



e-ISSN: 2319-8753 | p-ISSN: 2320-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 11, November 2020

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.512

 9940 572 462

 6381 907 438

 ijirset@gmail.com

 www.ijirset.com

A Study on Biometrics and How it Pertains Security

Aishwarya Chaudhari¹

IT Student, Department of Information Technology, B. K. Birla College of Arts, Science and Commerce
(Autonomous), Kalyan, Maharashtra, India¹

ABSTRACT: Information security has become an indivisible a neighborhood of the emerging Information and Communication Technology [ICT]. In particular, authentication plays a particularly important role in handling security. The basis of biometrics is that an individual is recognizable by a few characteristics and physiological parameters. To determine the identity of any particular individual, most of the systems require personal recognition schemes which are distinctive and equally reliable. This assures the authentication of the people seeking their services. This ensures that illegitimate users cannot access the services and not anyone else. Currently, biometrics is very much used for authentication and identification of an individual. The biometric systems itself must be more secured and reliable so it can provide secure authentication in various applications. To optimize the safety, it's vital that biometric identification frameworks are intended to face up to various sources of attack. In security sensitive applications, there's a shrewd adversary component which intends to deceive the detection system. The aim of this paper is to demonstrate attacks and theft to various biometric security systems and how to increase the security by these systems for cloud data, banks, airports and various organizations. A review on the biometric identification techniques and few future possibilities within the fields of data security is presented during this work. Using biometric identification theory, it are often presented that how biometric systems are the boundless computational resources and prospective of flexibility, reliability and price reduction along side high-security performance resources. So this paper focuses on human characteristics based security system which can't be pinched easily like iris, thumb, palm, DNA and voice-based authentication system.

KEYWORDS: Biometrics, Authentication, Multi-modal biometrics, Fingerprint authentication, Iris recognition, Biometrics security, Face spoofing attacks.

I. INTRODUCTION

A biometric system is the system which are basically pattern recognition systems which works by collecting the biometric data from an user, such as fingerprint, iris, palm pattern, face details, voice, etc which is extracted from the collected data, and then compare the extracted set of data with the data which is saved in database. Biometric system is usually used to measure individual's unique behavior or physical characteristics to recognize or authenticate their identity. As growth in use of internet, identity verification becomes important in web-based applications, such as online banking and online shopping. Traditionally, passwords, identity cards and pin numbers are used for the verification of an individual. They have several disadvantages as a pin number can be shared by many people and an identity card can be stolen by someone. Also attackers can get access to a system by guessing passwords and pin numbers. In order to beat various issues in traditional methods, human biological characteristics are wont to develop biometric based verification systems. The main advantage of using biometric system in identity systems is that they cannot be easily shared or stolen. In a way, biometric schemes are easier to use, as users do not need to remember passwords, pin numbers or carry their identification cards. In biometric system there are two modes the verification modes and the identification modes. In verification modes, biometric system already have user template stored in database, while validating the user, the system compares the collected data from the user with the data stored in database, and if they match, then the user is valid user, else not. Another method is identification method during which the system recognizes the user by comparing its data with all the saved templates within the database, that is, one-to-many comparisons take place for establishing an individual identity. Since biometric-based authentication has many advantages over traditional methods, so there is significant rise in the use of biometric systems in recent years. Such systems can risk the privacy of people if they're not designed appropriately. For example, a biometric system may store fingerprints or iris data, if this biometric data get exposed to an attacker, then the attackers can use this biometric data for undesired purposes such as impersonation. Since biometric data is derived from unique characteristics of an individual so it cannot be altered. That's why leakage of biometric data can cause serious and continuous threats to

privacy of individuals. So it is very important that a biometric system must be designed in such a way that it can tolerate attack when used in security critical applications. Biometric systems should also overcome various face spoofing attacks, as the face spoofing attacks are increasing in biometric systems. The goal of this paper is to study various basic types of attacks that can occur on biometric system and how various measures can be taken for protection against attacks on biometric security systems.

The remaining paper is organized as follows: section II covers the main objectives of this study, section III consists of related biometric security system works, section IV, V include the methodology and analysis and finally section VI concludes the study along with future scope.

II. RELATED WORK

Previous related works under the biometric security field is as follows: In [1] Datta P et. al. proposed a survey in which security and privacy issues on the biometric system were discussed, the varied case studies like E-passport and Aadhaar identification, followed by threats and issues. Several multi-modal biometric identification system have been proposed in the last decade, in [2] Aleem et. al. proposed how biometric identification is the key factor responsible for the provision of cyber-physical system. As the unimodal biometric systems do not have the potential to provide required level of security to cyber-physical systems and also they are affected by a variety of issues like noisy data, non-universality, etc. So to overcome this issues and to provide high level security, the combination of different biometric modalities is required, that is a secure cyber-physical system, a novel multi-modal biometric system based on face and fingerprint. Fingerprint matching was performed with the help of alignment based elastic algorithm. Also for improved facial feature extraction, Extended local binary patterns (ELBP) are used. Most recently, L. Ghammam et. al. [3] proposed cancelable biometric schemes because it provides secure biometric templates done by combining user specific tokens and biometric data in which he cryptanalyzed two recent cancelable biometric schemes, which were supported by particular locality sensitive hashing function, index-of-max (IoM): Gaussian Random Projection-IoM (GRP-IoM) and uniformly random permutation-IoM (URP-IoM). Kaushal Kumar et. al. [5] proposed different types of biometrics like fingerprint, ear, iris, vascular, retina, DNA, palm, hand geometry, voice recognition and many, and how it is used for unique identification of a human it also proposed that biometric is more secure and easy process for verification and identification. It is used to decrease crime and terrorism. It is also used by airport authority, police verification, military intelligence, and many other secrete services. Few cancelable biometric based security protocols have also been proposed, Joshua J. Tom et. al. [9] proposed a cancelable biometric based authentication protocol which guaranteed secure mutual authentication with customer privacy and also offers a secure end-to-end transmission of customer transaction data. There are numerous approaches focusing on face spoofing attacks, in [13] R. H. Vareto et. al. proposed face spoofing attacks made by an intruder to impersonate someone. These attacks are increasing as the use biometric authentication on mobile devices, high-security areas are increasing. There is lot of anti-spoofing work in the literature, Z. Zhang et. al. [14] proposed a face anti-spoofing database which covers a diverse range of potential attack variations, a database which contains 50 genuine subjects, and the fake faces are produced from high quality records of the genuine faces. In [15] C. Rathgeb et. al. proposed the vulnerability of a widely used open source face recognition system that's ArcFace, to makeup presentation attacks using the publicly available Makeup Induced Face spoofing (MIFS) and FRGCv2 databases, in which a makeup attack detection scheme was used to compare face depth data with face depth reconstructions obtained from RGB images of potential makeup presentation attacks.

III. METHODOLOGY

We have tested and validated our methodology with various documents from data center located everywhere, during this section, we present the conclusion from existing data centers, they being advertised for their energy efficiency performance. All data were collected from publicly available information.

IV. ANALYSIS

1 Objectives of attacks on a biometric system

A security system, whether it uses biometric information or not, can be subjected to a series of attacks. In this section we will describe the main types without taking into account either the architecture of the system or its technical details. We work on different types of attack on biometric systems, however, due to the generality of these, they have a lot in common with typical attacks on security systems.

1.1 Spoofing attacks

This type of attack is aimed toward gaining illegal access to a resource. It consists in impersonating a user with access to the desired resource. There are several variants of the attack depending on the point of the architecture that the attack

is directed at. Leaving aside the traditional attacks on computer systems and focusing specifically on biometric systems, the most common way to carry out this attack is with synthetic copies of biometric data of the target user. There are many mechanisms that can be used to obtain synthetic copies of the data. In general, the attacker's main goal is aimed toward two details. The first is to realize access to the user's biometric data and therefore the second is to form an artificial copy of the info obtained. Due to the widespread use of biometric identification systems, it's not difficult to seek out related news items. An example can be found in a car thief who cut off the finger of the car owner in order to start his car, protected with a security system based on fingerprints. In this scenario the attacker was able to start the car the first time with the owner's lifeless fingerprint. However, later an equivalent fingerprint could not be used to start the car because the car had protection systems against dead samples.

1.2 Biometric obfuscation

Most attacks on biometric systems are aimed toward impersonating a private so as to realize access to a protected resource. However, there are other sorts of attacks that require to be considered. In this situation, the biometric obfuscation is aimed at falsifying or masking the biometric data, before or after the acquisition of these by the system, in order to prevent the system from recognizing an individual. The following effects of an obfuscation attack can be as or more serious than those of a spoofing attack; therefore, these attacks should not be dismissed in the protection of systems. It should be noted that most people who carry out this type of attack are usually on checklists and most are wanted by law enforcement. Therefore, these people usually have strong reasons for modifying their biometric data. To know the severity of the attack we can consider biometric systems located on the borders between countries. In this case an individual wishing to enter the country is required to enter biometric data (usually fingerprints or facial data) in order to ensure that the individual has not committed crimes within the country or the police are not looking for them. There are several ways to perform this attack consistent with the methodology applied. There are two main methods. The very first one is that the physical alteration of one's own biometric data either by deterioration or by surgery. The second way is to use spoofing techniques to impersonate a private and obscure one's own identity. This second method also includes the use of synthetic data in order to obscure identity.

1.3 Denial of Service attacks

The goal of this attack is to slow down, stop or degrade the quality of the system. A system affected by this type of attack prevents legitimate users from using it in a normal way. This system malfunction can be used by the attacker with two clearly differentiated purposes. The first is aimed toward completing a secondary spoofing or obfuscation attack. The second, is of a more generic nature, and may be aimed at carrying out a secondary attack of extortion or possibly for political purposes. An easy methodology for performing such kind of type of attack is to insert large amounts of data with a lot of noise, which would lower the acceptance threshold and consequently increase the rate of accepted fakes. In this scenario the secondary attack should correspond to an impersonation attack, as non-licit biometric samples could be accepted as licit by the system. The denial of service attack can go beyond a slight degradation of the system and stop its operation, administrative staff would be forced to replace biometric systems with more traditional measures, such as a security guard. It is clear, that these traditional systems are more easily fooled than a biometric system. A good example would be a scenario where a secondary obfuscation attack is desired. If the attacker wants to access a resource protected by a fingerprint recognition system and supported by face recognition. In this scenario it'd be difficult to fool a well-calibrated automatic system, but not so difficult to fool a watchman.

1.4 Conspiracy and Coercion

The main difference between these attacks and the previous ones is that these types of attacks are carried out by legitimate users of the system. Like in conspiracy attacks, the user, possibly due to bribery, facilitates access to the system. Then in coercive attacks the victim is possibly under threat or blackmail, facilitates access to the system. These attacks evade the security system because the data is true. This type of attack can vary in severity depending on the user being attacked. It should be noted that it's not an equivalent to attack an administrator because it is to attack an unprivileged user.

2 Specific defences to improve security in biometric systems

There are a various number of measures for preventing the attacks discussed above. As a general methodology, a security system should never focus on a single security method but rather should apply the method in combination with other secondary or complementary methods.

2.1 Authentication by combining random data and multiple biometrics

The main idea of the mechanism is predicated on the user having different biometric features which will be requested randomly or sequentially counting on the implementation of the system. The increase in security is due to the fact that

the potential attacker must be able to correctly reproduce all possible data that can be requested from the user. If randomness is introduced in the process, then the attack is further complicated as it is not possible to know either the sequence or the amount of data that will be requested. A simple example of an implementation of this in a fingerprint system would be the verification of the fingerprints of several fingers at random. The potential attacker may have the copy of all fingerprints. In this case, moreover, it becomes impossible to attack by means of residues on the info capture device because the fingerprints of the varied fingers will overlap. Another possible example, of a more elaborate implementation, could be a speech recognition system in which the user is asked to repeat a random sequence of words. In this case the attacker must have an outsized number of recorded words so as to be ready to reproduce any requested combination.

2.2 Data retention

A major source of data that would be used for an attack is that the temporary information employed by biometric systems. Considering the system at a technical level it must be kept in mind that both in the extraction of the features and in the identification system it is necessary to store certain temporary information to perform the operations of the system. This temporary information if captured can give a lot of information to a possible attacker to carry out a great diversity of attacks. Therefore, to protect access to this information, severe measures must be taken to protect the system hardware from illicit access. Moreover, the system itself should not keep the temporary information longer than necessary. These mechanisms can be applied with a combination of low-level memory erasures on a regular basis. It should be noted that in order to store the history of authorized and unauthorized accesses by the biometric system, it is necessary to store historical data temporarily. Without considering that this data should be stored in a coded way in the system, the administrator must consider, through an analysis of each particular case, a good balance between security and usefulness of the stored information.

2.3 Life detection of the sample

The spoofing attack is one among the foremost typical attacks on a biometric system. Considering it the most common method used is a synthetic copy of biometric data of the person to be impersonated, one of the most used defences to prevent these types of attacks is life detection. It is usual to incorporate life detection mechanisms into the data capture device. It is also important to detect the life of the sample in obfuscation attacks, as the attacker may try not to be detected by the system by using synthetic samples belonging to other users. There are some ways to detect the lifetime of the sample. It depends largely on the biometric data used by the system. Here are some specific measures to detect the life of various types of biometric samples. For systems based on voice detection a method for detecting sample life may be to measure the air expelled in speech. This pattern provides a lot of information about the person as well as making it more difficult to violate the system through recorded copies of the original voice. Whereas in fingerprint-based systems, easy-to-detect measures such as temperature, oximetry, skin conductivity, detection of capillaries under the epidermis, or pulse, can give a lot of information about the life of the sample. In other systems, face recognition might be combined with a mixture of spectroscopic or thermal images. Finally, it's worth commenting on the case of biometric systems supported iris recognition.

2.4 Multi-factor authentication

Multi-factor authentication could be considered a generalization of multiple biometrics in which the system requires several mechanisms, not necessarily biometric mechanisms, to validate an individual. These mechanisms could be physical mechanisms, such as SmartCards, DONGLE1 or any other type of token, or mechanism, such as access keys. In a way, such type of mechanism helps to increase security, as in the case of multiple biometrics, because there are various elements that must be copied in order to carry out the spoofing attack. The possible disadvantages of using multi-factor authentication are due to an increase in validation time; therefore, those responsible for the design of the system need to find a balance between security and usability.

2.5 Cryptography and digital signature

Both cryptosystems and digital signatures are often used on many levels during a complex system like a biometric system. In this case, given the generality of the mechanism, we only focus on the protection of the data circulating through the communication mechanisms between the various machines that make up the system. The encryption and coding of data circulating in the network allows the system to protect itself from attacks produced by reading/writing data packets circulating in the system's communication network. The main purpose of encryption is to prevent any potential attacker from analysing the information circulating through the communication channel. Whereas the digital signature aims to verify the sender of the information, in this case preventing man-in-the-middle1 type attacks.

2.6 Security agents and control personnel

Today's technological systems still lack certain qualities or functionalities that a person can perform with extreme ease. In this case, many of the protection mechanisms discussed throughout this chapter can be performed by a security agent in a more efficient and cost-effective way than an automated system. The main security measure, and one that greatly helps to stop a breach of the system, is life detection of biometric data. So in a biometrics based security system, it is very important to combine automatic methods, for the search and detection of biometric data, with security personnel in order to verify the samples. To illustrate this fact it is only necessary to consider that for any person it is very easy to identify whether a sample is a simple photocopy or the actual face of a person. Another security mechanism that an agent can provide in order to increase a system's security is the identification of coercive attacks, where a lawful user of the system is required to enter their biometric data into the system in order to give access to an unauthorized user.

2.7 Security through obscurity

Security through obscurity is a mechanism for providing security in a system and is based on not disclosing details of its design and implementation. It should be noted that a system based on this type of security usually has known vulnerabilities, but because its architecture and implementation are unknown, these weaknesses cannot be exploited. This protection system is typically an honest complementary measure of protection.

2.8 Standards

As in most work systems or organizations, there are a series of standards that provide safety and efficiency in the system. In this scenario, leaving aside other standards applicable to organizations, such as ISO 9001, there are a number of standards related to the proper functioning and security of computer systems. Other standards related to biometric systems are: ANSI / INCITS 358, for the standardization of the interoperability of biometric systems; NISTIR 6529, which specifies the format of the data in the output interfaces of biometric systems; ISO/IEC 19794-2: 2005, which specifies the data format in fingerprint-based systems; and INCITS 378-2009, also aimed at standardizing the exchange of data in fingerprint-based systems. Both sides of interoperability standards must be considered. On the one hand, the standards improve the system's security because they have been designed by a team of specialists and, therefore, many of the weaknesses related to security have been eliminated. On the other hand, a system that meets the interoperability standard facilitates access to data as both the data format and the means of transmitting data are known.

V. CONCLUSION

In this paper an analysis on currently available and emerging biometric security systems was carried out. The different types of attacks and various measures to improve security in biometric system were discussed. A nice property of biometric security systems is that security level is nearly equal for all users during a system. This is not true for other security technologies. For example, in an access control based on password, a hacker just needs to break only one password among those of all employees to gain access. In this case, a weak password risks the overall security of every system that user has access to. Although biometrics offers an honest set of benefits, it's not been massively adopted yet. Its main drawback is that biometric data is not secret and cannot be replaced after being compromised by a third party. For applications with a person's supervisor (such as border entrance control), this will be a minor problem, because the operator can check if the presented biometric trait is original or fake. However, for remote applications like internet, some quite liveliness detection and anti-replay attack mechanisms should be provided. This is an emerging research topic. As a general rule, concerning security matters, a continuing update is important so as to stay on being protected. A suitable system for this time can become obsolete if it's not periodically improved. For this reason, nobody can claim that features a perfect security system, and even less that it'll last forever.

VI. ACKNOWLEDGEMENT

I would like to thank Prof. Swapna Augustine Nikale, Department of Information Technology, B.K Birla College Kalyan for providing guidance for this research work.

REFERENCES

- [1]. Datta P., Bhardwaj S., Panda S.N., Tanwar S., Badotra S. (2020) Survey of Security and Privacy Issues on Biometric System. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham.
- [2]. Aleem, S., Yang, P., Masood, S. *et al.* An accurate multi-modal biometric identification system for person identification via fusion of face and finger print. *World Wide Web* **23**, 1299–1317 (2020).

- [3]. L. Ghammam, K. Karabina, P. Lacharme and K. Thiry-Atighehchi, "A Cryptanalysis of Two Cancelable Biometric Schemes Based on Index-of-Max Hashing," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2869-2880, 2020.
- [4]. L. Ghammam, K. Karabina, P. Lacharme and K. Thiry-Atighehchi, "A Cryptanalysis of Two Cancelable Biometric Schemes Based on Index-of-Max Hashing," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2869-2880, 2020.
- [5]. Kaushal Kumar, Harshit Kumar, Piyush Singh, Amit Kumar, KM Shikha, Kaushal Kumar, Harshit Kumar, Piyush Singh, Amit Kumar, KM Shikha. "Biometric Security System for Identification and Verification." *International Journal of Scientific Research in Computer Science and Engineering*, vol. Vol.8, no. ssue.1, Feb. 2020, pp. 16–19. *E-ISSN*.
- [6]. Dr. S. Britto Ramesh Kumar Asst. Prof., Dept. of Comp. Science. "Biometric Security for Cloud Data Using Fingerprint." *Head, Dept. of Comp. Science Soka Ikeda College of Arts and Science for Women, Chennai*, vol. Volume IX I, no. Issue II, Feb. 2020, pp. 58–67. *ISSN, nce and Engineering*, vol. Vol.8, no. ssue.1, Feb. 2020, pp. 16–19. *E-ISSN*.
- [7]. ManoliuMitica-Valentin, Travediu Ana-Mariaand Racuciu Ciprian, "Biometric security: Recognition according to the palm veins." *Scientific Bulletin of NavalAcademy*, Vol. XXIII2020, pg.257-262.
- [8]. Gupta, Ankur and Kaushik, Dushyant and Gupta, Swati, Integration of Biometric Security System to Improve the Protection of Digital Wallet (May 7, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020.
- [9]. Joshua J. Tom, Boniface K. Alese, Aderonke F. Thompson. "A Cancelable Biometric Based Security Protocol for Online Banking System." *International Journal of Computer Science and Information Security (IJCSIS)*, vol. Vol. 18No. 6, no. june 2020, June 2020, pp. 21–35. *IJCSIS*.
- [10]. A. Dhoot, A. N. Nazarov and A. N. A. Koupaei, "A Security Risk Model for Online Banking System," 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2020, pp.
- [11]. Jindal, udit and Kaur, Harshdeep and das, subarna, Literature Review on Security Issues and Limitations in Biometric Applications (April 1, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020.
- [12]. Z. Ishak, N. Rajendran, O. I. Al-Sanjary and N. A. Mat Razali, "Secure Biometric Lock System for Files and Applications: A Review," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2020, pp. 23-28.
- [13]. R. H. Vareto, A. Marcia Saldanha and W. R. Schwartz, "The Swax Benchmark: Attacking Biometric Systems with Wax Figures," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020, pp. 986-990.
- [14]. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi and S. Z. Li, "A face anti-spoofing database with diverse attacks," 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, 2012, pp. 26-31, doi: 10.1109/ICB.2012.6199754.
- [15]. K. Pňihodová and M. Hub, "Biometric Privacy through Hand Geometry- A Survey," 2019 International Conference on Information and Digital Technologies (IDT), Zilina, Slovakia, 2019, pp. 395-401, doi: 10.1109/DT.2019.8813660.
- [16]. C. Rathgeb, P. Drozdowski, D. Fischer and C. Busch, "Vulnerability Assessment and Detection of Makeup Presentation Attacks," 2020 8th International Workshop on Biometrics and Forensics (IWBF), Porto, Portugal, 2020, pp. 1-6, doi: 10.1109/IWBF49977.2020.9107961.
- [17].M. Faundez-Zanuy, "Biometric security technology," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 21, no. 6, pp. 15-26, June 2006, doi: 10.1109/MAES.2006.1662038.
- [18].G. Heusch, A. George, D. Geissbühler, Z. Mostaani and S. Marcel, "Deep Models and Shortwave Infrared Information to Detect Face Presentation Attacks," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 4, pp. 399-409, Oct. 2020, doi: 10.1109/TBIOM.2020.3010312.
- [19].Fourati, E., Elloumi, W. & Chetouani, A. Anti-spoofing in face recognition-based biometric authentication using Image Quality Assessment. *Multimed Tools Appl* **79**, 865–889 (2020).
- [20].S. Fatemifar, M. Awais, A. Akbari and J. Kittler, "A Stacking Ensemble for Anomaly Based Client-Specific Face Spoofing Detection," 2020 IEEE International Conference on Image Processing (ICIP), Abu Dhabi, United Arab Emirates, 2020, pp. 1371-1375, doi: 10.1109/ICIP40778.2020.9190814.
- [21].Koppikar U., Sujatha C., Patil P., Hiremath P.S. (2021) Face Liveness Detection to Overcome Spoofing Attacks in Face Recognition System. In: Sharma M.K., Dhaka V.S., Perumal T., Dey N., Tavares J.M.R.S. (eds) Innovations in Computational Intelligence and Computer Vision. Advances in Intelligent Systems and Computing, vol 1189. Springer, Singapore.
- [22]. Bakshi, A., Gupta, S. An efficient face anti-spoofing and detection model using image quality assessment parameters. *Multimed Tools Appl* (2020). <https://doi.org/10.1007/s11042-020-10045-x>



- [23].Rosmansyah, Y., Hendarto, I. & Pratama, D. (2020). Impersonation Attack-Defense Tree. *International Journal of Emerging Technologies in Learning (iJET)*, 15(19), 239-246. Kassel, Germany: International Journal of Emerging Technology in Learning. Retrieved November 21, 2020 from <https://www.learntechlib.org/p/217913/>.
- [23].Syed Muhammad Saad, Abdullah Bilal, Sara Tehsin, Saad Rehman, "Spoof detection for fake biometric images using feature-based techniques," Proc. SPIE 11525, SPIE Future Sensing Technologies, 115251N (8 November 2020).
- [24].L. Etienne and H. Shahriar, "Attacks and Mitigation Techniques for Iris-Based Authentication Systems," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 1101-1102, doi: 10.1109/COMPSAC48688.2020.0-120.



INNO SPACE
SJIF Scientific Journal Impact Factor

**Impact Factor:
7.512**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details