measurements including: SNR and PNSR.

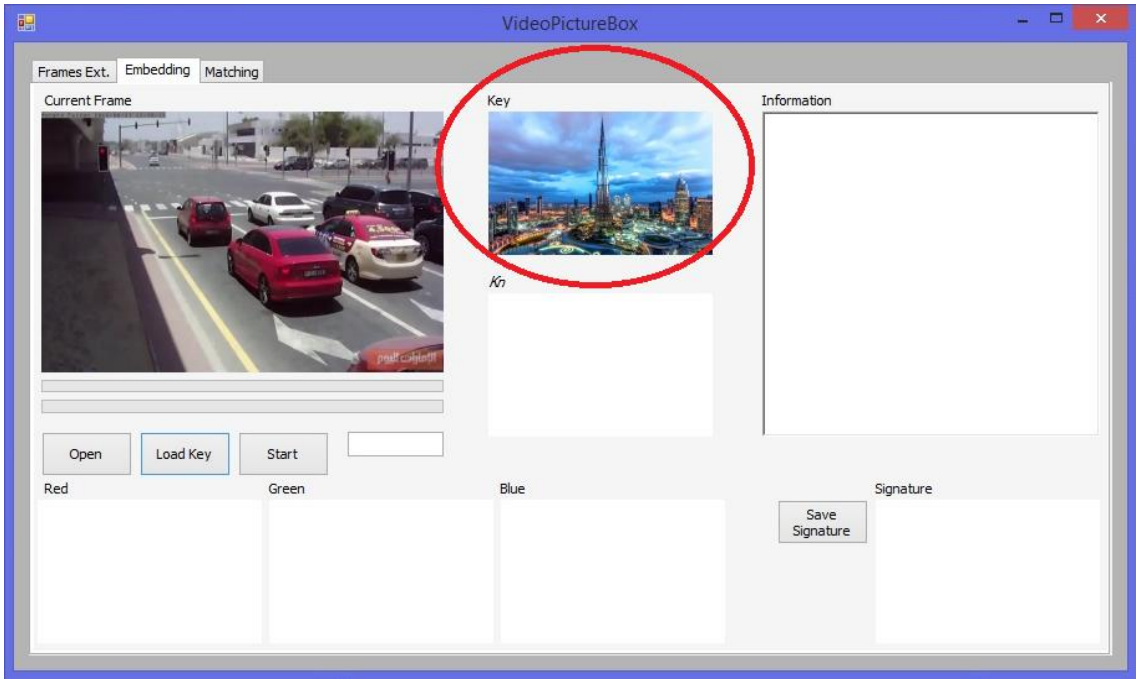

Fig. 10. Choosing Private Key.

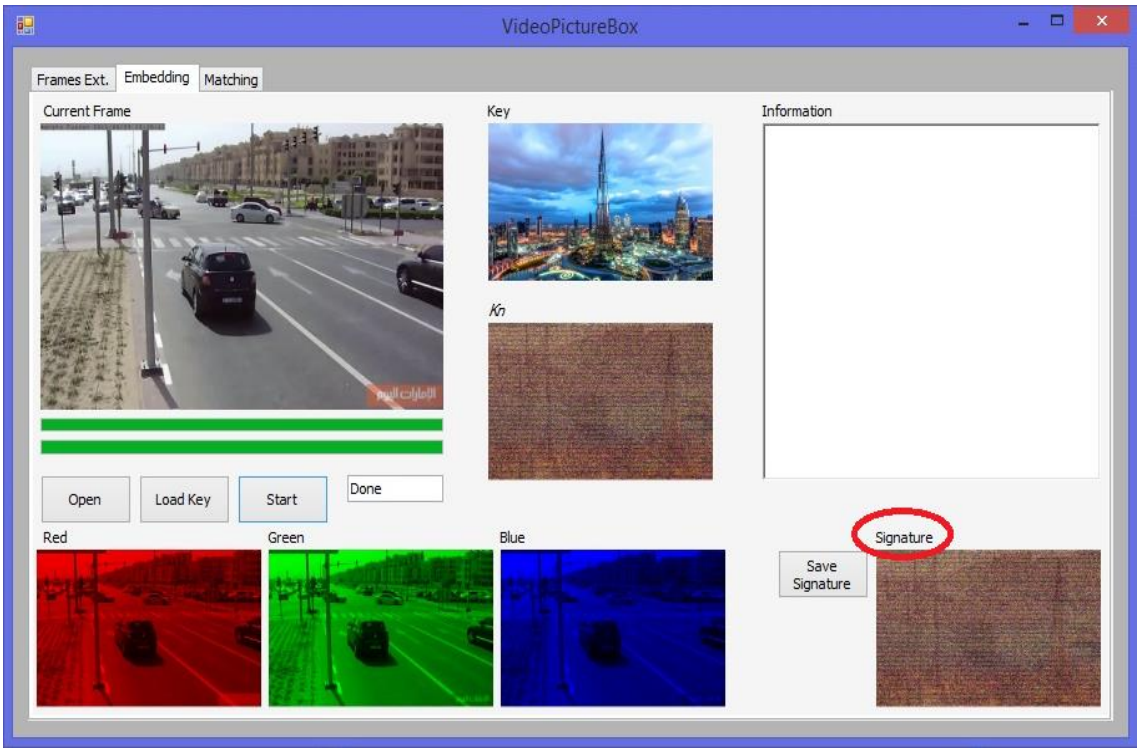

Fig. 11. Generate Sender Signature.

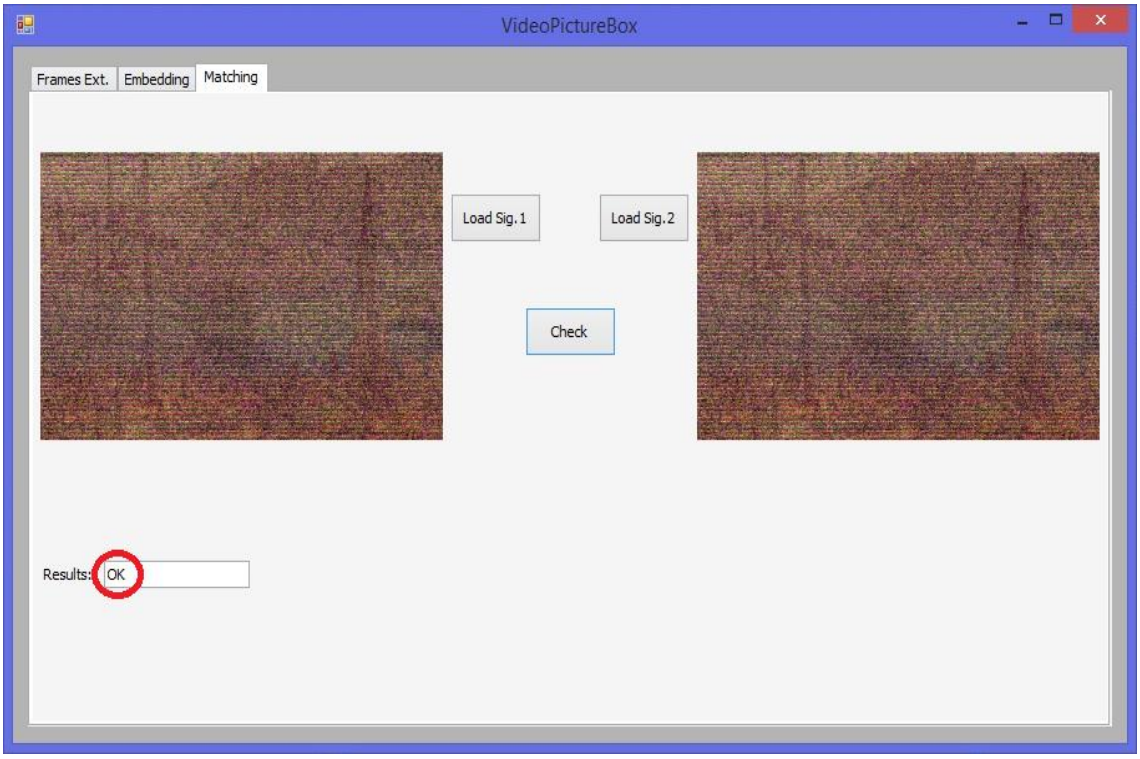

Fig. 12. Verification Process (Not Tampered Video).

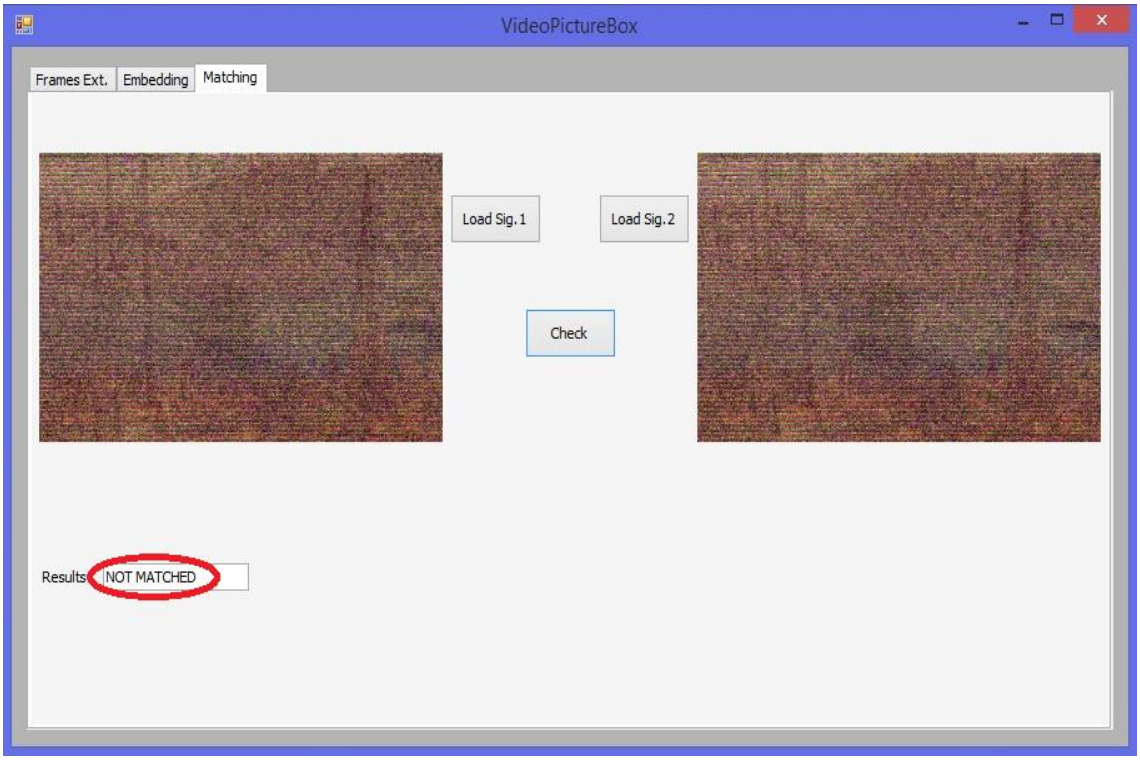

Fig. 13. Verification Process (Tampered Video).

The evaluation results including SNR and PSNR in the proposed method applied on two frames which are frame1 and signature as examples, because to find the final result we must apply this evaluation measurements on all video frames. The result of SNR= 3.4964 and PSNR= 8.9078.

IX. CONCLUSION

Video authentication is certainly really challenging issue in computer science area and very important subject in several applications specially with the growing of development tools

which are available in video editing software. The digital video can be exposed to tampering attacks which means the video content is not trusted.

In this paper, we proposed a new video authentication method called PLEXUS to improve the reliability of digital video against temporal attacks. This method consists of two basic steps: authentication step and verification step. In each step a signature will be generated and then the two signatures will be compared and must be matched if the video is not tampered. This method is tested using 10 different videos and achieve high accuracy.

REFERENCES

[1] Sethulekshmi U. S, Remya R. S, Mili Rosline Mathews. "A Survey on Digital Video Authentication Methods." International Journal of Computer Trends and Technology (IJCTT) – volume 22 Number 1– April 2015

[2] Lo, Chun-Chi, and Yu-Chen Hu. "A novel reversible image authentication scheme for digital images." Signal processing 98 (2014): 174-185.

[3] Yeswanth.P, Pothumani.s, "Tampering Detection in Digital Videos." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 3, March 2015.

[4] Atrey, Pradeep K., Wei-Qi Yan, and Mohan S. Kankanhalli. "A scalable signature scheme for video authentication." Multimedia Tools and Applications 34, no. 1 (2007): 107-135.

[5] Upadhyay, Saurabh, and Sanjay Kumar Singh. "Video authentication: Issues and challenges." International Journal of Computer Science 9, no. 2012 (2012).

[6] He, Dajun, Qibin Sun, and Qi Tian. "A secure and robust object-based video authentication system." EURASIP Journal on Advances in Signal Processing 2004, no. 14 (2004): 545469.

[7] Upadhyay, Saurabh, and Sanjay Kumar Singh. "Video authentication-an overview." International Journal of Computer Science and Engineering Survey 2, no. 4 (2011): 75.

[8] Christian, Aldrina, and Ravi Sheth. "Secured Digital Video Authentication System." (2017).

[9] Vartak, Reshma, and Smita Deshmukh. "Survey of Digital Image Authentication Techniques." International Journal of Research in Advent Technology 2, no. 7 (2014): 176-179.

[10] M. AL-ATHAMNEH, F. KURUGOLLU, D. CROOKES, M. FARID. "Video Authentication Based on Statistical Local Information." 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing.

[11] Al-Athamneh, Mohammad, Fatih Kurugollu, Danny Crookes, and M. Farid. "Video authentication based on statistical local information." In Utility and Cloud Computing (UCC), 2016 IEEE/ACM 9th International Conference on, pp. 388-391. IEEE, 2016.

[12] Kroputaponchai, Teerasak, and Nikom Suvonvorn. "Video authentication using spatio-temporal signature for surveillance system." In Computer Science and Software Engineering (JCSSE), 2015 12th International Joint Conference on, pp. 24-29. IEEE, 2015.

[13] Gupta, Ankita, Shilpi Gupta, and Anu Mehra. "Video authentication in digital forensic." In Futuristic Trends on computational analysis and knowledge management (ABLAZE), 2015 International Conference on, pp. 659-663. IEEE, 2015.

[14] Komal, A., Shipra Khurana, and Amit Kumar. "Comparative analysis of image quality assessment using HVS model." IJIRCCE 2, no. 7 (2014): 5033-5038.

[15] Berge, L.A., Dangler, J.R., Doyle, M.S., Liang, T.W. and Orozco, M., International Business Machines Corporation, 2018. TAMPERING DETECTION FOR DIGITAL IMAGES. U.S. Patent Application 15/376,314.

[16] Sowmya, K. N., H. R. Chennamma, and Lalitha Rangarajan. "Video authentication using spatio temporal relationship for tampering detection." Journal of Information Security and Applications 41 (2018): 159-169.

[17] Sowmya, K. N., H. R. Chennamma, and Lalitha Rangarajan. "Video authentication using spatio temporal relationship for tampering detection." Journal of Information Security and Applications 41 (2018): 159-169.

[18] Gusev, Pavel D., and Georgii I. Borzunov. "The Analysis of Modern Methods for Video Authentication." Procedia Computer Science 123 (2018): 161-164.

[19] Mohsen, Asmaa Hasan, and Shaimaa Hameed Shaker. "Authentication of Digital Video Encryption." Iraqi Journal of Science 57, no. 4C (2016): 2954-2967.