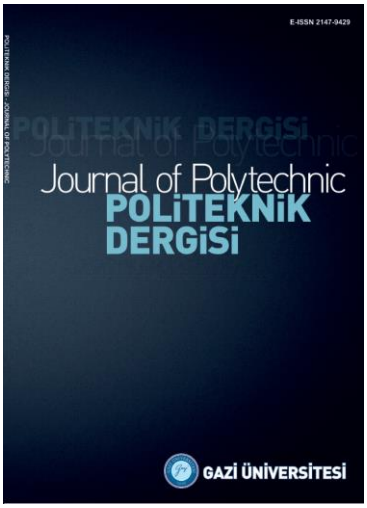


POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

A study on remote detection of Turkey digital identity card hologram element

Türkiye dijital kimlik kartı hologram öğesinin uzaktan tespitine yönelik bir çalışma

***Yazar(lar) (Author(s))**: Ender ŞAHİNASLAN[1], Abdullah KÖKSAL[2], Önder ŞAHİNASLAN[3]*

ORCID[1]: 0000-0001-8519-7612

ORCID[2]: 0000-0002-9872-6517

ORCID[3]: 0000-0003-2695-5078

To cite to this article: Şahinaslan E., Köksal A. ve Şahinaslan Ö., "A study on remote detection of Turkey digital identity card hologram element", ***Journal of Politechnic***, 27(2): 615-628, (2024).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Şahinaslan E., Köksal A. ve Şahinaslan Ö., "A study on remote detection of Turkey digital identity card hologram element", ***Politeknik Dergisi***, 27(2): 615-628, (2024).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.1167225**

A Study on Remote Detection of Turkey Digital Identity Card Hologram Element

Highlights

- *Technological developments and the pandemic have increased the demand for services offered remotely.*
- *Remote services have to be as secure, fast and compliant with the law as face-to-face services. However, remote control of qualified documents is quite difficult. There is a risk that it could turn into fraud and security issues.*
- *In Turkey, the authenticity of identity has been successfully determined remotely via the digital identity card hologram element.*

Graphical Abstract

The usability and performance level of the hologram element has been investigated in remotely detecting the authenticity of Turkey's digital identity cards with computer aid. 227 digital IDs were used through the application developed for this purpose, and 99.56% success was achieved as a result of the tests.

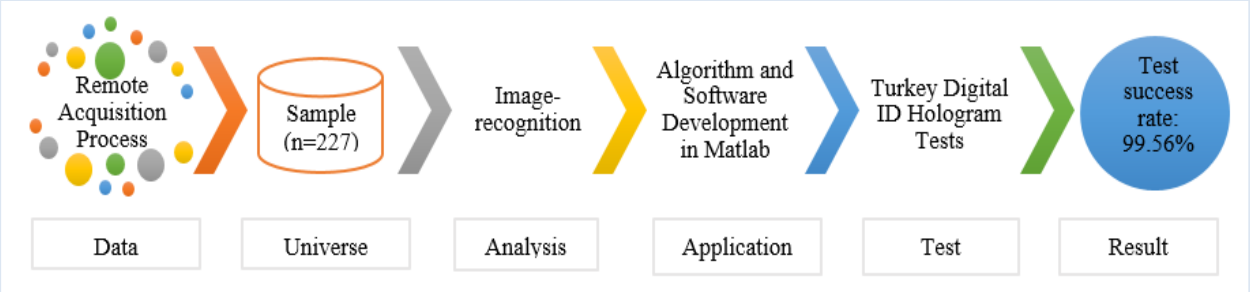


Figure. Turkey digital ID card hologram accuracy test process stages

Aim

It is aimed to investigate whether the authenticity of the hologram image on the TR digital ID card can be used safely in remote transactions.

Design & Methodology

Hologram detection was carried out over all the frames on the sample images taken by video shooting. Threshold values were determined for color level, similarity rate and similar data for control purposes. Neumann and Moor 2-D neighborhood method, one of the edge detection methods, was used to detect the crescent. Special functions have been developed for control purposes on the MATLAB application platform. Tests and controls were carried out using 227 digital ID cards on a single mobile device.

Originality

It is a computer-assisted original study to ensure that the authenticity of the qualified document can be detected in remote services, as well as the services provided in the presence.

Findings

A similarity of approximately 99.56% was found between the computer-assisted test and the visual controls. It was found that the only result that differed between the two tests was due to the flash firing during shooting.

Conclusion

As a result of the tests and controls performed on 227 digital ID cards, a success rate of 99.56% was achieved. The test result of a card was found to be unsuccessful due to the flash that exploded during shooting.

Declaration of Ethical Standards

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Türkiye Dijital Kimlik Kartı Hologram Öğesinin Uzaktan Tespitine Yönelik Bir Çalışma

Araştırma Makalesi / Research Article

Ender ŞAHİNASLAN[1], Abdullah KÖKSAL[2], Önder ŞAHİNASLAN[3*]

1Computer Engineering, Faculty of Engineering, Trakya University, Edirne, Turkey
[2]Computer Engineering, Faculty of Engineering and Natural Sciences, Maltepe University, Istanbul, Turkey
[3]Department of Informatics, Maltepe University, Istanbul, Turkey

(Geliş/Received: 26.08.2022 ; Kabul/Accepted: 09.11.2022 ; Erken Görünüm/Early View: 11.12.2022)

ÖZ

Teknolojik gelişmeler ve pandemi, uzaktan sunulan hizmetlere talep patlamasına neden olmuştur. Bankacılık, sigortacılık, noter gibi kritik süreçlerde uzaktan sunulacak hizmetin huzurda verilen hizmet kadar hızlı ve güvenli sunulma zorunluluğu vardır. Bu tür hassas süreçlerde kişi kimlik kartı gerçeklik tespiti doğru ve güvenli yapılmak zorundadır. Doğruluk tespitinde kullanılan tekniklerden birisi temassız yonga teknolojisini destekleyen mobil cihazların kullanılmasıdır. Ancak, günümüzde bu yöntemi kullanan mobil cihazların sayısı oldukça sınırlıdır. Bu durum, uzaktan verilen hizmet ve kaynakların etkin ve yaygın kullanımına engel teşkil etmektedir. Bu yüzden temassız yonga teknolojisine alternatif olacak, yaygın kullanımın önündeki engelleri kaldıracak ve sahtecilik gibi olayları azaltacak farklı bir çözüme yöntemine ihtiyaç duyulmuştur. Bu çalışmada, Türkiye dijital kimlik kartlarının doğruluk tespitinde kimlikte yer alan güvenlik ögelerinden olan hologramın kullanılıp kullanılamayacağı araştırılmıştır. Bu amaçla, hologram üzerindeki hilalin tespiti için 2-D komşuluk yöntemlerinden yararlanılarak özel fonksiyon ve program MATLAB uygulaması üzerinde geliştirilmiştir. 227 adet dijital kimlik kartı öncelikle renk düzeyi ve benzerlik oranı gibi belli eşik değerler üzerinden mobil bir cihaz üzerinden test edilmiştir. Ardından testte kullanılan her bir kart çıplak gözle tek tek incelenmiştir. Uygulama üzerinden yapılan test bulgularıyla çıplak gözle yapılan kontroller sonrası elde edilen bulgular arasında yaklaşık olarak %99,56 oranında benzer sonuçlar elde edilmiştir. Elde edilen bu yüksek başarım oranı dijital kimlik kartı üzerinde yer alan güvenlik öğelerinden güvenli hologram görselinin uzaktan sunulacak hizmetlerde bilgisayar destekli olarak kullanılabilir olduğu sonucuna ulaşılmıştır. Bu çözüm yöntemiyle banka, noter, eğitim gibi birçok alanda uzaktan verilmesi düşünülen hizmetlerin önündeki önemli bir engelin aşılmasına katkı sunulmuştur

Anahtar Kelimeler: Dijital kimlik, uzaktan edinim, hologram, bilişim, bilgi güvenliği.

A Study on Remote Detection of Turkey Digital Identity Card Hologram Element

ABSTRACT

Technological advances and the pandemic have caused an explosion in demand for remote services. In critical processes such as banking, insurance and notary public, the service to be provided remotely has to be provided as quickly and safely as the service provided in presence. In such sensitive processes, the identity card authenticity detection must be done accurately and securely. One of the techniques used in accuracy detection is the use of mobile devices that support contactless chip technology. However, the number of mobile devices using this method is limited today. This situation hinders the effective and widespread use of remotely provided services and resources. Therefore, a different solution method was needed that would be an alternative to contactless chip technology, remove the obstacles to widespread use and reduce incidents such as counterfeiting. In this study, it was investigated whether the hologram, which is one of the security elements in the identity, can be used in determining the accuracy of Turkey's digital identity cards. For this purpose, a special function and program has been developed on the MATLAB application by using 2-D neighborhood methods to detect the crescent on the hologram. 227 digital ID cards were first evaluated on a mobile device over certain threshold values such as color level and similarity ratio. Then, each card used in the test was examined one by one with the naked eye. Approximately 99.56% similar results were obtained between the test findings made over the application and the findings obtained after the controls made with the naked eye. It has been concluded that the secure hologram image, one of the security elements on the digital ID card with this high success rate, can be used as computer aided in remote services. With this solution method, it has contributed to overcome an important obstacle in front of services that are thought to be provided remotely in many fields such as banks, notaries and education.

Keywords: Digital identity, remote acquisition, hologram, informatics, information security.

1. INTRODUCTION

Today, there are a lot of developments such as internet of things, machine-to-machine communication (M2M), artificial intelligence, quantum computers, and blockchain technology [1]. With the development of information technologies and the widespread use of internet/mobile applications, digital platforms are increasingly taking place in human life [2]. As a result of the COVID-19 pandemic and the strict measures taken, it

*Sorumlu Yazar (Corresponding Author)
e-posta: ondersahinaslan@maltepe.edu.tr

has caused fundamental changes in people's buying habits of goods and services. Various researches and attempts have been made on the direction of this change, and its permanence and the fulfillment of needs. In studies conducted in Turkey, significant grows have been observed in the number of new and active users in the field of e-commerce and remote acquisition following the pandemic announced in March 2020. One of the studies on the increasing trend and whether this trend is permanent is the study of Hacıalioğlu and Sağlam. In accordance with this study, it is stated that there has been an expand of up to 200% in e-commerce transaction volume after the pandemic started (3/11/2020) in our country [3]. Following the results of the survey conducted by one of the international research institutions, McKinsey, in nine of the 13 large countries; At least two-thirds of the consumers surveyed revealed that they have tried new ways of shopping, and more than 65% are considering continuing to do so [4]. In compliance with the results of the Manager and SME survey conducted by Ernst & Young research company in Turkey in 2020, 40% of the participants stated that the changing consumer behavior after the pandemic will be permanent in the long run [5]. Another study by Deloitte, it was predicted that the share of e-commerce in retail globally exceeded 15%, it is expected to exceed 20% in 2025, and 80% of consumers will prefer online channels after the pandemic [6]. In the global assessment, it has been determined that the e-commerce boost seen in the first half of 2020 is equal to the previous ten years; It has been revealed that the decisions taken by companies and governments will play a key role in the persistence of post-pandemic habits [7]. Another study by KPMG shows that while the mobile e-commerce market had 41 percent of the total e-commerce market size before the pandemic, this rate escalated to 53 percent with the pandemic. In addition, the rise in the rate of smartphone usage in the future; With the development of new, practical and secure payment methods, the share of mobile e-commerce in the Turkish e-commerce market is predicted to raise to 80% in 2025 [8].

As a consequence of the changing habits after the COVID-19 epidemic, new needs have emerged in customer acquisition and service procurement based on wet signed contracts. Banking customer acquisition process is one of them. Prior to the pandemic, due to legal requirements, contracts with wet signatures were required by law during customer acquisition. The signature and identification of the contracts require the bank officials and the customer to be in the same environment and to make a statement in the presence. Nonetheless, as a result of the developments and needs arising after COVID-19, the new communiqué published by the Banking Regulation and Supervision Agency (BRSA) on 4/1/2021 enabled customer acquisition processes through remote identification [9]. In this new communiqué article drawing the general lines of the innovation, “Remote identification is done by online video calling and communicating with each other, without the need for the customer representative and the person to be physically in the same environment”. "Adequate security measures are taken, taking into account the risks" with the article, the responsibility of establishing the appropriate technological environment is left entirely to the banks. With the entry into force of this communiqué on 5/1/2021, banks started to receive requests via remote acquisition. Remote customer acquisition figures between May 2021 and February 2022 published by the Banks Association of Turkey (BAT) are shown in Figure-1 [10].

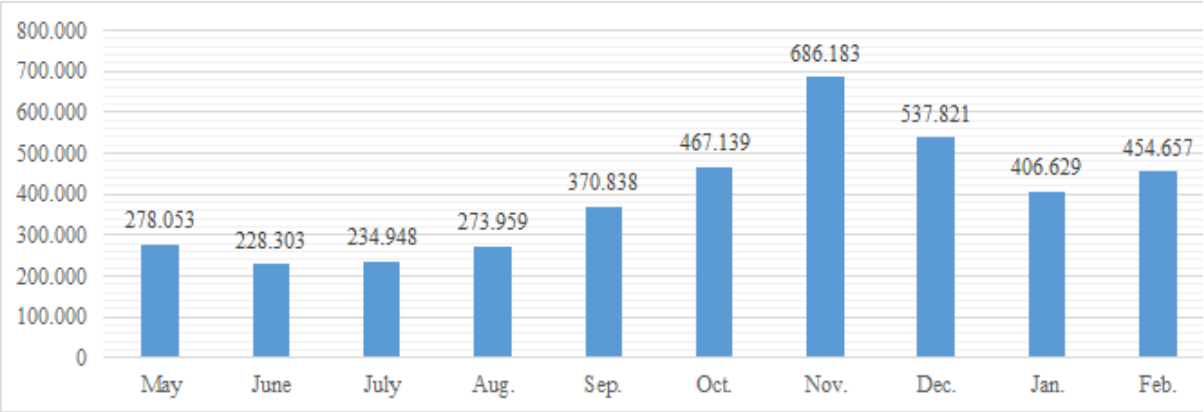


Figure 1. Number of remote customer acquisition applications from May 2021 to February 2022

As can be seen from these data, the demand for remote acquisition has shown an increasing trend day by day. While 278,053 applications were made in May 2021, 686,183 applications were made in November 2021. At the end of ten months, the number of remote acquisition applications made to banks was 3,938,530 in total. Nevertheless, despite the high number of applications, only 1,021,408 customers' transactions were successful. The remaining 2,917,122 applications were inconclusive or unsuccessful, with a high rate of approximately 74%. While some of the unsuccessful applications were due to technical infrastructure such as insufficient internet speed and lighting environment, the other part was due to the fact that Near Field Communication (NFC) technology

was not supported by all user mobile devices or could not be used. On the other hand, attending the video-interview unprepared, not having his identity card with her or applying with his old identity card are some of the he can't be a customer. As stated by the Communiqué, it is obligatory to make a video call between the customer and the bank official in applications. This requires that at least one bank official attend the interviews one-on-one in the applications made. Considering that approximately 74% of the applications are unsuccessful or not evaluated, it is seen that it causes a serious loss of business on the bank's side. This operated process will be used not only for customer acquisition, but also for other processes such as product sales or renewal of old contracts. This situation may cause loss of customers as well as loss of workforce. In the light of increasing demands and requirements, there is a need for research that offers innovative solutions with the more effective and efficient use of information technologies. One of them is to investigate the success of the computer-assisted hologram (kinegram) accuracy test, which contributes to the successful realization of remote acquisition service with mobile devices that do not support NFC technology. Kinegram is a kind of hologram that contains optical elements with special type of diffraction by computer. It is designed to display kinematics, color changing, reverse contrast and other special effects on the ID and is technically also called DOVID [11]. In the classical method, the way to understand whether the identity is real or fake/falsified was made by examining the visual security elements on the ID card by experts. In the new communiqué [9], it has been stated that in remote identification, in cases where verification cannot be made over the contactless chipset, the visual security elements of the identity document can be used. Our study will be aimed at investigating the feasibility of some visual security controls made with the eye with technological methods. The digital identity shared by the General Directorate of Population and Citizenship Affairs of the Republic of Turkey [12] and the security elements on the identity are shown in Figure-2.

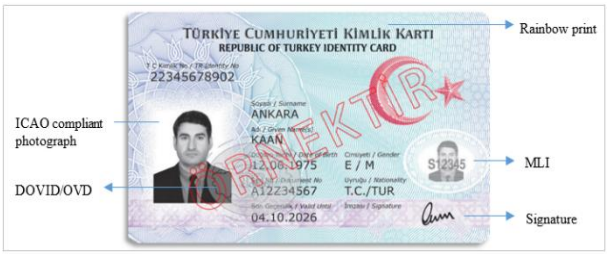


Figure 2. TR identity card sample and security items

There are various visual security elements on the Republic of Turkey (TR) digital identity (ID) card. Among them, the Diffractive Optically Variable Image Device (DOVID) element is a two- or three-dimensional, micro-structured design with kinematic and color-changing effects, which is difficult to imitate conforming to the reflection angle of the hologram optical variables with the laser technique. Optically Variable Device (OVD) is a security element that gives a different appearance depending on the viewing angle and verification conditions. Multiple Laser Image (MLI), on the other hand, is an item called ghost image, which is used to prevent tampering with cards. The photo of the person on the card is reduced in size, and the picture becomes clear when the card is angled [13].

In this study, using technological methods, the validity of the identity will be evaluated on the hologram element with the video shooting, which is considered to have taken place before the interview, and if it is successful, it will lead the expert for the interview.

2. LITERATURE

As specified by the BRSA communiqué published in the Official Gazette dated 4/1/2021; In identification, the use of the identity card defined in the Republic of Turkey Identity Card Regulation published in the Official Gazette dated 12/3/2019 and numbered 30967 is accepted as a basis. As one of the identification methods of the ID card, it was requested to verify the information and photos in the chip with NFC technology, which is called near field communication. If this verification cannot be done for any reason, it has been reported that at least four of the visual security elements of the identity document (clothing, rainbow printing, optically variable ink, hidden image, hologram, micro writing) must be verified in terms of form and content [9]. As specified by the information given on the official website of the General Directorate of Population and Citizenship Affairs; The development of the TR identity card has been provided by TUBITAK in accordance with international standards, compatibility and security principles. In the UEKAE magazine published by TUBITAK [14] TR detailed information about the identity card is given. In particular, under the title of 'TR Identity Card Management and Distribution', information about electronic identity card features and visual security elements is given, and it is stated that the Republic of Turkey identity cards are developed in line with ICAO-9303 standards. In agreement with the 'Chicago Convention' signed by 193 national governments in 1944, the International Civil Aviation Organization (ICAO) pioneered the development of travel document standards, detailing visual and technical issues in order to support their diplomacy and cooperation in air transport and to ensure the sustainable growth of the global civil aviation system and a set of standards named 'Machine Readable Travel Documents Doc 9303' has been developed [15].

Various studies have been carried out to use the TR identity card, whose infrastructure has also been developed for receiving electronic services, in payment recording devices. In the study conducted by Yoldaş [16], it was revealed that with the CHIP & PIN verification method, new TR identity cards can be a secure payment tool as well as bank cards; The benefits, innovations and integration solutions provided by the integration with new generation payment recording devices are discussed.

In the study conducted by Mutlugün and Adalıer [17], information about the electronic infrastructure, authentication architecture and components of the digital TR identity card is given. In this study, it has been revealed that serious precautions are taken against counterfeiting by means of the chipset on the card, and the importance of visual security measures in increasing the security measures or inability to read the chipset is emphasized.

Similar studies are still up-to-date in identity cards of other countries as well as in TR identity cards. Similar studies on the design and control of technical and visual security elements have been conducted on other country ID cards. Rusli et al. [18] analyzed 25 scanned images with 0.89 F-scores and 25 videos with 0.67 F-scores using OCR and NLP technologies to avoid fraudulent transactions. They calculated that 4510 milliseconds are needed to decode each card by working on these 50 images, which have an average of 0.78 F-scores in total. Abed et al [19] revealed that high-performance results can be obtained in terms of security as a result of the tests they performed on the 'cubic spline co-occurrence code (CCO code). Król et al. [20] demonstrated that with Laser-induced decay spectroscopy (LIBS) technology, the identification of kinegrams, date of birth and emblems on ID cards provides significant benefits in forensic science. Haga et al. [21] conducted research to prevent forgery, as the hologram printed on the cards cannot be reproduced technically, so that personal information can be stored in optical holograms that prove the authenticity of the card. In the study by Mohamed [22], passports of various countries were examined and some suggestions were made to maximize security with features such as micro printing, nano text, kinegram design. He also included in his research the issue of securely printing the photo on the card by combining black laser and CMY separation color inkjet technology. Hartl et al. [23] conducted a study on detecting the hologram on documents with mobile devices and artificial intelligence methods and demonstrated that this could be done in real time. One of the most important constraints of such studies is the need to keep the resource consumption at a minimum when using the information systems infrastructure. It makes recommendations for high performance by comparing the work done by Bataineh [24] on image-analysis and pattern-recognition algorithms. In the study of Zaitsev [25] on d-dimensional cellular automata, he examined the theoretical background of edge detection algorithms and made some suggestions. The determination of the similarities of two different images to each other is one of the topics considered in the detection of the hologram. In the study conducted by Lee and Lim, the formulas used in this subject were compared [26]. On the other hand, internet of things technology and its usage are becoming more and more common, integrated and complex architecture [27]. Digital identities are likely to experience some problems, especially in matters such as management and security. In remote identity detection, deepfeak video detection study was carried out to prevent fraud to be made during video conferencing by using deep learning algorithms [28]. The importance of blockchain technology has been emphasized against the difficulties experienced in associating digital identity and real identity with a secure method [29]. By using the artificial neural network method, 96.5% success was achieved in the diagnosis of breast cancer [30]. Similar studies are carried out on many different methods.

Another prominent topic in this study is edge detection algorithms. Edge detection algorithms are based on detecting local changes on the image. Neumann and Moor's 2-D neighborhood method is the most classic edge detection algorithm known. First order gradient, second order gradient and Gaussian are other classical algorithms [31]. In addition, there are algorithms that offer different approaches such as Geodesic Active Contours based on the primitive closed areas [32]. Various analysis and comparison studies have been carried out on edge detection methods [33].

3. MATERIALS AND METHOD

In this study, hologram detection was performed on all the frames in the sample images taken by video shooting. If the video footage is shot on a color photocopy instead of a real identity card, there are two situations. The first is when the hologram is not visible in the color photocopy. In this case, the hologram will not be detected in the images and a decision will not be able to taken as to whether the identity is real. The second situation is that the color photocopy was taken while the hologram was visible. In this case, the hologram will appear continuously during video shooting. Although this is almost non-existent in real identities, it will still not be possible to reach a definite decision as to whether this identity is real. Another point to consider is; It is a method of bypassing the control by quickly replacing the hologram photocopy and the non-hologram photocopy during video shooting. In order to eliminate this fraudulent situation, the similarity ratios of all frames will be determined consecutively, and if any deviation is detected, necessary actions will be taken to prevent fraud.

Hologram image on ID cards; With the effect of some environmental factors such as light and reflection, it is sometimes visible, and sometimes not. While the hologram (DOVID / OVD) image is clearly visible on the left-hand card of the two ID cards in Figure-3, the hologram on the right-hand card cannot be seen directly

Threshold values have been determined for color level, similarity ratio and some similar data to be used in the control stages leading to the conclusion. It was accepted that the effect of these values on the results was minimal. Instead of detecting the similarity of the detected hologram to its original shape, it was accepted that the count of the points where the reflection was detected is sufficient within the scope of this study. The study was conducted on a single mobile device. It has been observed that the resolution of the device, the variety of

(a) (b)

Figure 3. Examples of visible (a) and invisible (b) holograms on the TR ID card

colors and the number of frames per second are sufficient. Considering that the effect of this diversity on the results is insignificant, a study on device diversity has not been conducted. Again, it is assumed that the lighting is close to daylight in the environment where the process is operated, and the users generally will be in environments close to daylight. No research has been conducted on the effect of these factors on the result to be obtained.

Although MATLAB was used as the working platform, the ready functions of this program were not used in the algorithm we used. Instead, control operations were performed by considering each pixel of the images. The aim here is to make the developed algorithms easily portable on different platforms such as Java/Android, IOS or C++. In the study, the use of third-party libraries was not preferred against the potential to cause addiction or create a security vulnerability. It is aimed that the developed applications are platform independent, flexible and secure.

3.1. Process Flow

The main process steps of the method applied in this study are shown in Figure-4. Selection of a video containing the digital identity images to be used in the study from information system resources and preparation of the study data by separating the identity images over the video recording; analysis by means of mathematical models such as finding edges, determining coordinates in the Cartesian plane, detecting visual similarities; Development of application program parts on MATLAB platform; it consists of testing the method and evaluating the results.

3.2. Study Environment and Conditions

In the study, a video consisting of at least 7 seconds, 227 frames ('frame') and 1920 x 1080 resolution was used. The shots were taken in daylight and the flash was set to turn on automatically in low light. The ID image, which covers at least 80% of the frame, was moved at small angles during the video shoot. Within the scope of this study, identity images whose holograms can be seen with the eye and cannot be seen directly with the eye is selected and studies were conducted on these images. Using these two types of visual and technological methods, a test was conducted to the point that the hologram could not be detected by detecting it.

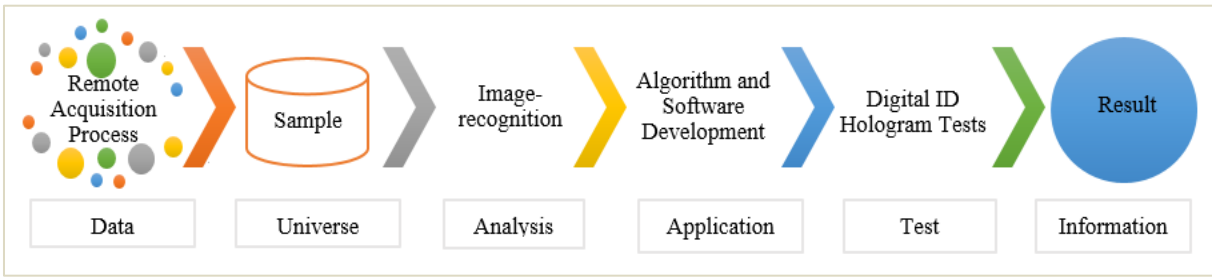


Figure 4. Hologram accuracy test process stages

In this study, some technical presuppositions were made in the selected study data in order to make quick decisions. It is predicted that these assumptions will not have a significant effect on the aim of the study. Identified data presuppositions:

- No fake identity is used in the data obtained from the shootings, the data used in the study is a secure data obtained from real identity cards through a secure application and stored,
- The shootings are performed as standard, with 1920 x 1080 resolution, 29.97 frames/second quality and approximately 20 seconds of footage,
- In cases where the ID image covers at least 80% of the screen, the items on it are visible and legible,
- The flash of the mobile device is turned on when the light is not sufficient,
- It is assumed that the recording with ID is moved slowly with small angles.

3.3. Analysis

It is a characteristic feature of the hologram that a partial part of the figure represented by the hologram is seen instead of the whole. Therefore, In the analysis phase of the study, instead of searching the hologram shape as a whole, it was aimed to determine the area seen on the hologram. Although the objects seen on the hologram are not visible enough, the analysis study also focused on the detection of the crescent on the identity. For this, first the crescent is determined and then the circumferential circle is determined with the help of the crescent's edge lines, and the radius and center point of this circle are calculated. The ID image for the detection of the crescent and hologram areas performed on the video image frame used in the study is shown in Figure-5.

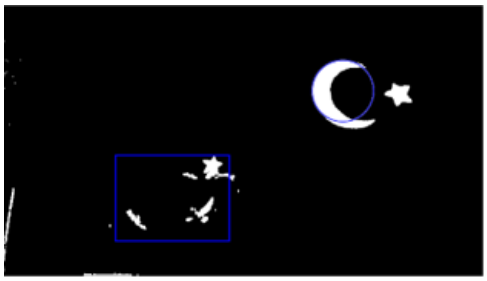


Figure 5. Detection of the crescent and hologram area

For the detection of the crescent, the classical neighborhood method was used in the edge detection method. Among edge detection methods, Neumann and Moor's 2-D neighborhood methods, shown in Figure-6, come to the fore.

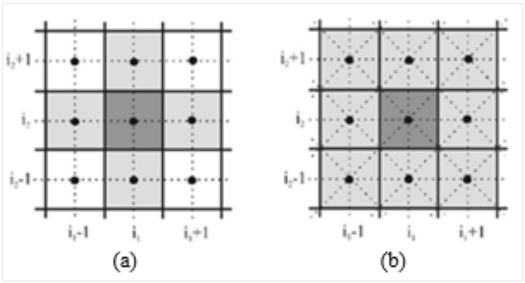


Figure 6. Neumann (a) and Moor's neighborhood (b) [25]

Von Neumann's neighborhood searches for neighborhoods at 4 points in the east, west, north and south directions of the central pixel, while Moor's neighborhood searches for neighborhoods at 8 points, including diagonal directions. In our study, by the Moor's method, while searching for a neighborhood in each point as east, west, north and south, neighborhood relations are also sought in the northeast, northwest, southeast and southwest directions. The edge of the crescent is found by combining the all the points with a neighborhood relationship. Then, the phase of detecting the crescent is started among the found edges. After calculating the radius and center point of the crescent on the image, the place to search for the hologram is calculated and it is analyzed whether the hologram is visible enough or not. The center point and radius of the crescent are found with the help of circumcircle formulas (2, 3 and 4) by using the three edge points (1) of the crescent we detected.

After the location of the hologram are determined, the number of pixels representing the hologram is divided by the number of pixels representing the rectangle covered by the hologram and it is checked whether it is seen sufficiently. The determination of this ratio is made by considering the visuals whose holograms are detected with the eye. The analysis made up to this stage is aimed at detecting the hologram on a single frame. Notwithstanding, fraudulent transactions can be made in such transactions. One of them is that the video was shot with a color photocopy with the hologram visible. In order to detect this deception, an analysis study was conducted to determine whether the hologram could be detected in all frames of the video. If hologram information is detected on all frames (227 units) taken from the video used in the study, or if hologram information cannot be detected on any frame, this situation is considered as a suspicious transaction.

Another attempt to mislead is the method of combining multiple videos with visible and invisible holograms. In

In Cartesian plane, A, B and C are 3 points on the circle; Let the center be represented by O and radius r [34, 35].

$$A = (A_x - A_y),\ B = (B_x - B_y),\ C = (C_x - C_y),\ O = (O_x, O_y) \quad (1)$$

The center of the circle is calculated with the help of the equations O coordinate (dx), y coordinate (dy) and radius r (2, 3 and 4).

$$d_x = \frac{({A_y}^2 + {A_x}^2) \times (B_y - C_y) + ({B_y}^2 + {B_x}^2) \times (C_y - A_y) + ({C_y}^2 + {C_x}^2) \times (A_y - B_y)}{\left(2 \times (A_x \times (B_Y - C_y) + B_x \times (C_Y - A_Y) + C_X \times (A_y - B_y))\right)} \quad (2)$$

$$d_y = \frac{({A_y}^2 + {A_x}^2) \times (C_x - B_x) + ({B_y}^2 + {B_x}^2) \times (A_x - C_x) + ({C_y}^2 + {C_x}^2) \times (B_x - A_x)}{\left(2 \times (A_x \times (B_Y - C_y) + B_x \times (C_Y - A_Y) + C_X \times (A_y - B_y))\right)} \quad (3)$$

$$r = \sqrt{(A_x - d_x)^2 + (A_y - d_y)^2} \quad (4)$$

order to determine this, the similarity of the two images with each other was studied. For this, formulas used in compression algorithms that mathematically measure the quality of the obtained images were used. MSE (5) and PSNR (6) formulas are the most frequently used formulas that provide information about the difference and degradation criterion of a compressed image from the original image [26]

$$\text{MSE} = \frac{1}{n}\sum_{i-1}^{n}(Y_i - Y_i')^2 \quad (5)$$

$$PSNR = 10log_{10}\left(\frac{Max^2}{MSE}\right) \quad (6)$$

In the MSE calculation, the difference of the pixel values of the same point on two consecutive images was taken and the square was calculated. Then, this process was done separately for all pixels and the sum was calculated, and the average value was calculated by dividing this result by the total number of pixels. The result obtained corresponds to a single real number, it is not possible to reach a meaningful result with this number alone. Since the ID is thought to be moved slowly and at small angles in the video, the PSNR value of each consecutive frame will be close to each other. Thus, a series is obtained by calculating PSNR on all consecutive frames. Max in PSNR formula is the maximum value a pixel can take. If a sudden deviation is detected in the sequential values, this process is considered suspicious.

3.4. Application

In this study, the accuracy of the method has been investigated by first working on an identity image the hologram of which is seen with the naked eye, and then another identity images the hologram of which is not seen or only slightly visible. Finally, the test was performed on another copy whose hologram was not visible. To show the feasibility of the study, it is preferred to use small parts instead of the whole algorithm. Due to its characteristic feature and environmental factors, the algorithm used cannot determine the exact shape of the hologram. Therefore, the ratio of the pixels to be detected to the searched area were considered as the decision point. For these and similar reasons, threshold values have been determined at some decision points, taking into account the risk perception of the work done. Thus, by assigning appropriate values for environments with low-risk perception and limited resource, it was ensured that the process progressed more easily.

As can be seen, the hologram on the TR ID card consists of colors red, blue and green tones. For this reason, the image is separated into 3 color channels as red, green and blue. Sample software source code is in Algorithm 1.

Algorithm 1. Code to parse color channel

```
% Red, green and blue color generation
  RM = uint8(I(:, :, 1));
  GM = uint8(I(:, :, 2));
  BM = uint8(I(:, :, 3));
```

In order to facilitate the detection of the crescent, the gray tone of each channel is changed to white and cleared. The hologram appears in different colors and as small particles. Therefore, the red-dominated color is only seen in the red channel and not in other channels. This also applies to the other channels. Thus, the images in all three channels are superimposed, allowing the hologram to appear more clearly. By creating a negative image of the resulting image, it is easier to see the results with the naked eye. The purpose of creating the negative is to see the image better during the study, for examination purposes. Here, threshold values of 40 for pGreyMin and 128 for pGreyMax were set to detect grayscales. The software source code used is given in Algorithm 2.

Algorithm 2. Code to remove grayscale and create negative.

```
% Clearing gray tones
CGreyMin = 40;  CGreyMax = 128;  V = 0;
İf (RM(i0,j0)-GM(i0,j0)<pGreyMin &&
   RM(i0,j0)-BM(i0,j0)<pGreyMin)   V = 255; end
if (RM(i0,j0)<pGreyMax)    V = 255; End
  RX(i0,j0) = V;    V = 0;
if (GM(i0,j0)-RM(i0,j0)<pGreyMin &&
   GM(i0,j0)-BM(i0,j0)<pGreyMin)   V = 255;  end
if (GM(i0,j0)<pGreyMax)    V = 255; end
GX(i0,j0) = V;    V = 0;
if (BM(i0,j0)-GM(i0,j0)<pGreyMin &&
   BM(i0,j0)-RM(i0,j0)<pGreyMin)    V = 255; end
if (BM(i0,j0)<pGreyMax)   V = 255; end
BX(i0,j0) = V;
% Superimposing the three channels and creating the negative
if ((BX(i0,j0)==0 ||GX(i0,j0)==0)||RX(i0,j0)==0)DX(i0,j0) = 255;
else DX(i0,j0) = 0; end
```

In order to detect the crescent on the new image obtained, all elements on the image must be a closed area. For this purpose, the neighborhoods of all objects on the image were examined, and the elements were converted into closed areas and the boundaries of these closed areas were determined. Thus, only the edges of each element were detected. The piece of software source code used for this is in Algorithm 3.

Algorithm 3. Code to detect visual element edges

```
% Converting the pixels of the detected items to a clearer area with
neighborhood relationship (CX)
  K = 0;
  K =K+DX(i0-2,j0-1) + DX(i0-2,j0) + DX(i0-2,j0+1);
  K =K+DX(i0-1,j0-1) + DX(i0-1,j0) + DX(i0-1,j0+1);
  K =K+DX(i0,j0-1)   + DX(i0,j0+1);
  K=K+DX(i0+1,j0-1)+DX(i0+1,j0)+ DX(i0+1,j0+1);
  K=K+DX(i0+2,j0-1)+DX(i0+2,j0)+ DX(i0+2,j0+1);
  if (K>0) CX(i0,j0)=255;   end
% Detection of edge points of detected elements (VX)
  K = 0;
  K = K+CX(i0-1,j0-1)+CX(i0-1,j0)+CX(i0-1,j0+1);
  K = K + CX(i0,j0-1);
  if (K>1 && K<4*255)   VX(i0,j0)=255;   end
```

Each of the closed areas obtained was evaluated and checked for crescent. At this stage, neighborhood distances were determined using the Moor's neighborhood method. The software source code of the method used to detect the crescent is shown in Algorithm 4.

Algorithm 4. Code to crescent detection

```
% Calculation of the approximate radius of the crescent
for i0=1:H
   for j0=1:W
      if VX(i0,j0)==255
       [isExist, x1, y1, x2, y2, x3, y3] = findCrescent(VX,i0,H,j0);
       if (~isExist)
            continue;
         end
       [isExist, x,y,r] = findCircle(x1,y1,x2,y2, x3, y3);
        if isExist
            [rIsExist] = findHologramArea(CX,x,y,r);
            return;
         end
       end
   end
end
% Detection of the crescent
function [isExist,x1,y1, x2,y2, x3,y3] = findCrescent(VX, i0,i1,j0)
   vec = [i1,2];     j1 = j0;
   for i2=i0:i1-2
      if VX(i2+1,j1-1)==255
          j1 = j1 -1;  vec(i2-i0+1,1) = i2;  vec(i2-i0+1,2) = j1;
      elseif VX(i2+1,j1)==255
         vec(i2-i0+1,1) = i2;    vec(i2-i0+1,2) = j1;
      else break;
      end
   end
   if ((i2-i0)<50 || i2==i1-2)
    isExist=false;  y1=0;  x1=0;  y2=0;  x2=0;  x3=0;  y3=0;
   else
     isExist = true;    y1 = i0;    x1 = j0;     y2 = i2;    x2 = j1;
     y3 = vec(int16((i2-i0)/2),1);  x3 = vec(int16((i2-i0)/2),2);
   end
end
```

Following the detection of the crescent, the software code fragments regarding the method used in calculating the center point and approximate radius of the circumcircle representing the crescent, and also in determining the area where the hologram will be searched are given in Algorithm 5.

Algorithm 5. Code to detection crescent circumference and hologram area

```
% Cresccent circums cribed circle center and radius determination
function [rIsExist, dx,dy,r] = findCircle(Ax,Ay,Bx,By,Cx,Cy)
CCircleRMin = 100;   CCircleRMax = 150;
D = (2*(Ax*(By-Cy) + Bx*(Cy-Ay) + Cx*(Ay-By)));
dx = ((Ay^2 + Ax^2)*(By-Cy) + (By^2 + Bx^2)*(Cy-Ay) + (Cy^2
+ Cx^2)*(Ay-By))/D;
dy = ((Ay^2 + Ax^2)*(Cx-Bx) + (By^2 + Bx^2)*(Ax-Cx) + (Cy^2
+ Cx^2)*(Bx-Ax))/D;
r = ((Ax-dx)^2 + (Ay-dy)^2)^0.5;
rIsExist = false;
if  r > CCircleRMin && r < CCircleRMax     rIsExist = true;
end
end


% Detection of the hologram area
function [rIsExist] = findHologramArea(IX,cx,cy,~)
CExistRatio=4; x1=int32(cx/3); w1=int32(x1);
y1=int32(1.75*cy); h1=int32(cy);    pC = 0;
for i0=x1:x1+w1
   for j0=y1:y1+h1
      if IX(i0,j0)==255    pC = pC +1;
       end
end
end
rIsExist = false;
xratio = pC*100/(w1*h1);
% Marking the specified items with a blue line
color = 'r';
if (xratio > CExistRatio) rIsExist = true;   color = 'b';  end
rectangle('Position',[x1,y1,w1,h1],'EdgeColor',color,
'LineWidth',3, 'LineStyle','-');
imwrite(IX, 'D:\output\10-Area.jpg','JPEG' )
end
```

Additional controls have been developed to prevent video forgery during shooting. This control method is based on the detection of the difference between two consecutive images. If a serious jump is detected between the differences of these consecutive frames, it is foreseen that some fraud prevention checks will be made at this point. MSE and PSNR formulas were used to find the difference between the two images. The program part in Algorithm 6 was used as the similarity method.

Algorithm 6. Code to detect similarity of video frames

```
% Detection of the difference between consecutive images obtained
from the video
Max = 227    Min = 1    Diff = [max,3]
for i0 = min:max
 [p,m]=detectDiff(i0);  Diff(i0,1)=p;  Diff(i0,2)=m;  Diff(i0,3)=i0;
end
-- Calculating the difference of two consecutive images
  function [p,m] = detectDiff(i0)
     f1 = strcat('D:\2\', int2str(i0), '.png');
     i1 = rgb2gray(imread(f1));
     i1 = i1(:,:,1) > 200;
     f2 = strcat('D:\2\', int2str(i0+1), '.png');
     i2 = rgb2gray(imread(f2));
     i2 = i2(:,:,1);
     [rows, columns] = size(i1);
     squaredError = (double(i1) - double(i2)).^ 2;
      m = sum(squaredError(:)) / (rows * columns);
     p = 10 * log10( 256^2 / m);
  end
```

4. RESULTS

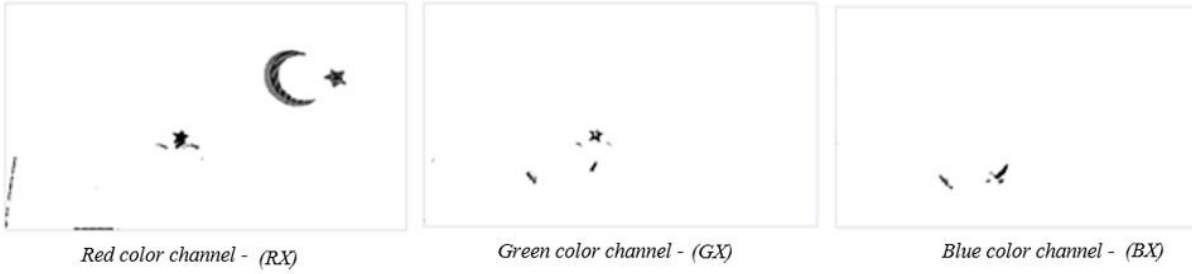
Tests for the detection of the hologram on the ID card and data integrity were conducted in three stages, through the programs developed in accordance with the methods proposed in this study. In the first stage, the hologram on the ID is clearly visible, the second stage is the situation where the hologram is not visible, and the third stage is for evaluating the situation of adding different images into the video recording.

4.1. Test findings of the situation where the hologram is visible on the ID

With this example; Studies were carried out to distinguish the main color on the identity, to clear the gray color areas, to take negative of image for determine the closed area boundaries of the elements, to calculate the crescent's center and radius and to determine the hologram. At the first test, the image was separated into 3 color channels, red, green and blue. The findings obtained as a result of this decomposition are shown in Figure-7

Red color channel result (RM) *Green color channel result (GM)* *Blue color channel result (BM)*

Figure 8. Red, green and blue color channel separation results



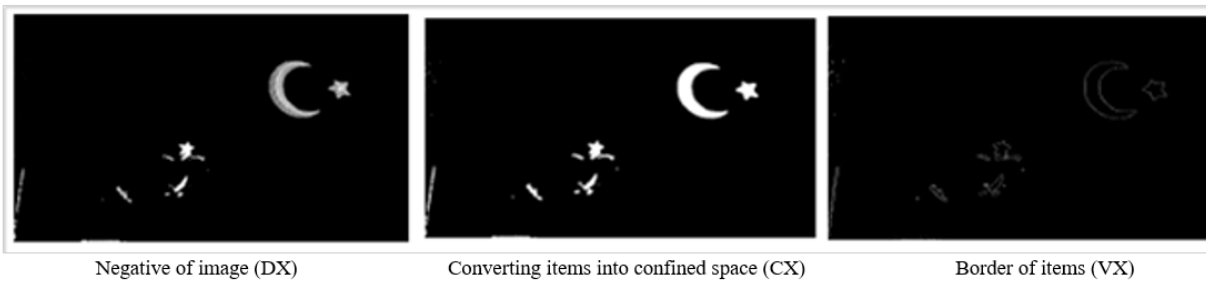
Red color channel - (RX) *Green color channel - (GX)* *Blue color channel - (BX)*

Figure 7. Results of clearing gray areas from red, green and blue color channel image

Each of the red, green and blue colors on the ID are predominantly seen in its own color channel. Intermediate colors other than these primary colors are in gray toning. To detect of the crescent, gray tones in the channels are converted to white. The findings regarding the images obtained as a result of the gray color cleaning study are shown in Figure-8.

The negative of the image was taken so that the hologram could be seen more clearly. Then, the neighborhood of the crescent and other objects was determined so that the items on the identity could be represented as a closed area, and the items were turned into a closed area. Then, the boundaries of the closed areas were determined and the elements were represented linearly (vectorial). Thus, the diameter of the approximation circle representing the crescent can be found more easily. In this determination, Moor's neighborhood' method was used. Findings related to the images obtained as a result of the processes are shown in Figure-9 in order of testing.

With the help of these methods used, the area where the hologram will be searched was determined. The image obtained from an example identity regarding this is shown in Figure-10. Since the video is shot at an angle to the ID, the crescent appears as an ellipse rather than a circle. Because of this angle was not taken into account, assuming that it was too small and its effect on the



Negative of image (DX) Converting items into confined space (CX) Border of items (VX)

Figure 9. Visual negative, closed space loop and linear translation images of elements

calculations would be limited. When the original ID card is examined, it is seen that the hologram consists of strong red, green and blue colors.

Figure 10. Image example of ID hologram area detection

4.2. Findings on the situation where the hologram does not appear in the digital identity

In this section, the results are emphasized when the hologram cannot be seen with the naked eye. The visual findings of the test performed on the ID card, which is not clearly visible by eye, are presented in Figure-11, respectively. As a result of the tests, the area searching for the crescent and hologram was determined, but no information pointing to the hologram could be accessed in this area. For this reason, it could not be determined whether the identity was a real identity or not.

.3. The state of adding image frames on the video

Aiming to evaluate this method, the 51st frame of the 227-frame video footage was manually replaced with a different image. For this process, another image from the same video with the same TR ID card was used. Using the algorithm in Figure-11, a test was performed to detect the similarity or deviation between consecutive frames. The findings obtained from the original-colored images as a result of this test are shown in Figure-12

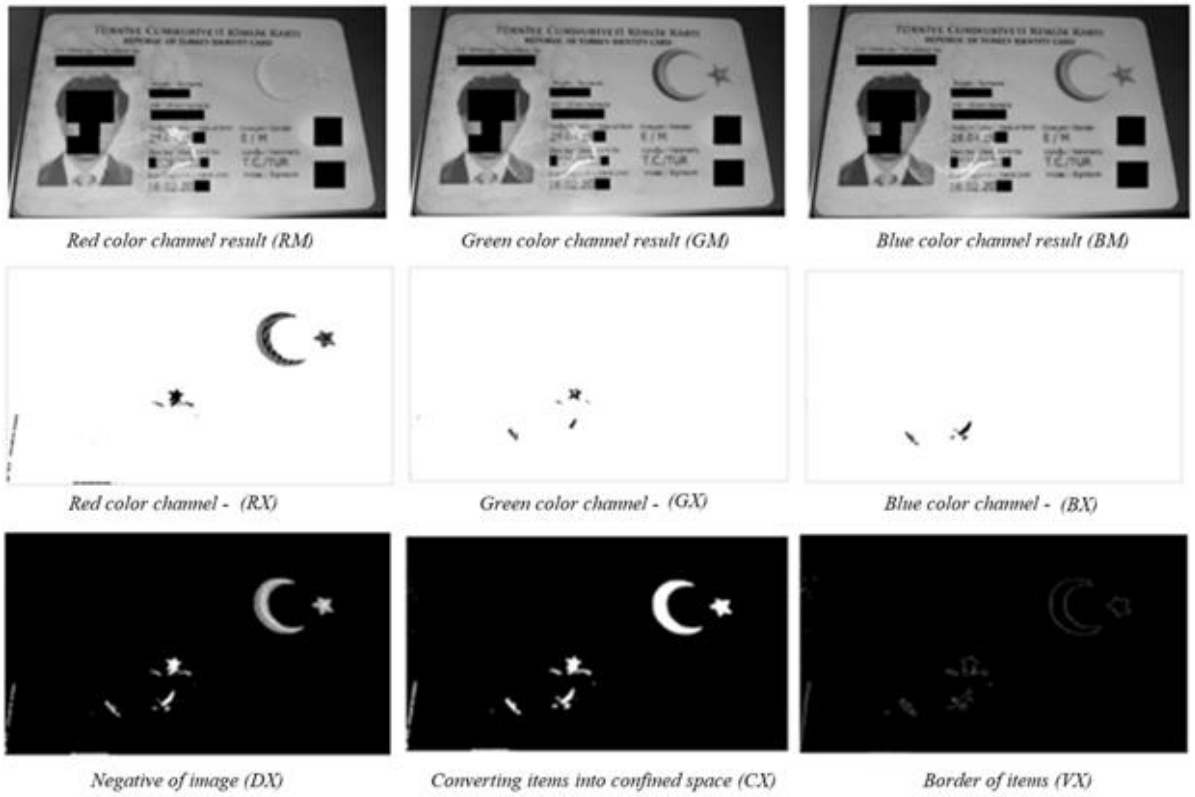


Figure 11. Test results on an ID card where the hologram is not clearly visible

Gray areas and weak colors were eliminated by bleaching. As a result of this bleaching, all remaining meaningful pixels were considered as part of the hologram. Thus, the number of significant pixels in this area, the ratio obtained by dividing the area by the number of all pixels, contributed to making the detection of the hologram more sensitive.

Figure 12. Similarity frequency of sequential original-color images

The graph of the similarity frequency test result made over the sequential images taken over the red color channel is shown in Figure-13. A sudden deviation is observed in the 51st and 66th frames of these two graphs.

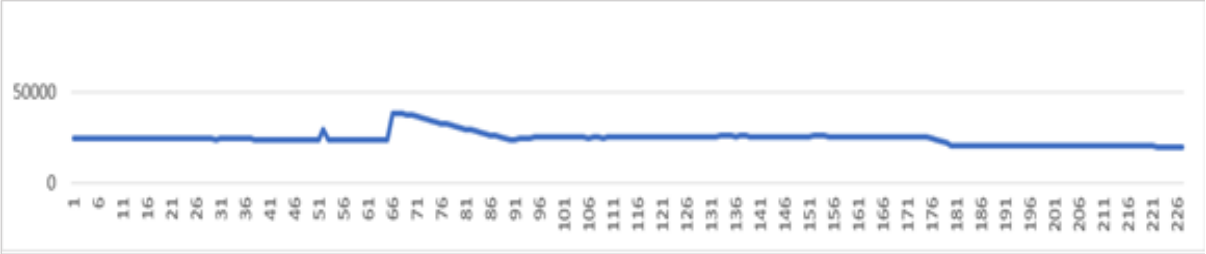


Figure 13. Similarity frequency of sequential red color channel images

5. DISCUSSION

The remote acquisition processes, which have started to be used in banks, have a guiding quality among other sectors. It is known that similar preparations are made in other public and private sectoral areas as well. Efforts are underway for regulations in the public sphere, especially for investment and other finance sectors, payment institutions and insurance companies. On the other hand, private institutions aiming to provide consultancy services in the fields of law or health are making various attempts to develop their processes in a similar framework and to provide remote services. Considering these trends, it is of significant importance to increase the performance of successful results to higher levels. For this reason, detecting visual security elements with technological methods before the video interview will give us serious gains in this regard. If it is not possible to determine that the customer ID is valid before the meeting with the authorized person, the process will be interrupted and thus the loss of work of the authorized person will be prevented and process performance problems will be minimized. On the other hand, dependency on mobile devices that do not have contactless chipset technology will be eliminated and customer satisfaction will be proliferating relatively.

In this study, a computer-assisted method was proposed and tests were carried out by using the hologram object, which is difficult to imitate and detect, in determining the validity of digital identity in remote acquisition processes. The test result of adding a different image frame on the video consisting of 227 frames is given in Figure-12 and Figure-13. A serious deviation was observed in the similarity ratio of the 51st and 66th frames of these graphs. Frame 51 were easily captured as it were a deliberately modified frame for testing purposes. In the 66th frame, it was determined that such a difference occurred due to the flash being turned on during video shooting. Therefore, the need to perform general controls separately in the [1, 50], [52, 66] and [67, 226] intervals has arisen. If continuous holograms are detected during the examination made at these intervals, we can assume that the video was shot with a color copy instead of an original ID. Although this is not proof that the ID is fake, it will not indicate that the ID is a valid ID. Again, if the hologram cannot be detected at all during the examination conducted at these intervals, then the validity of the identity will not be determined. If the number of frames with hologram detected is less than the number of frames of these intervals, the authenticity of the identity is confirmed.

This number of intervals and the ratio of the number of hologram frames detected is a threshold value that should be examined separately. As a result of the examinations and controls made on the images used in this study, the threshold value for hologram detection was found to be at least 4%. This value has been obtained as a result of visually labeling the hologram information in 227 identity images, which can be detected by eye or not. On the other hand, it is possible to accept a different threshold value depending on the sensitivity of this threshold value, the criticality of the process in which the identity information will be used, and the level of risk. For example, the sensitivity of identity verification to be used in banking, notary, land registry transactions and the level of risk perception and sensitivity expected from identification to be made in an e-training registration process are different. This labeling should be determined according to the criticality level and risk perception of the process to be used and the cost it will cause. In addition, in critical processes with a high-risk perception, the control mechanism can be strengthened by the use of other security elements such as the crescent, ellipse and Turkey map in the hologram, as well as the meaningful pixel ratio on the hologram. In the study, it was considered as a presupposition that the identity would stand straight, that is, the crescent would be positioned in the upper right. Although this is not directly within the scope of this study, it will create difficulties in terms of user experience. Instead, the fact that the ID is filmed in any position can contribute to increasing user satisfaction. In order to apply this method, the image must be normalized with coordinate transformations. Howbeit, this has the potential to create a negative value in terms of performance. The determination of the elements on the image was made with the simple neighborhood relationship method on the x and y axis on a pixel basis. Instead, deeper graph-theory-based algorithms such as global nearest neighbor (GNN), connected-component labeling (CCL) and connected-component analysis (CCA) can be used. However, the disadvantage of these algorithms is that they consume a lot of resources. A number of studies have been made on

the resource consumption of CCL algorithms. Halıcı and Demirhan [36] worked on multi-person real-time pose tracking with the global nearest neighbor method. Bataineh [24] examined the performance results were shared the resource needs of CCL algorithms. Without regard to, considering the resource capacity of mobile devices, these algorithms were not preferred in our study.

In our study, the detection of the hologram was made by considering the number of pixels. Considering the risk perception of the process, methods for determining the similarity of the hologram to the original shape can be used instead of the number of pieces. Despite, since these Image-recognition-based methods still use CCL algorithms, they are not included in our study. On the other hand, pre-control with real-time quantity ratio in the mobile layer and then using image-recognition methods in the back-end system with stronger resources can be an alternative method. The issue to be considered in such a hybrid structure is that the back-end controls are asynchronous and do not adversely affect the user experience.

193 national governments, including Turkey, use the ICAO Doc 9303 standard in the design of their identity cards and passports This study we have done covers only their TR identities. In spite of using machine learning methods, work can be done to determine the identity and passports of all these countries. Hartl et al. [23] used methods that detect the position and size of holograms on valuable papers in real time. This study, which we have done, can be extended for all valuable papers using the ICAO Doc 9303 standard by using similar methods. Another issue to consider is the need to minimize the processing time and resources consumed for detection. For this, issues such as using parallel algorithms and optimizing video resolution should be examined separately. Depending on the criticality of the process to be used in such a study; Dimensions such as resource, speed, performance, quality and reliability should be evaluated together. Foreground and background noise pixels have a significant impact on the quality of success in detecting and tracking objects from video. In investigating this effect, edge detection and contour evolution methods can be worked on. The use of the contour method contributes positively to the determination of the optimal contour area and the separation of the background and foreground of the image [37, 38].

6. CONCLUSION

This study has been conducted to develop a computer-aided process for remote identification is more reliable and faster of. For this purpose, the hologram element, which is difficult to imitate and detect, is preferred among the security elements on the TR ID card. Because of the difficulties of the detection of hologram, first of all crescent element on the ID cart detected. For this, the radius and center point of this crescent was detected. An application has been developed on the MATLAB program for computer aided tests. In the tests, threshold values have been assigned to control points to manage the impact of environmental factors on the process. The hologram images on 227 IDs were labeled as clearly visible and invisible. The tests have been first performed on sequential image frames on a video recording taken later on each card separately. Then, naked eye controls have been performed on each identity card used in the test. There is approximately 99.56% similarity between computer aided testing and visual controls. The only result that differed between the two tests is found to be due to a flash fired during shooting. Such a successful detection will be sufficient to make decisions in remote acquisition processes. It will especially contribute to remote applications made via devices that do not support NFC. It can be used in areas such as banks, insurance, notary public, telecom, which need remote identification and have a high transaction volume.

In the study, time and resource performance are not taken into account. The study is conducted on the hologram data on the TR ID card. Researchers can use similar methods for detecting hologram-like elements in identity cards of other countries using the ICAO Doc 9303 standard and for accuracy testing of valuable papers such as passports. In addition, different studies can be conducted on the subjects that are assumed or ignored in this study. On the other hand, in this study; The ratio of the number of detected pixels of the hologram and the area covered by the original shape to each other was used as the threshold value in the detection. Rather than the ratio; a study of the similarity of the detected edges, will help carry the research to a further point.

DECLARATION OF ETHICAL STANDARDS

The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHORS' CONTRIBUTIONS

Ender ŞAHİNASLAN: Contributed to problem definition, study design, analysis, interpretation, writing, and editing.

Abdullah KÖKSAL: Analysis, coding, data, testing, findings and evaluation contributed to the fieldwork and writing.

Önder ŞAHİNASLAN: Contributed to the analysis, writing, content control, interpretation and execution of the results of the study.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Sahinaslan O., Sahinaslan E., "Cross-object information security: A study on new generation encryption", ***AIP Conference Proceedings***, 2086(030034), (2019).

[2] Sahinaslan O., Sahinaslan E., Gunes E., "Review of the contributions of contactless payment technologies in the

COVID-19 pandemic process", ***AIP Conference Proceedings***, 2334(070002),(2019).

[3] Hacıoğlu A.B., Sağlam M., "Covid-19 Pandemi sürecinde tüketici davranışları E-ticaretteki değişimler", ***Medya ve Kültürel Çalışmalar Dergisi,*** 16-29, (2021).

[4] Sneader K., Singhal S., Kendi C., "The next normal arrives: Trends that will define 2021 and beyond", **McKinsey & Company**, (2021).

[5] Koç E., Özçelik H., "Covid-19 Yönetici ve Kobi Anketleri", ***EY-Parthenon Press*** (in Turkish), (2020).

[6] Deloitte Digital, "Euromonitor international retailing in world", ***Deloitte analysis***, (2021).

[7] Remes J., Manyika J., Smit S., Kohli S., Fabius V., Dixon-Fyle S., "The consumer demand recovery and lasting effects of Covid-19", ***McKinsey & Company***, (2021).

[8] https://home.kpmg/tr/tr/home/gorusler/2021/11/e-ticaretin-yukselisi.html

[9] https://resmigazete.gov.tr/eskiler/2021/04/20210401-7.htm

[10] https://www.tbb.org.tr/content/upload/istatistikiraporlar/ekler/3768/uzaktan_ve_subeden_musteri_edinimi_istatistikleri-Subat_2022.pdf

[11] Andrulevičius M., Tamulevičius T. and Tamulevičius, S., "Formation and Analysis of Dot-matrix Holograms", ***Material Science***, 13(4), (2007).

[12] https://www.nvi.gov.tr/tc-kimlik-karti

[13] Çetiner H., Cetişli B., "Real time recognition of identification cards of Turkish Republic with wavelet transforms", ***21st Signal Processing and Communications Applications Conference (SIU)***, 1-4, (2013).

[14] Yücel M., "T.C. Kimlik kartı yönetim ve dağıtım sistemi", ***UEKAE Dergisi***, 2(4): 35-41, (2010).

[15] Vaudenay S., Vuagnoux M., "About machine-readable travel documents", ***Journal of Physics: Conference Series***, Volume 77, Conf. Ser. 77 012006, Centre des Congrès, Saint Etienne, France (2007).

[16] Yoldaş, R., "Adaptation/ integration of new tckk and ekds environments in payment recorder device environments", ***MasterThesis***, Marmara University, Engineering Sciences, (2018).

[17] Mutlugün M., Adalier O., "Turkish national electronic identity card", ***In Proceedings of the 2nd international conference on Security of information and networks (SIN '09)***. Association for Computing Machinery, 14–18, (2009).

[18] Rusli, F.M., Adhiguna K.A., Irawan H., "Indonesian ID card extractor using optical character recognition and natural language post-processing 2021", ***9th International Conference on Information and Communication Technology (ICoICT)***, 621-626, (2021).

[19] Abed D.M., Jaber A.M., Rodhan A., "Improving Security of ID Card and Passport Using Cubic Spline Curve", ***Iraqi Journal of Science,*** 57(4A): 2529-2538, (2016).

[20] Król M, Kowalska D, Kościelniak P., "Examination of polish identity documents by laser-induced breakdown spectroscopy", ***Analytical Letters***, 51(10):1592-1604, (2018).

[21] Haga K., Kawano K., Hayashi K., Yoshizawa H., Minabe J., "Secure card with optically recordable hologram". ***IEEE LEOS Annual Meeting Conference Proceedings***, 489-490, (2005).

[22] Mahmoud M.K., "The latest security techniques used in passport design", ***Journal of Architecture, Art & Humanistic Science***,(2019).

[23] Hartl A., Arth C., Schmalstieg D., "AR-based hologram detection on security documents using a mobile phone", ***Lecture Notes in Computer Science***, vol:8888, Springer, (2014).

[24] Bataineh B., "A fast and memory-efficient two-pass connected-component labeling algorithm for binary images", ***Turkish Journal of Electrical Engineering & Computer Sciences***, 27:1243-1259,(2019).

[25] Zaitsev D.A., "A generalized neighborhood for cellular automata", ***Theoretical Computer Science***, 666:21-35, (2017).

[26] Lee D., Lim S., "Improved structural similarity metric for the visible quality measurement of images", ***J Electron Imag***, 25(6)063015, 10.1117/1.JEI.25.6.063015, (2016).

[27] Sahinaslan E., "On the internet of things: Security, threat and control", ***AIP Conference Proceedings***, 2086(030035), (2019).

[28] Korkmaz Ş., Alkan M., "Derin Öğrenme Algoritmalarını Kullanarak Deepfake Video Tespiti", ***Politeknik Dergisi***, 1-1, (2022).

[29] Karahan Ç. and Tüfekci A., "Blokzincir Teknolojisinin Dijital Kimlik Yönetiminde Kullanımı: Bir Sistematik Haritalama Çalışması", ***Politeknik Dergisi***, 23:483-496, (2020).

[30] Ateş, İ., Bilgin, T.T., "The Investigation of the Success of Different Machine Learning Methods in Breast Cancer Diagnosis", ***Konuralp Medical Journal***, 13:347-356, (2021).

[31] Jain R., Kasturi R. and Schunck B.G., "Edge Detection, Machine Vision", ***McGraw-Hill***, (1995).

[32] Caselles V., Kimmel R., and Sapiro G., "Geodesic active contours", ***International Journal of Computer Vision***, 22(1):61-79, (1997).

[33] Sun R., Lei T., Chen Q., Wang Z., Du X., Zhao W. and Nandi A., "Survey of Image Edge Detection", ***Frontiers in Signal Processing,*** 2(826967),(2022).

[34] Johnson R. A., "Modern geometry: an elementary treatise on the geometry of the triangle and the circle", Houghton Mifflin Co, p. 189, Republished by ***Dover Publications as Advanced Euclidean Geometry***, (2007).

[35] Buchholz R.H. and MacDougall J.A., "Cyclic polygons with rational sides and area", ***Journal of Number Theory,*** 128:17–48,(2008).

[36] Halıcı A.S. and Demirhan A., "Kalman filtresi ve küresel en yakın komşu yöntemi ile çok kişili gerçek zamanlı poz takibi", ***Politeknik Dergisi***, 1-1, (2022).

[37] Karasulu B., "Süperpiksel küme bölgeleri tabanlı aktif çevrit ve grabcut sinerjisini kullanarak insan kulağının otomatik bölütlenmesi", ***Acta Infologica*** 5:117-128, (2021).

[38] Karasulu B., "Videolardaki haraketli nesnelerin tespit ve takibi için uyarlanabilir arkaplan çıkarımı yaklaşımı tabanlı bir sistem", ***Uludağ Üniversitesi Mühendislik Fakültesi Dergisi,*** 18:93-110, (2013).