



Vojnotehnicki glasnik/Military Technical Courier
ISSN: 0042-8469
ISSN: 2217-4753
vojnotehnicki.glasnik@mod.gov.rs
University of Defence
Serbia

Identification of soldiers and weapons in military armory based on comparison image processing and RFID tag

Bogi#evi#, Dušan Lj.; Tot, Ivan A.; Prodanovi#, Radomir I.; Todorovi#, Bojan J.

Identification of soldiers and weapons in military armory based on comparison image processing and RFID tag

Vojnotehnicki glasnik/Military Technical Courier, vol. 69, no. 1, 2021

University of Defence, Serbia

Available in: <https://www.redalyc.org/articulo.oa?id=661771133008>

DOI: <https://doi.org/10.5937/vojtehg69-28114>

<http://www.vtg.mod.gov.rs/copyright-notice-and-self-archiving-policy.html>



This work is licensed under Creative Commons Attribution 4.0 International.

Identification of soldiers and weapons in military armory based on comparison image processing and RFID tag

Идентификация солдат и вооружения на складе оружия, основанная на сравнительной обработке изображений и RFID-меток


Идентификација војника и наоружања у магацину наоружања заснована на поређењу процесирања слика и RFID тагова

Dušan Lj. Bogićević
Serbian Armed Forces, Serbia
dusan.bogicevic@gmail.com

DOI: <https://doi.org/10.5937/vojtehg69-28114>
Redalyc: <https://www.redalyc.org/articulo.oa?id=661771133008>

 <https://orcid.org/0000-0002-4300-2490>

Ivan A. Tot
University of Defence in Belgrade, Serbia
ivan.tot@va.mod.gov.rs
 <https://orcid.org/0000-0002-5862-9042>

Radomir I. Prodanović
Serbian Armed Forces, Serbia
radomir.prodanovic@vs.rs
 <https://orcid.org/0000-0002-2067-2758>

Bojan J. Todorović
Serbian Armed Forces, Serbia
todorovicbojan@yahoo.com
 <https://orcid.org/0000-0002-7028-274X>

Received: 24 August 2020

Revised document received: 02 November 2020

Accepted: 04 November 2020

ABSTRACT:

Introduction/purpose: The process of issuing and retrieving weapons in the military should be fast enough and should provide immediate availability of accurate information on the status of weapons.

Methods: This paper deals with the problem of digitizing the recording of issuing and returning weapons through the use of modern Edge computing technology. The problem is presented through two approaches. The first approach is based on the application of machine learning algorithms for recognizing the serial number of a weapon based on the camera image, while the second approach concerns the application of RFID technology. User authentication is based on the application of biometrics.

Results: The results obtained from testing the architecture for identifying weapons using a camera indicate that such an architecture is not suitable for identifying weapons. A weapon identification solution using RFID technology overcomes the problems of the previously mentioned solution. However, RFID technology requires additional modifications regarding the implementation of tags on or into weapons so that readings can be made.

Conclusion: The implemented weapon identification solution based on RFID technology and a user identification solution with biometric authentication enables easy and reliable identification, speed of issuing and retrieval of weapons, network relieving, and real-time monitoring of the weapon status.

AUTHOR NOTES

ivan.tot@va.mod.gov.rs

KEYWORDS: image processing, fingerprint, RFID, artificial intelligence, Internet of Things, Raspberry Pi.

Р е з ю м е :

Введение/цель: Процедура выдачи и возврата оружия в армии должна проводиться быстро и обеспечивать немедленный доступ точной информации о состоянии оружия.

Методы: В данной статье рассматривается проблема о цифровке регистрации выдачи и возврата оружия с использованием современных компьютерных технологий Edge. В статье представлены два подхода к решению данной проблемы. Первый подход основан на применении алгоритмов машинного обучения для распознавания серийного номера оружия по изображению, сделанного камерой, а второй подход относится к применению технологии RFID. Идентификация пользователя проводится с помощью биометрической аутентификации.

Результаты: Результаты, полученные тестированием архитектуры идентификации вооружения с помощью камеры, показывают, что такая архитектура не подходит для идентификации оружия. Решение для идентификации оружия с использованием технологии RFID преодолевает проблемы вышеупомянутого решения. Однако для более успешного считывания информации технология RFID требует дополнительных модификаций, касающихся внедрения меток оружия.

Выводы: Внедренное решение идентификации оружия на основании технологии RFID и биометрическая аутентификация обеспечивают простую и надежную идентификацию, скорость выдачи и возврата оружия, разгрузку сети и наблюдение за состоянием оружия в реальном времени.

К л ю ч е в ы е с л о в а : обработка изображений, отпечаток пальца, RFID, искусственный интеллект, интернет вещей, Raspberry Pi, процессинг изображения, сканирование отпечатка пальца, RFID, метка интеллигенция, интернет ствари, Raspberry Pi.

ABSTRACT:

Увод/циљ: Процес издавања и враћања наоружања у војсци треба да буде довољно брз, као и да омогући доступност тачних информација о стању наоружања.

Метод: У овом раду разматра се проблем дигитализације записивања података о издавању и враћању наоружања, коришћењем савремене рачунарске технологије Едге. Проблем је разматран на два начина. Први се заснива на примени алгоритма машинског учења за препознавање серијског броја наоружања коришћењем слике израђене помоћу камере, док други начин разматра примену RFID технологије. Корисничка аутентификација заснива се на примени биометрије.

Резултати: Резултати добијени након тестирања архитектуре за идентификацију наоружања коришћењем камере показују да таква архитектура није одговарајућа. Решење за идентификацију наоружања коришћењем RFID технологије превазилази проблеме претходно наведеног решења. Међутим, RFID технологија захтева додатне модификације које се односе на имплементацију ознака на наоружању како би њихово читавање било успешно.

Закључак: Имплементирано решење за идентификацију наоружања засновано на RFID технологији, уз примену биометрије за аутентификацију корисника, омогућава једноставну и поуздану идентификацију, брзину при издавању и враћању наоружања, растерећење рачунарске мреже, као и надзор над статусом наоружања у реалном времену.

INTRODUCTION

The process of issuing and retrieving weapons in the military should be fast enough and should provide immediate availability of accurate information on the weapon status. Manual maintaining records of weapons issuing and returning is slow and error-prone. This approach is inappropriate for a military organization. Therefore, it is necessary to develop a system based on state-of-the-art technologies that will enable rapid and accurate record keeping of the weapon status, as well as information on when the weapon was taken, returned, and who used the weapon.

In (Lien, 2011), the author describes the implementation of active and passive RFID tags in the military to improve accountability and accuracy. The paper cites its price as one of the advantages of a system based on RFID tags. On the other hand, in (Nicholls, 2017), the author describes what would be the advantages and disadvantages of implanting RFID tags in military personnel. The authors in (Chattaraj et al, 2009) see the implementation of RFID tags in traffic control. In terms of authentication of military personnel, in addition to RFID tags that would be embedded in them, biometrics can also be applied. Biometrics can be used for authentication to improve various systems as presented in (Kour et al, 2016), who see the application of biometrics as the key to the future of cyber security.

It is necessary first to identify the weapon which has to be issued or returned. One way to do it is by using a camera as a sensor and the Optical Character Recognition (OCR) technique. Using the OCR, we can extract the text or the serial number of the weapon from the image. Algorithms that allow a text to be read from an image are machine learning algorithms and fall under the domain of Artificial Intelligence (AI). The authors in (Hanmandlu et al, 2017) used an image of a finger knuckle for the personnel authentication.

This paper explores the possibility of improving the process of keeping records of weapons issued and returned. The possibility of identifying weapons and identifying users is being explored. Weapon identification is considered by identifying the serial number by processing the image obtained from the camera as well as processing data from the RFID sensor in the process of weapon identification. User identification is considered through the application of one of the biometric techniques, such as fingerprint identification.

The authors developed an architecture for identifying weapons using RFID technology and identifying weapons users using fingerprint recognition. The architecture allows collection and processing of identification data in real time because processing is performed on the device itself, where the data is generated.

MATERIAL AND METHODS

The problem with weapons identification, in terms of research, can be classified as the Internet of Things (IoT). The IoT is a term that refers to connecting various devices to a network. These devices are present at the edge of the network, where real-time data is generated and processed. The amount of data generated at the edge of a network can be large. The architecture where data processing is done on Edge devices is called Edge computing (Reale, 2017). Edge computing provides: privacy, delay reduction, data filtering, and pre-processing.

Conversion of a text from paper to a digital text is known as Optical Character Recognition (OCR). This conversion method has been explored for decades (Prajapati et al, 2018). Artificial intelligence is used for image processing and text recognition, and OCR is one of the branches of artificial intelligence (Pawar et al, 2019). One of the AI techniques used for text recognition is the Artificial Neural Network (ANN) (Prajapati et al, 2018). There are a number of currently implemented OCR software programs. Common to all software programs currently developed is that they cannot read every text without making an error. In the case of a handwritten text, the Intelligent Character Recognition (ICR) technique is used (SimpleSoftware, 2020). One of the software solutions that can be used for OCR is the Tesseract engine (Pyimagesearch, 2018).

Radio Frequency Identification (RFID) belongs to a group of short-range wireless communications. This type of communication is based on the RFID reader and the RFID tag. The reader emits a radio signal, to which the tag, if within the range of the reader, responds by sending its code (tag). Depending on the tag power type, there are a passive reader (powered by the power it receives from the reader), a semi-passive reader (has a battery that powers the processor), and an active reader (has its own power). The frequency bands 125-134.2 kHz and 140-148.5 kHz belong to the LF-Low Frequency readers and their range is less than 0.5 meters. The range 6.775-6.795 MHz belongs to midrange readers. The high frequency group includes readers with a frequency higher than 13.553 MHz (HF-High Frequency) and their range can go up to one meter, and if the frequency range 858-930 MHz (UH-Ultra High Frequency) is used, it can go up to 10 meters. Using self-powered tags can increase the range of the reader in all operating ranges, and in the case of using the UHF range, the range can go up to 500 meters (Electronicsnotes, 2020), (SkyRFIDInc, 2020).

The Fingerprint is one of the biometric recognition techniques and it can be used for face, iris, voice, or palm recognition (Maltoni et al, 2009). Technologies which can be used to digitize fingerprints can be grouped in optical (Frustrated Total Internal Reflection), electrical (capacitive, thermal, electric field, and piezoelectric), and ultrasound (Maltoni et al, 2009). One of the problems with finger digitization is the

storage of a large number of prints. In order to optimize the memory space needed for storage, compression mechanisms have been created. The most famous is Wavelet Scalar Quantization (WSQ). This algorithm was developed by the FBI, the National Institute of Standards and Technology (NIST), and the Los Alamos National Laboratory (Thakkar, 2020). Biometric data are left on most of the objects people touch. This fact represents one of the biggest flaws, which is reflected in the generation of a false fingerprint (Nogueira et al, 2016).

An Edge computing architecture was proposed in this paper for research purposes. Edge devices were used to digitize the process of keeping records of weapons issuing and returning. These devices should be able to process image and data from RFID and biometric readers.

The Edge device used is the Raspberry Pi 3 (Processor: 64 bits, 4 cores, 1.2GHz; RAM 1 GB) which has 4 USB ports and 40 GPIO pins, Ethernet, Wi-Fi, Bluetooth. Due to the possibility of connecting a greater number of different devices and sensors, its small dimensions (85 x 49 mm), price, as well as satisfactory performances, this device was chosen. The Raspberry Pi Camera (5-megapixel OV5647 sensor) and Tesseract Engine for OCR and OpenCV software were used to test the serial number recognition on the image. The NFC-tag (Ntag213) and the RFID reader RC522 were used to test the possibility of applying RFID technology.

RESULTS

Two approaches have been used to address the problem of identification of weapons and keeping their records. The first approach to solving the problem of identifying a weapon is based on something possessed by the weapon, while the second approach is based on something attached to the weapon. In the first approach, a camera was used to read the existing serial number of the weapon, while in the second approach, RFID technology was used.

Analysis of proposed solutions

For the purpose of the research, two weapons identification architectures were created. The architectures are based on a Raspberry Pi computer, a monitor, and a data acquisition device (camera or RFID reader), as shown in Figure 1.

A weapon identification architecture that uses a camera to read a weapon's serial number is shown in Figure 1a. With this architecture, the user brings in a weapon facing the serial number towards the camera. After generating the image, the computer processes the image by trying to identify the serial number of the weapon.

Before testing the image processing from the camera, the architecture was tested by recognizing the text from the previously processed image. The aim was to determine whether the Raspberry Pi could extract a text from the image. During testing, we determined that the Raspberry Pi could read a text from an image for 2s to 8s depending on the image quality. However, the percentage of read characters of the serial number from the image ranged from 78% to 100%. The whole serial number recognition rate is 28% of all attempts (75 attempts, 21 serial numbers recognized).

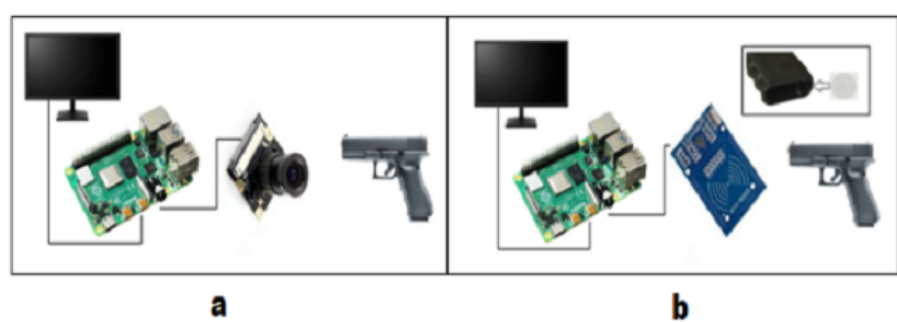


FIGURE 1
System architecture: (a) for image testing, (b) for RFID tag processing)

We then tested the reading of the serial number of the weapon from the image generated by the camera. Figure 2 shows the images of the weapon serial numbers.



FIGURE 2
Weapon serial numbers

The time required to recognize a serial number is greater than that of the image previously processed and ranged from 5s to 20s. The precision was much lower and ranged from 0 to 70% of the maximum read characters of the serial number. The reading results are shown in Table 1. Characteristically, the whole serial number of the weapon was not recognized in any of the 150 recognition attempts. One possible solution to solving image processing speed and serial number recognition quality would be to use a server that recognizes the image as described in (Saleous et al, 2016).

TABLE 1
Comparative overview of weapons serial number readings

Type of Weapon	Serial Number length	Number of letters	Image						RFID	
			Prepared			Not-prepared			Distance (mm)	
			No. of attempt	No. of read characters		No. of attempt	No. of read characters		start reading	in weapon
MIN	MAX	MIN		MAX						
Pistols	6	3	5	5	5	10	2	4	25	15
	6	3	5	5	5	10	1	3	25	15
	7	3	5	4	6	10	1	3	26	12
	7	4	5	5	7	10	1	2	26	11
	7	1	5	6	6	10	2	4	24	15
	7	1	5	4	4	10	0	3	25	12
	7	1	5	4	4	10	2	4	25	12
Rifle	5	0	5	4	4	10	1	2	30	3
	5	0	5	5	5	10	2	3	30	3
	5	0	5	5	5	10	3	4	30	3
	6	0	5	3	3	10	0	2	27	5
	8	0	5	7	8	10	4	6	30	4
	8	0	5	8	8	10	5	6	30	4
	9	0	5	7	7	10	5	6	30	3
	9	0	5	6	7	10	1	5	30	3

The second approach to problem solving was to use RFID readers. When testing the RFID weapons identification architecture, an NFC-tag test environment (Ntag213) was developed and the RFID reader RC522 was used. The architecture of the test system for processing RFID tags is shown in Figure 1b. A flexible NFC tag with a diameter of 25mm is placed inside the weapon. Figure 1b, as a separate section, shows the handrail and the exact location of the NFC tag. During testing, the response was found to depend on the tag distance from the RFID reader as well as where the tag was placed. Table 1 shows that the maximum distance from which RFID tag readings start is 25 to 30 mm, depending on the position of the tag in the weapon.

Based on the performed testing, Table 2 shows a comparative overview of the two architectures. Based on the analysis, the architecture for weapons identification using RFID technology was selected.

TABLE 2
Comparative overview of the advantages and disadvantages of the tested architectures

Weapon identification	Advantages	Disadvantages
Using the camera	No weapon modifications. It can be used to identify the weapon type. The ability to use the camera to authenticate the person.	Low serial number recognition accuracy. It requires a computer with better performances. It requires more time to identify the weapon.
Using RFID	Reliability in reading weapon identifiers. Processing speed of read data.	Providing tags and labeling weapons. Non-uniform tag placement on different types of weapons.

In terms of person authentication, finger, iris, and facebiometrics was considered as well as RFID tag-based authentication. It was concluded that in order to achieve adequate reliability and speed of authentication based on iris and face biometrics, additional conditions were required. These conditions apply to the lighting and hardware on which the authentication would be performed (Maltoni et al, 2009). We opted for solutions that did not require special environmental conditions and were not hardware-demanding. The solutions that could be implemented are the fingerprint and the RFID tag. As RFID tags are not embedded in persons, it is suggested that person identification should be based on fingerprint authentication.

Proposed architecture for identifying weapons and users

Based on the results of the testing and comparative analysis of weapons identification architectures, a combined architecture for weapons and user identification is proposed. This architecture uses RFID technology for weapon identification while user identification is based on the fingerprint method. In addition to visual notification of the identification of a user and weapon on the monitor, voice notification is also proposed for faster release or return dynamics. The architecture of the proposed solution is shown in Figure 3.

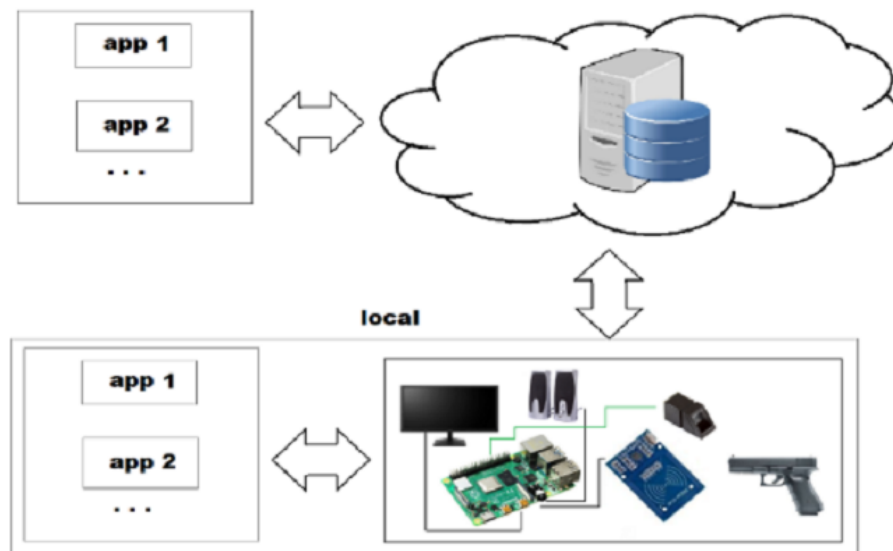


FIGURE 3

Proposed weapon and user identification architecture

Weapon and user identification is done as follows:

- The user logs on to the system with a fingerprint. When a person logs in, he or she has 30s to read their weapon, otherwise they need to log back in,
- When a person is logged in, the weapon tag is read and the status of the weapon changes (issued or returned by the user),
- After each change, the system notifies the status of the weapon or a new person.

The system allows the verification of weapon data (weapon type, model, serial number) based on RFID tags even if the user is not logged in. The weapon and user identification algorithm is shown in Figure 4.

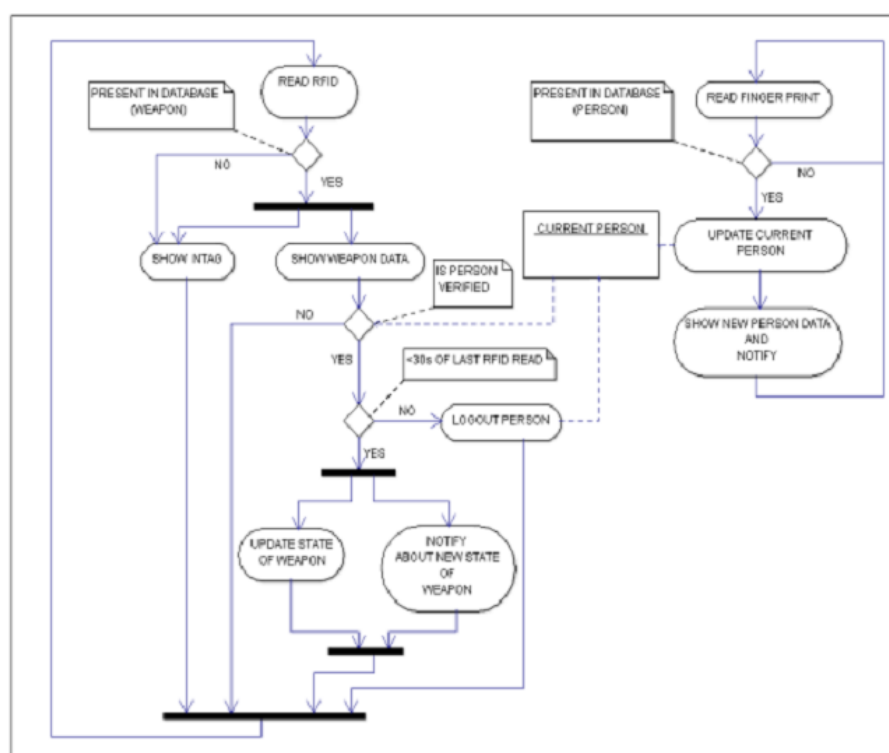


FIGURE 4
Weapon and user identification algorithm

The architecture consists of the Raspberry Pi computer, which is an integrator of the whole system, to which status notification devices (monitor, speakers) and data acquisition devices (RFID reader and fingerprint reader) are connected. The architecture also includes a database, which allows records to be kept. In order to enable faster logging in and logging out, data processing and database are hosted on the Raspberry Pi. In this way, most of the data processing is done at the edge of the network. This kind of approach in the architecture relieves network resources.

EDGE architecture takes data processing near the source. In this work, we use the Raspberry Pi as a local server. The layers which are above the local layer use Containerization and Orchestration to receive data from multiple different sources. In the upper layers, it is possible to apply some of the techniques such as AI and Machine learning. These techniques can lead to better analyses and recommendations for some organizational changes and also changes regarding weapons which are in use in a unit, which in return can provide better efficiency of the unit.

The Raspberry PI enables applications on all layers of architecture to exchange information. This architecture reduces latency and provides reliability. In terms of security, it decreases potential weaknesses in communication with the main server is reduced. In military systems, it is important to reduce communication because military band widths are often limited.

Implementation of the proposed solution

The architecture was practically designed by deploying the Raspberry Pi computer inside each weapon warehouse with data collection and notification devices. The Raspberry Pi is connected to the network. An online service has been implemented enabling the collection of data on the current status, processing and exchange of data, presentation of data and remote administration of the system.

Each weapon is intended to have an RFID tag as an identifier. The implemented architecture enables the exchange of data with a central database. In this way, the network is relieved and information processing is provided as close as possible to the source, which is the tendency in similar systems that belong to the concept of the Internet of Things.

All the needed hardware introduced as System architecture and presented in Figure 3 is housed in a special shielded box. The process of registering an individual is shown in Figure 5a, and begins with the person pointing his or her finger at the fingerprint reader. The application identifies the person, and if the identification is successful, the person's information is displayed on the monitor or spoken through the speakers. We used the text-to-speech library FreeTTS (Freetts.Sourceforge, 2017) to ensure that the person's name was read.

The process of identifying the weapon is shown in Figure 5b and is carried out by moving the weapon to the side where the RFID tag is attached to the RFID reader. After reading the RFID tag, the application checks for the existence of such a weapon and records it as being issued or returned. Figure 5c shows the place selected for the RFID tag placement.



FIGURE 5

Implemented solution: (a) registering, (b) weapon identification, (c) tag placement

DISCUSSION

The results obtained from testing the architecture for identifying weapons using a camera indicate that such an architecture is not suitable for identifying weapons. The test results show that there was no successful reading of all characters of the serial number regardless of the number of characters and the number of attempts. The reasons for the unsuccessful reading are due to the following problems: determining the most suitable distance between the weapon and the camera, poor visibility of the serial number due to the color of the print, wear, or concealment of accessories that can be mounted on the weapon. Another issue which makes this architecture a not so good solution is the problem of image processing speed which recognizes a serial number from an image. Testing has shown that the processing speed is low, which can create a problem of crowding when taking or returning a weapon from or to a weapon warehouse. One solution that can fix the results of processing the image obtained from a camera is to paste stickers with a serial number or an OCR code onto the weapon on its outside.

A weapon identification solution using RFID technology overcomes the problems of the previously mentioned solution. RFID technology requires additional modifications regarding the implementation of tags on or into weapons so that readings can be made. The position of the tag in the weapon affects the

distance required to read. However, in the event that the weapon is propped up against the reader, a secure reading is made, thereby achieving system reliability.

The weapons used for testing are newer generation weapons. They have places where plastic-like materials can be used to include the stock (where wood was commonly used) or grips. Such places are suitable for tagging.

The Fingerprint is one of the most commonly used authentication methods. In military processes where reliability and speed are required, the fingerprint can meet the requirements. There are fingerprint sensors on the market that do not require high-performance computers. On the other hand, the amount of memory required to store a fingerprint is small, so that fingerprint readers can store the prints in their memory.

CONCLUSION

The implemented weapon identification solution based on RFID technology and a user identification solution with biometric authentication enables easy and reliable identification, speed of issuing and retrieval of weapons, network relieving, and real-time monitoring of weapon status. In this way, a solution can be implemented to improve the process of recording and monitoring weapons in weapon warehouses.

Tracking the development of science in fields such as the IoT, AI, and Edge computing is certainly of interest in military applications. This paper shows the disadvantages of using AI in weapons image processing. The main drawback is a low degree of reliability. RFID systems are reliable systems for keeping track of things. By combining more techniques and technologies such as RFID, IoT, and AI, it is possible to increase the performance of military systems. Digitization of basic military processes results in better use of time as a resource.

ACKNOWLEDGMENTS

The authors would like to thank the Military Academy, University of Defence in Belgrade (project name: Access control management of protected resources in the Ministry of Defence and Serbian Armed Forces computer networks based on multimodal user identification, project code: VA-TT/3/18-20).

REFERENCES

- Chattaraj, A., Bansal, S. & Chandra, A. 2009. An intelligent traffic control system using RFID. *IEEE Potentials*, 28(3), pp.40-43. Available at: <https://doi.org/10.1109/MPOT.2009.932094>.
- Electronicsnotes. 2020. *RFID Frequency Bands & Spectrum* [online]. Available at: <https://www.electronics-notes.com/articles/connectivity/rfid-radio-frequency-identification/frequency-bands-spectrum.php/> [Accessed: 20 August 2020].
- Freetts.Sourceforge. 2017. *FreeTTS 1.2.3 - A speech synthesizer written entirely in the Java™ programming language* [online]. Available at: <https://freetts.sourceforge.io/> [Accessed: 20 January 2020].
- Hanmandlu, N., Mittal, N. & Vijay, R. 2017. A robust Finger Knuckle Print Authentication using topothesy and Fractal dimension. *Defence Science Journal*, 67(1), pp.66-73. Available at: <https://doi.org/10.14429/dsj.1.9003>.
- Kour, J., Hanmandlu, M. & Ansari, A.Q. 2016. Biometrics in cyber Security. *Defence Science Journal*, 66(6), pp.600-604. Available at: <https://doi.org/10.14429/dsj.66.10800>.
- Lien, T. 2011. *Automatic identification technology tracking weapons and ammunition for the Norwegian Armed Forces*. MA thesis. Monterey, California: Naval postgraduate school [online]. Available at: <https://calhoun.nps.edu/handle/10945/5715> [Accessed: 20 August 2020].
- Maltoni, D., Maio, D., Jain, A.K. & Prabhakar, S. 2009. *Handbook of Fingerprint Recognition*. Springer Nature Switzerland AG. Available at: <https://doi.org/10.1007/978-1-84882-254-2>. ISBN: 978-1-84882-254-2.

- Nicholls, R. 2017. Implanting Military RFID: Rights and Wrongs. *IEEE Technology and Society Magazine*, 36(1), pp.48-51. Available at: <https://doi.org/10.1109/MTS.2017.2654288>.
- Nogueira, R.F., de Alencar Lotufo, R. & Campos Machado, R. 2016. Fingerprint Liveness Detection using Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security*, 11(6), pp.1206-1213. Available at: <https://doi.org/10.1109/TIFS.2016.2520880>.
- Pawar, N., Shaikh, Z., Shinde, P. & Warke, J.P. 2019. Image to Text Conversion Using Tesseract. *International Research Journal of Engineering and Technology (IRJET)*, 6(2), pp.516-519 [online]. Available at: <https://www.irjet.net/archives/V6/i2/IRJET-V6I299.pdf> [Accessed: 20 August 2020].
- Prajapati, S., Joshi, S., Maharjan, A. & Balami, B. 2018. Evaluating Performance of Nepali Script OCR using Tesseract and Artificial Neural Network. In: *IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, Kathmandu, Nepal, pp.104-107, October 25-27. Available at: <https://doi.org/10.1109/CCCS.2018.8586808>.
- Pyimagesearch. 2018. *OpenCV OCR and text recognition with Tesseract* [online]. Available at: <https://www.pyimage search.com/2018/09/17/opencv-ocr-and-text-recognition-with-tesseract/> [Accessed: 20 August 2020].
- Reale, A. 2017. *A guide to Edge IoT analytics* [online]. Available at: <https://www.ibm.com/blogs/internet-of-things/Edge-iot-analytics/> [Accessed: 20 August 2020].
- Saleous, H., Shaikh, A., Gupta, R. & Sagahyroon, A. 2016. Read2Me: A cloud-based reading aid for the visually impaired. In: *International Conference on Industrial Informatics and Computer Systems (CIICS)*, Sharjah, UAE, pp.1-6, March 13-15. Available at: <https://doi.org/10.1109/ICCSII.2016.7462446>.
- SimpleSoftware. 2020. *OCR Guide* [online]. Available at: <https://www.simpleocr.com/ocr-guide/> [Accessed: 20 August 2020].
- SkyRFID Inc. 2020. *RFID Tag Maximum Read Distance* [online]. Available at: http://skyrfid.com/RFID_Tag_Read_Ranges.php [Accessed: 20 January 2020].
- Thakkar, D. 2020. *Fingerprint Image Compression: Know Why It Matters* [online]. Available at: <https://www.bayometric.com/fingerprint-image-compression/> [Accessed: 20 August 2020].

FUNDING

Funding source: Military Academy, University of Defence in Belgrade
 Contract number: Project name: Access control management of protected resources in the Ministry of Defence and Serbian Armed Forces computer networks based on multimodal user identification, project code: VA-TT/3/18-20
 Award recipient: Dušan Lj. Bogićević, Ivan A. Tot, Radomir I. Prodanović, Bojan J. Todorović

ADDITIONAL INFORMATION

FIELD: Computer sciences, IT

ARTICLE TYPE: Professional paper

ALTERNATIVE LINK

<https://scindeks.ceon.rs/article.aspx?artid=0042-84692101179B> (html)
<https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2021/0042-84692101179B.pdf> (pdf)
<https://elibrary.ru/item.asp?id=44584153> (pdf)
<http://www.vtg.mod.gov.rs/archive/2021/military-technical-courier-1-2021.pdf> (pdf)