International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 9, pp 62-65, September-2022

https://doi.org/10.47001/IRJIET/2022.609009

Video Authentication Using Elliptic Curve Encryption Algorithm

[1]Rahma Nazar Ibrahim, [2]Shahd Abdulrhman Hasso

[1,2]Software Engineering Department, University of Mosul, Mosul, Iraq

Authors E-mail: [1]roraalhayali2@gmail.com, [2]shahd_hasso@uomosul.edu.iq

***Abstract* - A video record plays a crucial role in providing evidence for crime scenes or road accidents. However, the main problem with the video record is that it is often vulnerable to various video tampering attacks. Although visual evidence is required to conduct an integrity verification before investigations, it is still difficult for human vision to detect a forgery, we suggest applying the feature extraction technique for each frame in the video file (except for the first frame) and then calculating the hash function to find a fixed length and then apply the elliptic curve algorithm to the resulting value from the Hash function and then hide the encoder output in the video itself.**

Keywords: Video tampering detection, video integrity, elliptic curve cryptography (ECC), Digital Media.

I. INTRODUCTION

Video authentication is still a topic of great interest and attraction to researchers in the past few years as digital video authentication is the technology of determining whether a transmitted video is authentic and has not been tampered with. He also added challenges related to information [1].

Video manipulation is now within the reach of any lay person due to the easy availability of many video editing tools in the open source platform. Simple PC or mobile devices In a surveillance system where digital video is essential, modification is unacceptable which greatly reduces the reliability of the video [2][10].

Security and privacy issues in multimedia technology have become an important concern Many multimedia applications require secure transmission, the level of security required depends on the sensitivity of the information in these applications different types of video applications require different levels of security. For example, for video-on-demand, it will be Low security is a good thing, while for military or financial information purposes, a high level of security is required to completely prevent unauthorized access [3][9].

1.1 The electronic message's digital finger print

Although encryption prevents snoopers from seeing the contents of a message, it does not prevent vandals from tampering with it. That is, encryption does not guarantee the integrity of the message (integrity). Hence the need for the message digest, which is a digital fingerprint that is, derived according to certain algorithms called hash functions. These algorithms apply mathematical calculations to the message to generate a fingerprint (small string) that represents an entire file or message. (Big series). And the electronic fingerprint of the message can distinguish the original message and identify it accurately, so that any change in the message, even if it is in one bit - will lead to a completely different electronic fingerprint of the message, It is not possible to derive the same electronic fingerprint from two different messages.

Electronic fingerprints are distinguished from each other according to the private keys that generated them, and they can only be decrypted using the public key belonging to them. This is why the blur coupling used to create the fingerprint is called another name, the one-way hash function that using the fingerprint algorithm is faster than doing asymmetric encryption using the public key text, and that's why the fingerprint algorithm is used Electronic creation of digital signatures [6].

1.2 Elliptic Curve Cryptography (ECC)

It is a type of public key cryptographic system, such as RSA, that offers the same level of security with shorter keys Using shorter keys provides less space for key storage, which saves time. In order to design a new system, we need to understand what is expected of the new system. The requirements are that it should be mathematically strong as in RSA it should have a strong mathematical base and machines should not be able to solve it easily Ideally we need something that does the same job faster and something that takes up less space as computers get more powerful, we'll need something that doesn't require us to constantly increase the size of the key in order to keep up with the machines. This is where the elliptical curves come in. [7][8]

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 9, pp 62-65, September-2022

https://doi.org/10.47001/IRJIET/2022.609009

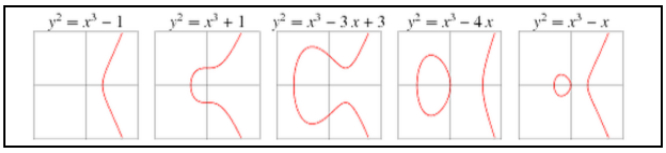

Figure 1: Different shapes of elliptical

Table 1: Security levels for some symmetric and asymmetric encryption algorithms

Encryption type	Algorithm	Bit security level			
		80	128	192	256
Symmetric	Advanced standard encryption (AES)	80	128	192	256
Asymmetric	(RSA)	1024	3072	7680	15360
	Elliptic curve Cryptography (ECC)	160	256	384	512

II. RELATED WORK

In this [1], we propose a new video authentication method. PLEXUS is a method for improving digital dependability and sporadic video assaults. There are two steps in this process. Basic actions Steps of authentication and verification In each instance, The two signatures, as well as the signature function, will be created. If the video is authentic, they will be compared and should match.

An improved approach for verifying the integrity of the videos is proposed in [2] using the watermark method. The technique isolates the header and time code hash values from the actual video data in order to distinguish between attacks and natural changes. According to the review research, the integrity check algorithm is superior to current methods that apply the concepts of a digital signature.

In [4] a proposed method for compressed video encryption was made available. Using this proposed algorithm, highly confidential video files might be sent safely so as to be protected from illegal viewing. By applying the compression technique to the video before the encryption, they achieve a balance between security and processing time since the compression method uses less bandwidth and less storage. Since the authors did not utilize steganography, data can be concealed within the movie's encryption frames to boost video security.

In [5], a method of improving digital video authentication in surveillance systems using a three-dimensional histogram of oriented gradient of chosen DCT (discrete cosine transform) coefficients was described. The effectiveness of this strategy depends on the appropriate threshold, which must be high in order to disregard any tampering. The outcomes of the experiment demonstrate that when applying a high threshold, modified footage is disregarded.

III. PROPOSED METHOD

In the proposed method, the video is taken as input and separated into frames where the properties of the frames are extracted after the hash algorithm called SHA-512 is used to calculate the hash values for all these frames where these are plaintext. Then it is encoded by the elliptic curve algorithm. The generated hash value is sent with video to the receiver, the recipient checks Video integrity by separating frames first and then Retail account. If the hash values match there is no messing around.

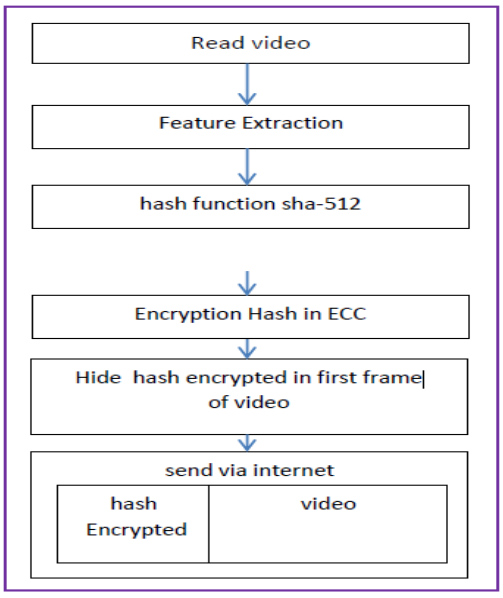

Figure 2: Sender system

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 6, Issue 9, pp 62-65, September-2022
https://doi.org/10.47001/IRJIET/2022.609009

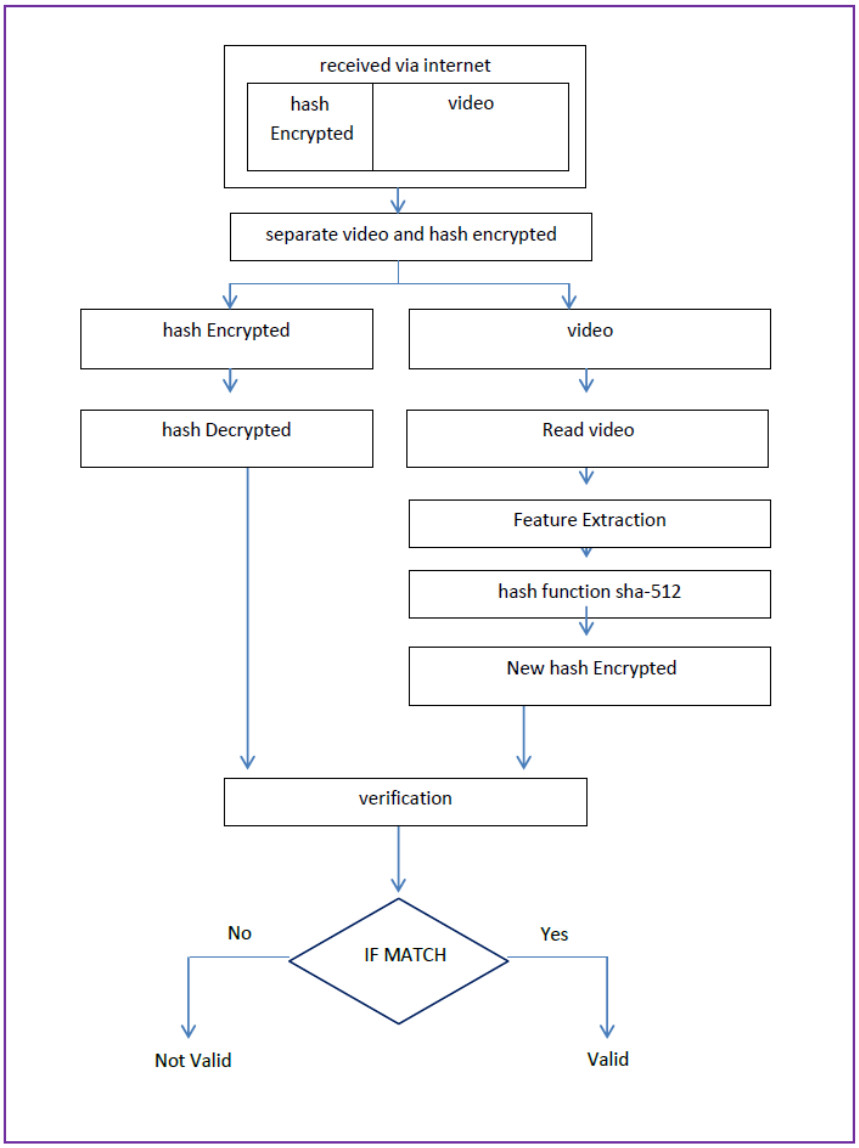

Figure 3: Receiver system

IV. CONCLUSION

In this paper, we proposed a new method for video based on extracting video properties and encoding it using the sha512 camouflage function in order to achieve the integrity of video data and then encode it with ECC algorithm in order to achieve authentication and masking of the encrypted data in the first video frame and send it over the Internet to the recipient, Upon receipt, the hidden data is extracted and decrypted. Attributes are extracted and the hash is calculated for the received video. After that, we compare the decrypted hash with the new hash to verify the validity of the video clip through comparison. Experimental results show that the proposed method is much stronger against tampering detection of other traditional computer-equipped methods environment, as well as in an embedded system. In addition to, Computational complexity analysis in ECC, a higher level of security compared to traditional methods.

REFERENCES

[1] Abdulwahab, Hala Bahjat, Khaldoun L. Hameed, and Nawaf Hazim Barnouti. "Video Authentication using PLEXUS Method." *(ijacsa) International Journal of Advanced Computer Science and Applications* 9.11 (2018).

[2] Echizen, Isao, et al. "Integrity verification system for video content by using digital watermarking." *2006 International Conference on Service Systems and Service Management*. Vol. 2. IEEE, 2006.

[3] Parmar, Zarna, and Saurabh Upadhyay. "A review on video/image authentication and temper detection techniques." *International Journal of Computer Applications* 63.10 (2013).

[4] Kulkarni, Ajay, et al. "Proposed video encryption algorithm v/s other existing algorithms: A comparative study." *arXiv preprint arXiv:* 1303.3485 (2013).

ISSN (online): 2581-3048
Volume 6, Issue 9, pp 62-65, September-2022
https://doi.org/10.47001/IRJIET/2022.609009

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

[6] https://aljanbh.yoo7.com/t136-topic

[7] https://prateekvjoshi.com/tag/cryptography/

[8] Nabil, G., Naziha, K., Lamia, F., & Lotfi, K. (2012, July). Hardware implementation of elliptic curve digital signature algorithm (ECDSA) on Koblitz curves. *In 2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)* (pp. 1-6). IEEE.

[9] A Hasso, Shahd, and Taha B Taha. "A New Tamper Detection Algorithm For Video." *Journal of Engineering Science and Technology (JESTEC)* 15.5 (2020): 3375-3387.

[10] PARMAR, Zarna; UPADHYAY, Saurabh. A review on video/image authentication and temper detection techniques. *International Journal of Computer Applications*, 2013, 63.10.

Citation of this Article:

Rahma Nazar Ibrahim, Shahd Abdulrhman Hasso, "Video Authentication Using Elliptic Curve Encryption Algorithm" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 9, pp 62-65, September 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.609009

****

