Digital Watermarking for Enriched Video Streams in Edge Computing Architectures Using Chaotic Mixtures and Physical Unclonable Functions

Borja Bordel[1(✉)] and Ramón Alcarria[2]

[1] Department of Computer Systems, Universidad Politécnica de Madrid, Madrid, Spain
borja.bordel@upm.es

[2] Department of Geospatial Engineering, Universidad Politécnica de Madrid, Madrid, Spain
ramon.alcarria@upm.es

Abstract. Authentication in advanced video applications is a pending challenge, especially in those scenarios where video streams are enriched with additional information from sensors and other similar devices. Traditional solutions require remote devices (such as cameras) to store private keys, a situation that has been proved to be very risky. On the other hand, standard authentication methods, such as digital signatures or secure sessions, prevent systems to operate at real-time, as they are very computationally costly operations which, besides, are designed to work with information blocks, not with streams. Other solutions, furthermore, require the integration of gateways or aggregation points in video infrastructures, which creates bottlenecks and difficulties the dynamic adaptation of systems to the environmental conditions and devices' lifecycle. Therefore, in this paper, we address this problem by proposing an authentication procedure based on digital watermarking. In our proposal, video infrastructures are organized as edge computing architectures, where enriched video streams are protected by watermarks and devices may delegate functionalities dynamically. This new watermarking technology is based on chaotic mixtures and secret keys provided by Physical Unclonable Functions. In order to evaluate the performance of the proposed solution an experimental validation is also carried out.

Keywords: Digital watermarking · Physical Unclonable Functions · Chaotic systems · Edge computing · Security · Authentication

1 Introduction

Augmented reality is one of the most promising technologies nowadays [4]. Although most popular applications involve users immersed in enriched environments, relating with devices through smart phones and other similar devices;

I. You et al. (Eds.): MobiSec 2019, CCIS 1121, pp. 112–125, 2020.
https://doi.org/10.1007/978-981-15-9609-4_9

other solutions may be created using this new approach. In particular, surveillance systems composed of video infrastructures can be improved by integrating additional information into video streams [1]. These advanced mechanisms produce enriched video streams where visible information is augmented with addition data such as temperature, positioning, etc. [6].

These advanced applications, any case, must meet two essential requirements. First, enriched video streams must be generated, sent and consumed at real-time. That is especially relevant where critical infrastructures (such as borders) are protected by these solutions. And, second, in order to guarantee the availability and reliability of the hardware infrastructure and the surveillance service, the hardware platform and software components must be able to dynamically adapt to the environmental conditions and the devices' and software modules' lifecycle.

These requirements are, currently, fulfilled by most video solutions, such as cameras, real-time video processing algorithms, etc. including those developed for systems with sparse resources. However, security mechanisms are still complicated to integrate in that kind of technologies. As a consequence, most video systems are still manually configured, so although they can dynamically adapt to the environmental conditions [7], they cannot remove or add elements in the infrastructure in a fast, secure and automatic manner. In fact, authentication mechanisms are still far to be lightweight, dynamic or real-time.

On the one hand, most typical authentication mechanisms are too slow. To avoid the use of onerous certificates Identity-Based Signatures (IBS) [16] appear as a way to permit secure bootstrap in a local spaces. However, secure sessions require complex initiation procedures and digital signatures are designed to work with information blocks, not with video streams [23]. Streams could be split into different packets, but this process would be very computationally heavy. Besides, mathematical operations required by these mechanisms are very costly, and resource constrained devices may not be able to support those operation. As a possible solution, camera and other similar devices may send their outputs (video and augmented data) to a central aggregation point or gateway, powerful enough to perform those authentication operations at real-time. However, these elements tend to act as bottlenecks and prevent the system to adapt dynamically to the environment, as they are essential elements whose failure causes the entire system fails.

On the other hand, all authentication mechanisms require the device to store a private key (symmetric or asymmetric) or other information used as key, such as the MAC address [19]. These approaches are very unsecure as the key is accessible for everybody with physical access to the devices [5]. That is especially problematic if devices are geographically sparse and unattended.

Therefore, in this paper we investigate a new authentication method based on digital watermarking. Devices will include a watermark in enriched video streams, proving their identity. In order to generate a secure watermark, chaotic mixtures are employed. The key feeding these mechanisms is also generated using Physical Unclonable Functions, so the resulting key is totally secure as it would get destroyed if anyone attempt to access to it.

The rest of the paper is organized as follows: Sect. 2 describes the state of the art on authentication solution for video infrastructures; Sect. 3 contains the main contribution; Sect. 4 presents a first experimental validation based on the proposed simulation scenario; and Sect. 5 concludes the paper.

2 State of the Art

Different proposals for authentication in video systems have been reported in the last years. Probably, the most popular and studied technology is digital signature. This is also the oldest solution. Digital signature schemes to sign every frame in a video stream [27], or solutions to sign streams following specific sequences (including signed frames, partially signed frames and not signed frames) [18]. Moreover, schemes to packetize video into information blocks which may be easily signed have been also reported [29]. As these mechanisms tend to be very heavy and costly, some proposals to turn them into a more scalable approach [2] may be found.

Other approaches consider the content in the video stream to determine if it is a valid flow. Techniques to identify people in video streams have been reported [9,13], although these schemes are only adequate for applications where video is expected to record specific people.

Video integrity and authentication may also be determined using specific algorithms. Mechanisms to detect fake or duplicated frames in video streams have been proposed [14], and noise analyses to detect small electrical perturbations produced by communication networks and evaluate the video integrity may also be found [15].

Most modern proposals are based on artificial intelligence technologies such as neural networks [26] to evaluate video falsifications. Any case, apart from these solutions, many other application-specific mechanisms and algorithms have been reported in the last years to identify the video integrity and authentication [17,28].

The other and second important authentication technology for video streams is digital watermarking. Initial proposals were based on inserting a visible watermark in every frame in a video stream [12], although most modern tampering mechanism were proposed almost immediately [22]. In this context, chaotic watermarking is also a recurrent topic in works about video authentication [8,30]. Solution to integrate digital watermarking into MPEG2 algorithms may also be found [32], and specific watermarking algorithms for surveillance applications have been also reported [3]. Watermarking and authentication algorithms for other video formats, such as H.264, have been also analyzed [31]. Besides, hardware-supported algorithms for video watermarking have been studied [25]. As in the previous technology, application specific watermarking technologies may be found, such as technologies for compressed video [10] and solutions for mixtures of private video and audio streams [11].

In this paper we propose a novel watermarking technology for video authentication, integrating it with other lightweight technologies in order to improve its

performance. In particular, the proposed scheme is developed following an edge computing approach, and chaotic mixtures are employed to generate watermarks in a computationally low-cost way. Besides, in order to improve the security of the global scheme, the secret key employed in the watermarking algorithm is generated by Physical Unclonable Functions, which may produce long keys using simple hardware devices and technologies.

3 A New Authentication Method Based on Digital Watermarking

We are modeling a video application as a mathematical function (1), representing all operations from video generation, to data collection and integration, and watermark injection and authentication. This function may be decomposed on several different components, each one representing an atomic operation (2): video generation and temperature measuring among other functionalities (depending also the particular application under study).

$$\mathcal{F}(\cdot) = f_1 \circ f_2 \circ ... \circ f_N \tag{1}$$

$$\mathcal{F}(\cdot) = f_1(f_2(...f_N(\cdot))) \tag{2}$$

In respect to the digital watermarking mechanism f_{mark}, four different atomic operations may be identified (3): key generation f_k, watermark generation f_w, video decomposition f_v and watermark insertion f_i (four atomic operations, in fact, one for each component -blue, red, green and luminosity-). Equally, the watermark extraction may be understood as the combination of another four atomic operations.

$$f_{mark}(\cdot) = f_k \circ f_w \circ f_v \circ f_i \tag{3}$$

These atomic operations may be performed by a single device, or performed by a collection of devices, according to the environmental conditions at each particular moment. To reach that objective, the proposed algorithm, as we are seeing, is composed of four totally independent operations, so they could be performed, if needed, by four different elements. This approach is usually known as edge computing. Three different layers are identified in edge computing architectures: cloud, fog, edge and physical layer (see Fig. 1).

In our proposal, video (together with the additional data) is generated at physical layer, but it is processed and marked at edge layer. However, if required, some of the atomic operations needed to mark enriched video streams may be delegated to the physical layer, or to the fog or cloud layers (although this second option is not recommendable, as an unprotected video stream will be sent through unsecure communication networks).

Next subsection will describe the algorithms included in each one of the described atomic operations.

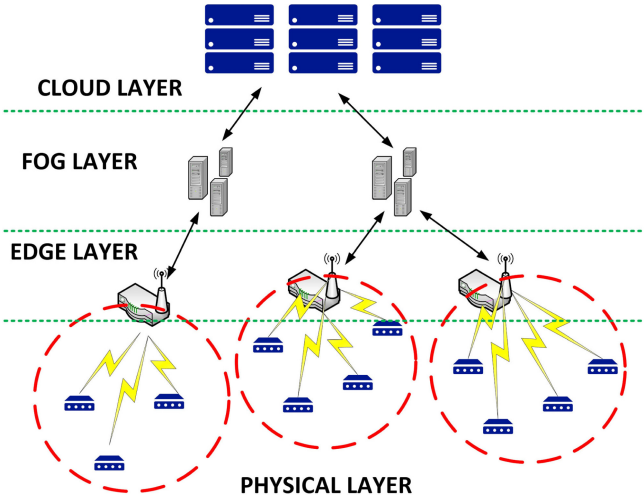

Fig. 1. Edge computing architecture

3.1 Digital Watermarking

Digital watermarking is a stenography technique (technology to hide private information in common elements), employed to hide copyright or identity data in digital materials such as videos or images. Although different schemes have been reported, in the most common one, the marking algorithms takes three inputs: the original object, the key, and the mark to be inserted. As output it is obtained the marked object (see Fig. 2).

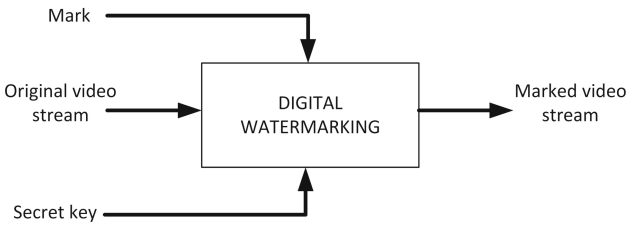

Fig. 2. Architecture of a digital watermarking scheme

In general, four different types of watermarks are defined:

- Private watermarking: In this case, using the original object, the key, the watermarked and the marked object, it is determined if the marked object was marked by an honest sender.
- Half-private watermarking: In these algorithms, the objective and approach is similar to private watermarking; however, in this case, the original object is

nor required to determine if the marked object was manipulated by an honest sender.
- Public watermarking: These algorithms are different, as they are focused on obtaining the hidden watermark or hidden information in the marked object. To recover that information, these algorithms only need the marked object and the key.
- Visible watermarking: Contrary to public watermarking, in this case the objective is to recover the original object from the marked object, not the hidden information. To recover the original object, these algorithms only require the marked object and the key.

Figure 3 shows the watermarking procedure proposed in our solution. As can be seen, it is a hybrid approach. The proposed mechanism reconstructs both, the hidden watermark (employed to authenticate the sender) and the original object (the enriched video stream).

In the first step, the video stream is split into four different streams, one per each basic color (blue, red and green) and one additional component for luminosity. The algorithm employed to extract these four components is very simple and may be found in the state of the art [20]. Then, each component is marked independently, before reconstructing the global video stream another time and send it to its destination (usually the cloud), where sender identity is authenticated.

In order to guarantee the frames in the video stream are not severely degraded, each color component (channel) is manipulated in the frequency spectrum, not in the temporal-spatial domain. To do that, the second step in the proposed mechanism is a discrete wavelet transform (DTW). In particular, in order to preserve spatial information, we are employing the Daubechies wavelet. The proposed algorithm may be based on any level of coefficients. In general, we are employing the j-th level coefficients.

On the other hand, the watermark is generated using chaotic mixtures. As can be seen in Fig. 3, in the proposed scheme the secret key is only injected in the watermark generation module. In that way, it is reduced at maximum the agents which must know and manipulate the key. Section 3.2 is describing the watermark generation process.

Once the watermark to be inserted is generated (see Sect. 3.2), a watermarking algorithm is run. This algorithm considers a watermark with dimensions $M \times N$ pixels. Frames in the video stream are considered to have $Q \times S$ pixels. Then, pixels in the video frames are analyzed in blocks of $Q/M \times S/N$ pixels. It is calculated the spatial mean vale of pixels in this block, $E[B]$, and the value of the pixel in the central point, p_{center}. If the center of this block is not uniquely defined (in a geometric sense), it must be selected which pixel is going to be considered the center. Besides, we are considering a degradation threshold, Th_{deg}. If difference between the spatial mean in the block and the value of the central pixel is above this threshold (4), it is considered this block has a relevant

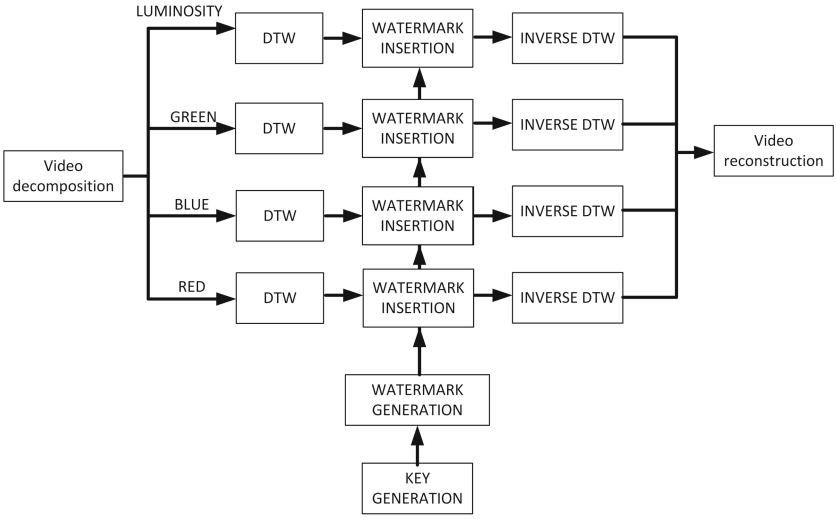

Fig. 3. Architecture of the proposed digital watermarking scheme

entropy, so pixels cannot be modified without a relevant information lost. Thus, in this case, the watermark is not inserted in that block.

$$Th_{deg} \leq |E[B] - p_{center}| \tag{4}$$

If this condition is met, then, the value of the central pixel is modified according to the insertion function (5). In this expression, W represents the watermark and i and j are spatial indexes which are scrolled from left to right and from top to bottom.

$$p_{center}^{new} = p_{center} + \frac{10}{9} W(i,j) \cdot |E[B] - p_{center}| \tag{5}$$

After watermark insertion, the four independent color channels are aggregated another time, and enriched video stream reconstructed.

3.2 Watermark Generation Through Chaotic Mixtures

A chaotic mixture is a procedure to increase the entropy of images. In the proposed algorithm, we are considering a coherent watermark with $M \times N$ pixels, which must be randomized before being inserted. To perform this process, we are using a chaotic map (6) which is iterated a certain number of times, R. This map indicates the position T^r where the (i, j) pixel must be placed after the iterations.

$$T^r(i,j) = A(\boldsymbol{k})T^{r-1}(i,j) = A^r(\boldsymbol{k})T^0(i,j) \quad r = 1, ..., R \tag{6}$$

The watermark W is a binary image, where pixels can take two values: 1 or -1 (instead of zero). Moreover, the matrix $A(\boldsymbol{k})$ represents a chaotic function.

Typically, this matrix represents the logistic map or other similar and well-known functions. In this case, however, in order to increase entropy as much as possible, we are selecting more complex chaotic dynamics. In particular, we are employing the linearized Lorenz system [21] (7–8). As the Lorenz system is a three-dimensional system, marks are only bidimensional, we must extend the matrix T^r to be three-dimensional (9). Besides, in order to guarantee the image keeps its dimensions, operations are defined on cycle groups (9).

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= \rho x - y - xz \\ \dot{z} &= xy - \beta z \end{aligned} \tag{7}$$

Being σ, ρ and β positive real parameters

$$A(\boldsymbol{k}) = \begin{pmatrix} -\sigma & \sigma & 0 \\ \rho - k_3 & -1 & -k_1 \\ k_2 & k_1 & -\beta \end{pmatrix} \tag{8}$$

$$T^r(i,j) = A^r(\boldsymbol{k}) \begin{pmatrix} x_i \\ y_j \\ 1 \end{pmatrix} \begin{pmatrix} modM \\ modN \\ -- \end{pmatrix} \quad r = 1, ..., R \tag{9}$$

It is also considered a vector $\boldsymbol{k}$, which is the key of the watermarking generation algorithm. This key, in the context of the proposed algorithm, it is the point around which the Lorenz system is linearized (10). Parameters σ, ρ and β must be selected to make the Lorenz system chaotic, although as there are several different possibilities, these parameters may also be understood as a key. Moreover, the number of performed interactions, R, may also be considered as a secret key. After this operation, we are obtaining a binary watermark with a great entropy, which is perfect to be injected into enriched video streams as authentication mechanism.

$$\boldsymbol{k} = (k_1, k_2, k_3) \tag{10}$$

3.3 Secret Key Generation Using PUF

The last detail we must address to complete the description of this digital watermarking solution is the generation of the secret key. In order to do that, we are using Physical Unclonable Functions (PUF). In particular, we are using magnetic PUF [24] to generate unique and unclonable keys, which can be only produced by devices provided with identical magnetic devices. The proposed PUF, then, will generate a unique response as a combination of harmonic signals with different frequencies and amplitudes (these unclonable values depend on the magnetic material).

Using a lock-in, all these frequencies and amplitudes will be clearly identified and introduced into a processing system. In this processing step different techniques may be employed to translate the unclonable magnetic response of the proposed PUF into a private a unique digital key.

In the simplest and easiest solution, to each combination of electrical signals it is associated a fixed key from a catalogue or table. However, this mapping procedure highly reduces the entropy of the proposed key generator. Thus, in this case it is employed a Σ-Δ encoder to sample the generated signal and create a secure private key, with the desired length (no theoretical limits must be considered).

Figure 4 describes the implementation of a standard Σ-Δ encoder. Mathematically (11), the Σ-Δ encoder may be easily described, considering a bit time T_Δ and the Heaviside function $u[n]$.

$$\begin{aligned} e[n] &= u[m[n] - e_d[n-1]] \\ m_d[n] &= e[n] \cdot (u[n] - u[n - T_\Delta]) \\ e_d[n] &= e[n]T_\Delta + e_d[n-1] \end{aligned} \tag{11}$$

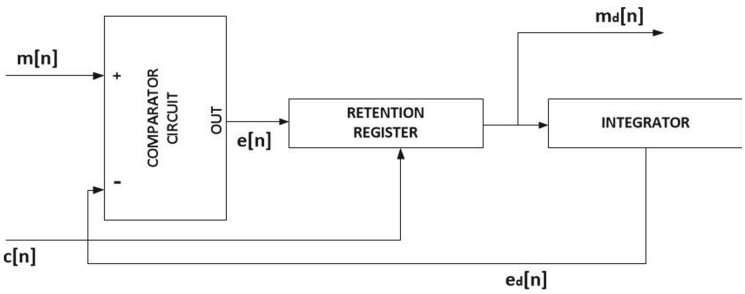

Fig. 4. Basic block diagram for a Σ-Δ encoder

4 Experimental Validation: Simulation Results

In order to validate the proposed solution as a valid technology for authentication in video applications, a simulation scenario was deployed and an experimental validation carried out. Using advanced simulation techniques and the NS3 network simulator a real surveillance application based on video infrastructure and enriched video streams was implemented including the proposed authentication solution. NS3 is a network simulator whose scenarios and behavior are controlled and described by means of C++ programs.

The proposed algorithm was implemented using TAP bridges and ghost nodes, which can integrate real virtual instances into NS3 simulations. In this experiment, virtual instances were defined as Linux 16.04 virtual machines (containers), where the proposed algorithm was implemented and executed using C language and native mechanisms of the operating system.

The proposed simulation scenario is an adaptation of a real video infrastructure. The scenario was designed to present twenty-five (25) nodes in the physical layer, communicating with some gateways in the edge layer and a central

server in the cloud layer. Although the performance of the proposed solution in a real environment may be different from the performance in a simulated scenario, the described simulation is enough close to a real deployment to be an acceptable first experimental validation. In particular, the most important and characteristic aspects of video streams and devices are represented in the proposed simulation.

Each simulation represented thirty hours of operation in the system.

The experimental validation was focused on evaluating the percentage of successful authentications and the overhead the proposed authentication scheme introduces. The first experiment was repeated for different level of coefficients in the DWT and number of iterations in the chaotic mixture. Figure 5 shows the obtained results in the first experiment. The second experiment was repeated for different types of video streams, with various entropy levels, and different numbers of iterations in the chaotic mixture. Figure 6 shows the obtained results in the second experiment

As can be seen in Fig. 5, successful probability is always above 75%. Errors in authentication are more common in low and high values for the number of iterations; and when level one coefficients in the DWT are considered. In that way, if a low number of iterations is going to be considered, level three coefficients should be considered. On the contrary, if medium or large values for the number of iterations are going to be considered, then level two coefficients are preferable.

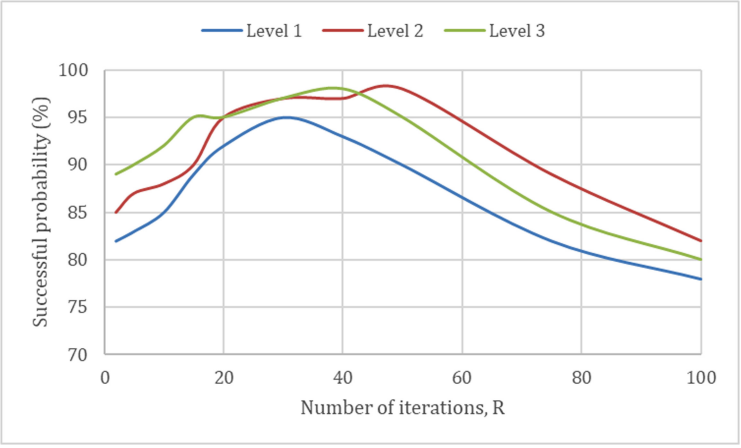

Fig. 5. Results of first experiment: success probability

As can be seen in Fig. 6, introduced overhead is never higher than 15%. In general, for low number of iterations, the introduced overhead is smaller. Besides, as the entropy of the video frames goes up, the introduced overhead also reduces, as original frames are already chaotic-like (contrary to null entropy frames, which

are totally regular). In an standard situation (around forty iterations in the chaotic mixture and medium entropy video streams), the introduced overhead is around 10%, similar to most efficient protocols in the state of the art.

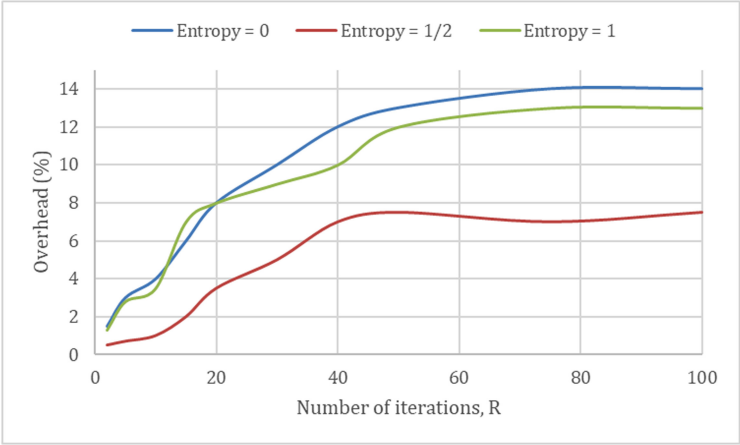

Fig. 6. Results of second experiment: Overhead

5 Conclusions and Future Works

This paper describes an authentication procedure based on digital watermarking. In our proposal, video infrastructures are organized as edge computing architectures, where enriched video streams are protected by watermarks and devices may delegate functionalities dynamically. This new watermarking technology is based on chaotic mixtures and secret keys provided by Physical Unclonable Functions.

In order to evaluate the performance of the proposed solution an experimental validation is also carried out. Results shows the proposed mechanisms is a valid technology for authentication in video applications.

Future works will consider more complex chaotic maps, as well as different discrete transforms and injection functions, in order to reduce the computational cost of the solution and improve the rate of successful authentications.

Acknowledgments. The research leading to these results has received funding by the Ministry of Science, Innovation and Universities through the COGNOS (PID2019-105484RB-I00) project.

References

1. Alcarria, R., Bordel, B., Manso, M.Á., Iturrioz, T., Pérez, M.: Analyzing UAV-based remote sensing and WSN support for data fusion. In: Rocha, Á., Guarda, T. (eds.) ICITS 2018. AISC, vol. 721, pp. 756–766. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73450-7_71
2. Atrey, P.K., Yan, W.Q., Kankanhalli, M.S.: A scalable signature scheme for video authentication. Multimed. Tools Appl. **34**(1), 107–135 (2007). https://doi.org/10.1007/s11042-006-0074-7
3. Bartolini, F., Tefas, A., Barni, M., Pitas, I.: Image authentication techniques for surveillance applications. Proc. IEEE **89**(10), 1403–1418 (2001). https://doi.org/10.1109/5.959338
4. Billinghurst, M., Clark, A., Lee, G.: A survey of augmented reality. Found. Trends® Hum. Comput. Interact. **8**(2–3), 73–272 (2015). https://doi.org/10.1561/1100000049
5. Bordel, B., Alcarria, R.: Physical unclonable functions based on silicon micro-ring resonators for secure signature delegation in wireless sensor networks. J. Internet Serv. Inf. Secur. (JISIS) **8**(3), 40–53 (2018)
6. Bordel, B., Alcarria, R., Ángel Manso, M., Jara, A.: Building enhanced environmental traceability solutions: from thing-to-thing communications to generalized cyber-physical systems. J. Internet Serv. Inf. Secur. (JISIS)(JISIS) **7**(3), 17–33 (2017)
7. Bordel, B., Alcarria, R., de Rivera, D.S., Martín, D., Robles, T.: Fast self-configuration in service-oriented smart environments for real-time applications. JAISE **10**(2), 143–167 (2018). https://doi.org/10.3233/AIS-180479
8. Chen, S., Leung, H.: Chaotic watermarking for video authentication in surveillance applications. IEEE Trans. Circuits Syst. Video Technol. **18**(5), 704–709 (2008). https://doi.org/10.1109/TCSVT.2008.918801
9. Chetty, G., Wagner, M.: Liveness verification in audio-video speaker authentication. In: Cassidy, S., Cox, F., Mannwell, R., Palethorpe, S. (eds.) Proceedings of the 10th Australian Conference on Speech, Science and Technology, pp. 358–363. Australian Speech Science and Technology Association (ASSTA) (2004)
10. Cross, D., Mobasseri, B.G.: Watermarking for self-authentication of compressed video. In: Proceedings of International Conference on Image Processing, vol. 2, pp. II-II, September 2002. https://doi.org/10.1109/ICIP.2002.1040100
11. Dittmann, J., Mukherjee, A., Steinebach, M.: Media-independent watermarking classification and the need for combining digital video and audio watermarking for media authentication. In: Proceedings International Conference on Information Technology: Coding and Computing (Cat. No.PR00540), pp. 62–67, March 2000. https://doi.org/10.1109/ITCC.2000.844184
12. Dittmann, J., Steinmetz, A., Steinmetz, R.: Content-based digital signature for motion pictures authentication and content-fragile watermarking. In: Proceedings IEEE International Conference on Multimedia Computing and Systems, vol. 2, pp. 209–213, June 1999. https://doi.org/10.1109/MMCS.1999.778274
13. Duc, B., Bigün, E.S., Bigün, J., Maître, G., Fischer, S.: Fusion of audio and video information for multi modal person authentication. Pattern Recogn. Lett. **18**(9), 835–843 (1997). https://doi.org/10.1016/S0167-8655(97)00071-8
14. Fadl, S.M., Han, Q., Li, Q.: Authentication of surveillance videos: detectingframe duplication based on residual frame. J. Forensic Sci. **63**(4), 1099–1109 (2018). https://doi.org/10.1111/1556-4029.13658

15. Grigoras, C.: Applications of ENF analysis in forensic authentication of digital audio and video recordings. J. Audio Eng. Soc. **57**(9), 643–661 (2009). http://www.aes.org/e-lib/browse.cfm?elib=14835
16. Gritti, C., Önen, M., Molva, R., Susilo, W., Plantard, T.: Device identification and personal data attestation in networks. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. **9**(4), 1–25 (2018). https://doi.org/10.22667/JOWUA.2018.12.31.001
17. Gusev, P.D., Borzunov, G.I.: The analysis of modern methods for video authentication. Procedia Comput. Sci. **123**, 161 – 164 (2018). https://doi.org/10.1016/j.procs.2018.01.026. 8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017 (Eighth Annual Meeting of the BICA Society), held August 1-6, 2017 in Moscow, Russia
18. Kunkelmann, T.: Applying encryption to video communication. In: Proceedings of the Multimedia and Security Workshop at ACM Multimedia (1998)
19. Liu, J., Ke, Y., Kao, Y., Tsai, S., Lin, Y.: A dual-stack authentication mechanism through SNMP. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. **10**(4), 31–45 (2019). https://doi.org/10.22667/JOWUA.2019.12.31.031
20. Lugiez, M., Ménard, M., El-Hamidi, A.: Dynamic color texture modeling and color video decomposition using bounded variation and oscillatory functions. In: Elmoataz, A., Lezoray, O., Nouboud, F., Mammass, D. (eds.) ICISP 2008. LNCS, vol. 5099, pp. 29–37. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-69905-7_4
21. Mareca, M.P., Bordel, B.: Improving the complexity of the Lorenz dynamics. In: Complexity 2017, pp. 1–16, January 2017. https://doi.org/10.1155/2017/3204073
22. Mobasseri, B.G., Sieffert, M.J., Simard, R.J.: Content authentication and tamper detection in digital video. In: Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101), vol. 1, pp. 458–461, September 2000. https://doi.org/10.1109/ICIP.2000.900994
23. Nimbalkar, A.B., Desai, C.G.: Digital signature schemes based on two hard problems. In: Detecting and Mitigating Robotic Cyber Security Risks, pp. 98–125 (2017)
24. Pérez-Jiménez, M., Sánchez, B., Migliorini, A., Alcarria, R.: Protecting private communications in cyber-physical systems through physical unclonable functions. Electronics **8**(4), 390 (2019). https://doi.org/10.3390/electronics8040390
25. Roy, S.D., Li, X., Shoshan, Y., Fish, A., Yadid-Pecht, O.: Hardware implementation of a digital watermarking system for video authentication. IEEE Trans. Circuits Syst. Video Technol. **23**(2), 289–301 (2013). https://doi.org/10.1109/TCSVT.2012.2203738
26. Sajjad, M., et al.: CNN-based anti-spoofing two-tier multi-factor authentication system. Pattern Recogn. Lett. (2018). https://doi.org/10.1016/j.patrec.2018.02.015
27. Schneider, M., Chang, S.-F.: A robust content based digital signature for image authentication. In: Proceedings of 3rd IEEE International Conference on Image Processing, vol. 3, pp. 227–230, September 1996. https://doi.org/10.1109/ICIP.1996.560425
28. Singh, R.D., Aggarwal, N.: Video content authentication techniques: a comprehensive survey. Multimed. Syst. **24**(2), 211–240 (2017). https://doi.org/10.1007/s00530-017-0538-9
29. Sun, Q., He, D., Tian, Q.: A secure and robust authentication scheme for video transcoding. IEEE Trans. Circuits Syst. Video Technol. **16**(10), 1232–1244 (2006). https://doi.org/10.1109/TCSVT.2006.882540

30. Vidhya, R., Brindha, M.: A novel dynamic key based chaotic image encryption. J. Internet Serv. Inf. Secur. **8**(1), 46–55 (2018). https://doi.org/10.22667/JISIS.2018.02.28.046
31. Xu, D., Wang, R., Wang, J.: A novel watermarking scheme for H.264/AVC video authentication. Image Commun. **26**(6), 267–279 (2011). https://doi.org/10.1016/j.image.2011.04.008
32. Yin, P., Yu, H.H.: A semi-fragile watermarking system for mpeg video authentication. In: 2002 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 4, pp. IV-3461–IV-3464, May 2002. https://doi.org/10.1109/ICASSP.2002.5745399