Primjena kriptografije i biometrije u automobilskoj industriji

The use of cryptography and biometrics in the automotive industry

Edin Ćatović, Saša Adamović, Univerzitet Sinergija, Bijeljina

***Sažetak*— U radu težište je na opisu primjene kriptografije i biometrije u automobilskoj industriji od samog početka pa do danas. Osim toga bitno je bilo istaknuti kakve nam sve prednosti donosi njena primjena, a koje nedostatke. To se prije svega odnosi na primjenjena kriptografska rješenja, kao i opis hardwera koji je djelimično ili u cjelosti učestvovao u implementaciji istih. U tu svrhu su detaljno opisani, sve vrste automobilskih ključeva, kao i primjena RFID sistema u automobilima. Nakon detaljno obradjene problematike, cilj je bio ponuditi vlastito rješenje, te isto i implementirati. Kao razvojno okruženje korišten je Arduino IDE (Arduino Uno R3 board), uz podršku namjenskog hardware-a. Ponuđeno rješenje, dio je oblasti biometrije, preciznije paljenje automobila nakon skeniranja otiska prsta (Adafruit biometric fingerprint sensor).**

***Ključne riječi:* kriptografija; automobilska industrija; RFID; biometrija; Arduino**

Abstract – The paper focuses on the description of the application of cryptography and biometrics in the automotive industry from the very beginning until today. Furthermore it was important to point out what adventages brings its application, and which disadvantages. This primarily refers to the applied cryptographic solutions, as well as a description of hardware that is partially or fully involved in the implementation thereof. To this purpose are described in detail all kinds of car keys, as well as the application of RFID systems in cars. After thoroughly deals with the problems, the goal was to offer my own solution, and implement it. As a development environment is used Arduino IDE (Arduino Uno R3 board), with the support of dedicated hardware. The solution that is offered is part of the field of biometrics,more precisely ignition car after scanning a fingerprint (Adafruit biometric fingerprint sensor).

***Keywords* – cryptography; automotive industry; RFID; biometrics; Arduino**

I. UVOD

Svjedoci smo svakodnevnih naslova, u elektronskim, a i štampanim medijima, tipa „Automafija ne poznaje granice“, „Automafija i ove godine korak ispred policije“, „Automafija hara Balkanom“ i sl. Sve to ukazuje da je jedan od glavnih problema u regionu, a i Evropi, kako zaustaviti, ili bar smanjiti krađu vozila na tim prostorima.

Naime, dnevno se u BiH ukradu tri vozila, a pronalaze ih u Crnoj Gori, Albaniji, Rusiji, Srbiji i na Kosovu. Krađe automobila u Bosni i Hercegovini ponovo postaju sve ozbiljniji problem, a policijske agencije ukazuju na gotovo dramatičan porast broja ukradenih vozila. Posljedica je to djelovanja organiziranih i opasnih grupa kriminalaca, opremljenih visokosofisticiranom opremom, odnosno automafije.

Kriptografija u autoindustriji, veže se za kraj 80-ih i početak 90-ih godina, sa pojavom pristupa vozilu bez ključa (eng. Remote Keyless Entry, RKE) i pokretanju vozila bez ključa (eng. Keyless Go). Nakon toga dolaze elektronski imobilajzeri. U izoliranom sistemu, kakav je današnji automobil, imamo dosta kriptografskih rješenja. Međutim, o njima se jako malo govori. Govori se zapravo tek onda, kada neko od rješenja poklekne pred napadima zlonamjernih ljudi. Kao primjer ću navesti, 40 bitnu enkripciju, na transponderima firme Texas Instruments, koja je vrlo brzo probijena. Osim ovoga, imamo i Hitag2 enkripciju, vlasništvo NXP-a, koja je takođe probijena. RKE sistem KeeLoq, koji se koristio za otvaranje garažnih vrata, ali i na nekim automobilima, postao je nepopularn, nakon što su otkriveni propusti, uslijed par napada.

Pored svega, poslednjih godina se puno radilo na razvijanju jakih kriptografskih rjesenja za autentifikaciju. Na primjer, 2014 godine, firma Atmel, predstavila je novi „single chip“ AES-128 imobilajzer i „keyless entry“ AVR mikrokontroler. Čak se sada raspravlja i o asimetričnim solucijama, a kao primjer navešću ECC Remote Control Entry, od Fraunhofer SIT, razvijen uz pomoć Siemensa.

U ovom radu razvijeno je sopstevno rješenje za zaštitu auomobila bazirano na biometrijskim podacima – otisak prsta. Iskorišćena je hardverska osnova Arduino IDE, na kome je obezbeđena implementacija softvera za biometrijski servis autentifikacije.

II. TEORIJSKE OSNOVE

U poglavlju diskutovaćemo o softverskom i hardverskom djelu implemenatcije. Za potrebe eksperimentalnog rada korišćen je Adafruit biometrijski senzor otiska prsta, napisana je funkcija za uzimanje, čuvanje i poređenje otiska prsta. Takođe, Arduino Uno R3 ploča pruža mogućnost pohranjivanja do 160 različitih ID-ova, dakle 160 različitih otisaka prsta. Kao finalni produkt, zamišljena je

DOI: 10.7251/ZRSNG1501068C

implementacija na automobilu, tačnije startanje automobila otiskom prsta.

A. *Biometrija otiska prsta*

Biometrija, sama po sebi, uključuje upotrebu specijalnih uređaja, koji nam služe za praćenje određenih fizičkih, ili karakteristika ponašanja. Osim toga, neophodni su nam programi, koji će izvršiti analizu i upoređivanje dobijenih rezultata. Pri radu se koristi kombinacija uzorkovanja sa umjetnom inteligencijom. Uzorci se digitalizuju, i nakon toga upoređuju.

Prvi koji je uvidio mogućnost primjene otiska prsta za identifikaciju osobe bio je Henry Faulds, naučnik iz Škotske (1880 g.). Francis Galton, engleski naučnik, 1888 godine otkrio je značaj individualnosti i postojanosti otiska prsta. On takođe prvi put pominje pojam minucije (varijacije i različitosti papilarnih linija).

U procesu automatskog prepoznavanja otiska prsta postoji šest (standardizovanih) koraka, i to : akvizicija odnosno snimanje otiska prsta, zatim segmentacija slike, rekonstrukcija slike, ekstrakcija karakteristika, poređenje minucija (traženje para), i klasifikacija (smještanje u jednu od 7 grupa-petlja, duplja petlja i sl.)

Za akviziciju najpogodniji su skeneri koji optički (optičkom metodom) skidaju otisak prsta, tako se dobija bolja kvaliteta (najčešće 512 dpi). Segmentacija se odnosi na dvajanje slike, dobijene skenerom, od pozadine. Rekonstrukcija podrazumijeva povećanje kontrasta između grebena i dolina, te ponovo povezivanje grebena koji imaju prekid. Što se tiče extrakcije, imamo onu koja se zasniva na binarizaciji, i drugu koja se naziva neposredna skala sivog.

B. *Korišćeni hardver - Arduino*

Arduino predstavlja fizičko-računarsku platformu otvorenog koda. Arduino hardver je jednostavan (otvorenog tipa), i sastoji se od arduino ploče, sa Atmel AVR procesorom i pratećim ulazno-izlaznim komponentama. Arduino softver se sastoji od standardnog kompajlera i bootloader koji se nalazi na samoj ploči. Razvojno okruženje je aplikacija napisana u Java programskom jeziku.

Arduino integrisano razvojno okruženje dolazi sa C/C++ bibliotekom zvanom "Wiring" koja čini uobičajene ulazno-izlazne operacije veoma jednostavnim. Arduino programi se pišu u C/C++ programskom jeziku, mada korisnici moraju da definišu samo dve funkcije kako bi napravili izvršni program. Te funkcije su:

- setup() - funkcija koja se izvršava jednom na početku i služi za početna podešavanja
- loop() - funkcija koja se izvršava u petlji svo vrijeme dok se ne isključi ploča

Za hardversku implementaciju korišćen je Arduino Uno R3 ploču, Ardafruit biometrijski senzor otiska prsta, par dioda, testnu ploču, dupont kablove.

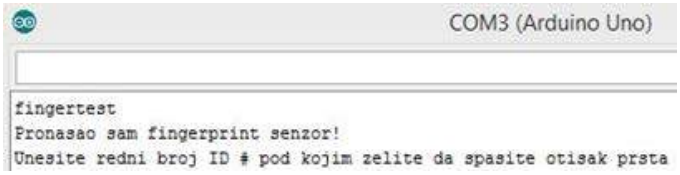
III. EKSPERIMENTALNI DEO

U ovom poglavlju predstavićemo naše predloženo rješenje. Pre nenog što pređemo na eksperimentalni deo rada, pojasnićemo okruženje u kojem je rađeno, te ukratko opisati isto. Nakon toga slijedi i prikaz koda, odnosno softverskog dijela i analiza dobijenih rezultata. Takođe, navešćemo primenu predloženog rješenja.

Kao softversko okruženje odabran je Arduino. Arduino predstavlja fizičko-računarsku platformu otvorenog koda. Arduino hardver je jednostavan (otvorenog tipa), i sastoji se od arduino ploče, sa Atmel AVR procesorom i pratećim ulazno-izlaznim komponentama.

Slika 1. Funkcija kojom se uzima i pohranjuje otisak prsta

Na slici 1. prikazana je funkcija očitavanja otiska prsta, obrada biometrijskih podtaka i pohranjivanje biometrijskog templejta u bazu podataka.



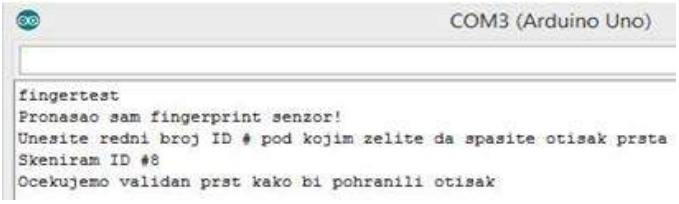
Slika 2. Arduino serial monitor

Vidimo da je komunikacija uspješna (slika 2), na COM3 portu. Nakon uspješno upisane funkcije na Arduino Uno R3 ploču, pokrećemo serial monitor, i slijedimo upute. Vidimo da je program uspješno prepoznao senzor otiska prsta, nakon odrađenog testa, i sve je spremno da unesemo ID, pod kojim želimo da pohranimo otisak. Jednostavno unesemo broj pod kojim želimo da se nalazi naš otisak (npr. broj 8), i pritisnemo tipku enter.

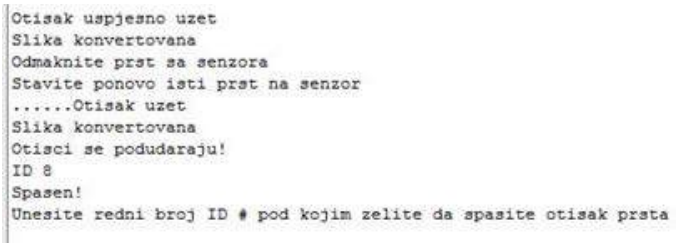
Slika 3. Unošenje ID-a pod kojim želimo da spasimo otisak

DOI: 10.7251/ZRSNG1501068C

Nakon što smo unijeli željeni broj prikazano na slici 3, na serial monitoru ispisuje nam se poruka, da se očekuje da pozicioniramo željeni prst na senzor, kako bi se uspješno uzeo otisak, kao što se može vidjeti na slijedećoj slici

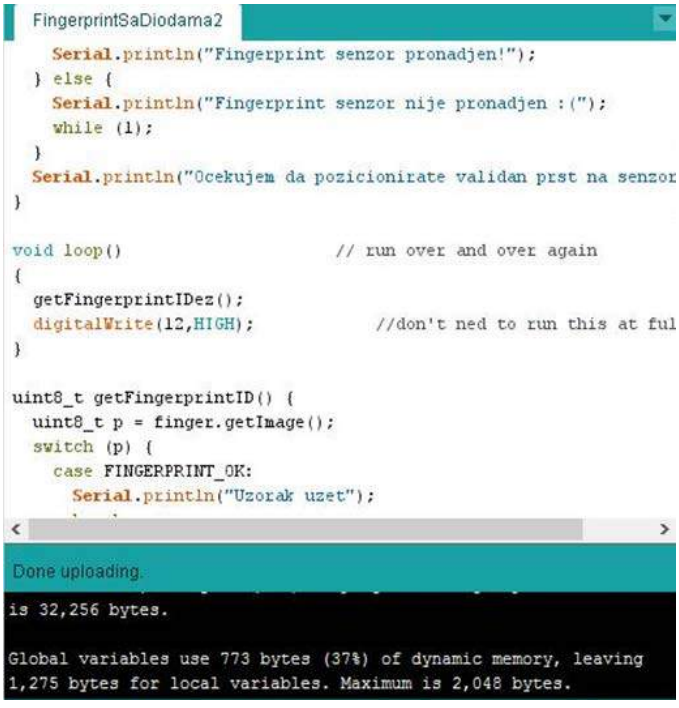


Slika 4. Senzor je spreman, očekuje pozicioniranje prsta

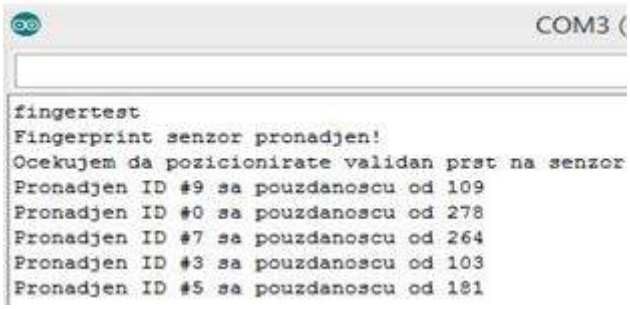


Slika 5. ID uspješno pohranjen

Nakon učitavanja funkcije na Arduino Uno R3 ploču, sistem je spreman za autentifikaciju, prikazano na slici 6. Sada možemo testirati one ID-eve koje smo unijeli, i vidjeti sa kojom pouzdanošću će ih senzor prepoznati. Ukoliko se uzeti otisak ne podudara ni sa jednim otiskom koji se nalazi u memoriji kontrolera (bazi otisaka), korisniku ce biti ispisano da takav otisak nije pronađen, te da pokuša ponovo. Kod sistema koji je spojen u automobilu, senzor otiska prsta ce na „kontakt“ raditi 15 sekundi, ocekujuci da skenira prst. Ukoliko se prst ne pozicionira na senzor u navedenom periodu, senzor ce ici u „sleep“ mode, a sve to zbog stednje energije.



Slika 6. Funcija za autentifikaciju

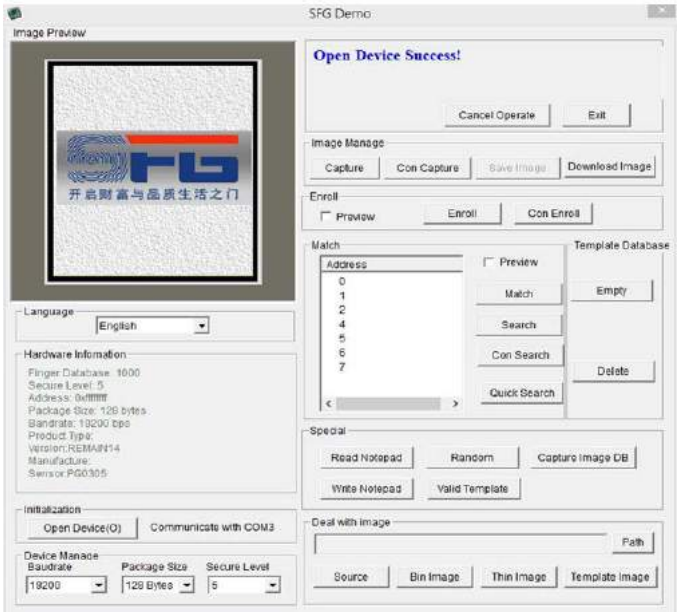


Slika 7. Uvid u ID-eve, i nivo preciznosti identifikacije

U scenariju koji je osmišljen, prilikom pronalaska ID-a (slika 7), koji se nalazi pohranjen na ploči, palila bi se zelena dioda, što označava da je autentifikacija uspješna. Ukoliko ID ne odgovara onima koji su pohranjeni na ploči, crvena dioda konstatno gori, što znači da ID ne odgovara, i isti nema pristup sistemu (automobilu, objektu i sl.).

Osim u ovakvim sistemima, Ardafruit biometrijski senzor otiska prsta, može se koristit za direktno uzimanje otiska prsta, uz sliku otiska. Za to nam je potreban dekstop računar ili laptop, Arduino Uno R3 ploča, i senzor.

Na Arduino Uno R3 ploču potrebno je učitati posebnu funkciju, kako bi ploča bila u ulozi mosta-a između senzora, i računara/laptopa.

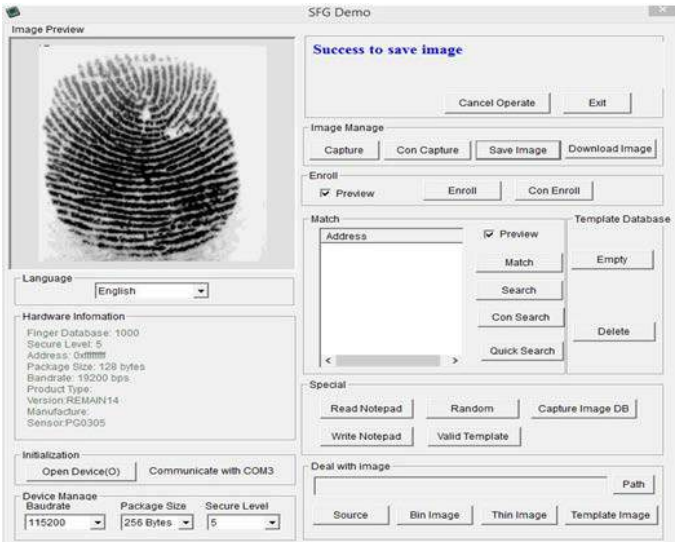


Slika 8. SFGV2 interface

U ovom softveru na slici 8. možemo pregedati već unijete korisnike (ID-eve), te unijeti nove, i eventualno pohraniti sliku željenog otiska.

Dakle sve što preostaje da uradimo, je da pozicioniramo željeni prst, i sačekamo pohranjivanje slike. Nakon uspješne pohrane, na malom displeju, moći ćemo vidjeti i sliku prethodno uzetog otiska.

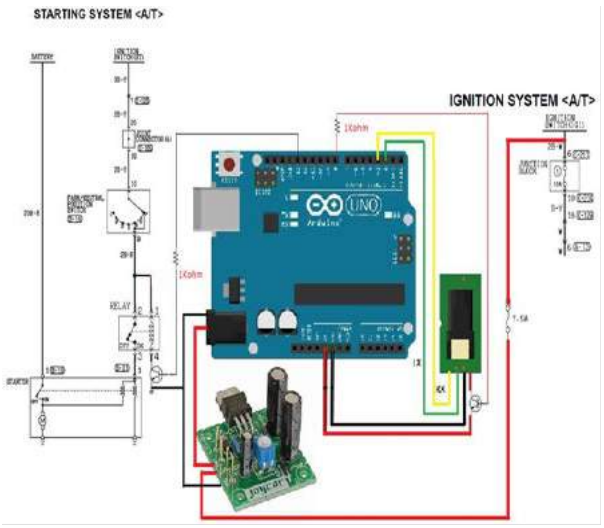
DOI: 10.7251/ZRSNG1501068C



Slika 9. Prikaz uzetog otiska ID1

Nakon kompletiranih svih prethodnih koraka, imamo gotove uzorke otisaka prsta vidljive na slici 9.

Kako bi sve do sada pomenuto primjenili na automobilu trebat ce nam i odgovarajuća šema spajanja koja je data na slici 10.



Slika 10. Šema potrebna za spajanje sistema na automobil

Osim do sada navedenih dijelova (Arduino Uno R3 ploča, senzor, kablovi), uz prethodno pohranjene ID-eve, bit će nam potreban relej izvor napajanja u automobilu (12 volti). Treba istaknuti da se shema spajanja, razlikuje od automobila do automobila, i da je prije instalacije potrebno prethohno poznavanje rasporeda i načina spajanja elektronskih uređaja u datom automobilu.

IV. ZAKLJUČAK

U radu je razvijeno rješenje bazirano na biometriji otiska prsta. Slična rješenja su u ponudi u nekim zemljama (Sjedinjene Američke Države) po veoma visokoj cijeni (cca. 700 USD). Primarna primjena zamišljena je u automobilima, kao sredstvo za autentifikaciju. Međutim postoji mogućnost veoma široke primjene i u drugim sferama (zastita objekata, kuća, garaža i sl.).

Kada gledamo u prošlost, vidimo da su kriptografska rješenja, korištena za zaštitu na automobilima, „padala“ prije ili kasnije. Naročito su bili kritični „propriatery“ sistemi, čije je kompromitovanje vješto skrivano. Rješenja bazirana na kriptografskim algoritmima, u kombinaciji sa remote keyless sistemima, uvijek su bila ograničena hardverom. Ukoliko se primjeni malo zahtjevnijie rješenje, odma bi se postavljalo pitanje da li će hardver biti usko grlo, u smislu sporog pretraživanja ili sporog odgovora. Ne tako rijetko, i napajanje je znalo biti ograničavajući faktor.

Zbog toga je i odabrana biometrija otiska prsta, kao rješenje. Vjerovatnoća da se na neki način kompromituje je veoma niska, gotovo nikakva. Uz pomoć još par mudrih poteza (uklanjanje brave sa vozačevih vrata, promjenu OBD konektora, bilo kakav tip mehaničke brave na letvi volana) mislim da će Vaš automobil biti krupan zalogaj i za napadače koji su u veoma sofisticirani u ovoj oblasti.

Ono što je u planu u skorijoj budućnosti, jeste pronalazak rješenja za zaštitu (softversku i hardversku) Arduino Uno R3 ploče, od nezakonitog pristupa, te manipulacije podacima na istoj. Kreiranje šema instalacije, za više vozila, naravno onih koja su zastupljenija na našem tržištu, i tržištu regiona.

LITERATURA

[1] Bogdanov, A. „Cryptanalysis of the KeeLoq block cipher“, 2010
[2] CARNet. „Biometrija“, 2010..
[3] CARNet CERT, L. (2007). RFID identifikacija .
[4] CIS. (2012). Sigurnost automobila .
[5] Kagin, R. „Keyless Entry“, 2007.
[6] MarkoWolf, A. W. „State of the Art: Embedding Security in Vehicles“, 2007.
[7] Qinghan Xiao, T. G. „RFID Technology, Security Vulnerabilities, and Countermeasures“ 2008.
[8] Roel Verdult, F. D. „Gone in 360 Seconds: Hijacking with Hitag2“, 2009.
[9] Schütze, D. T. „Automotive Security: Cryptography for Car2X Communication“, 2011.
[10] Soja, R. „Automotive Security:From Standards to Implementation“, 2014.
[11] Šimko, A. „Security of car keys“, 2014.

DOI: 10.7251/ZRSNG1501068C