ISSN 2278-3091
Volume 10, No.1, January - February 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse461012021.pdf
https://doi.org/10.30534/ijatcse/2021/461012021

Description of Research Design using Articles for Biometrics Technology Security and Countermeasures

Irfan Iqbal
Department of Natural and Applied Sciences, Buraydah Community College, Qassim University, Saudi Arabia
e.eqbal@qu.edu.sa

ABSTRACT

In this paper, we search different articles and journals by using different scientific databases (Elsevier, Emerald, IEEE, Springer and ACM). The selection of relevant articles and journals is made through proper study of the relevant material's abstract, conclusion with respect to our problem domain. After that, selected articles/papers are motivated by various arguments that depend upon the investigated area and develop motivation for the results.

Key words: Biometrics Technology, Authentication system, Research design, Article selection, Biometrics Security & Privacy

1. INTRODUCTION

Biometrics measure individual's unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry, retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component).
Most commonly, security field uses three different types of authentication:

Something you know: Password, PIN, etc Something you have: card key, smart card, etc Something you are—a Biometric
A biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible.

In this paper, our focus was on "Biometric Technology Security concerns and its countermeasures". The division of the title is made by observing its depth and wideness. So the

1st Division: covers the Biometric Security concerns like factors influencing the adoption of Biometric security technologies by decision making when trying to adopt biometric security technology solutions.

2nd Division: Covers the Biometric Security Attacks and its countermeasures. In other words, analyzing biometric authentication's weakness to various spoofing attacks, and efforts to defeat the spoofing attack are presented.
Both of the division are being treated parallel to make sure of the search process. Firstly, we designed research questions and after that keywords are derived by conducting a search on different scientific databases. The exact selection of relevant articles/papers is made through its inclusion and exclusion criteria.

2. STRATEGY

Before defining the strategy of finding the articles/papers that mostly related to our research area, firstly we formulate the questions that does relate to our research area. ***Final Stage***

2.1 Research Questions

RQ1: What are the different attacks related to biometrics authentication system?
RQ2: What are the different spoofing methodologies?
RQ3: What steps are useful against the spoofing techniques?
RQ4: Factors influencing the adaptation of Biometrics Security technologies
RQ 5: Evaluating the biometrics system.

2.2 Search Process

Based upon the above research questions, we derived some initial keywords. These initial keywords help to further derive some new alternative keywords by using the search Engines as described in Table 1.

Table 1: Search hits on different databases for research questions

Main Keywords	Biometrics, Biometrics Security Concerns, Biometrics privacy concerns, Biometrics Security Evaluation, Biometrics Security Evolution, Biometrics security Adoption, biometrics Security solutions, biometrics security issues, multimodal biometrics
Alternative Keywords	Biometrics Security technology, Biometrics security, Biometrics authentication, Biometrics Security system acceptability, Biometrics public awareness, biometrics issues, biometrics attacks, spoofing attack, anti-spoofing attacks
Different Publishers/ Organization	Elsevier, Science Direct, Emerald, Springer, Ei Village, ACM, Google Scholar

Before deciding either we will include or exclude relevant papers we always go through the contents of the papers/articles like abstract and conclusion and do the little bit skimming. We have defined the criteria of including and excluding article on the following ways.

*We consider only those papers/articles that discuss our research area in detail.

*We consider the papers which published between 2000 and 2020.

*We only consider the articles that are mostly related to biometrics security issues and threats and different anti spoofing attack and countermeasures against the attack.

*We exclude those papers which have no citation and also those who published in 2009 because of the immaturity.

*We try to consider those paper/article whose authors are actively involved or attached with particular area of research.

*We try to include those paper/articles that are reviewed by two or three authors.

During the selection of the papers/articles that are relevant to problem domain and very close to the investigated area. We analyze the creditability of the author with help of tool “Harzing’s Publish or Perish”[42].

3. STATE OF THE ART

Nowadays there is threat of international Terrorism, high level of security measures are enforced to make fool proof check on the people who crossing the borders. There are lots of techniques which can easily fool biometrics authentication system. But some smart and efficient work is still going on in the biometrics system. Like facial biometrics System capable of creating a facial 'DNA'[43].

4. HISTORICAL IMPORTANCE

Table 2 [44]: History of Biometrics Research

Year	Description
1858	First Systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1896	Henry develops a finger print classification system
1936	Concept of using the iris pattern for identification
1963	a research paper on finger print automation published
1965	Automated signature research begins
1969	FBI pushes to make finger print recognition an automated process
1974	First commercial hand geometry system become available
1986	Exchange Finger print data is published
1992	Biometric Consortium is Established within US Govt
1997	Generic biometric interpretability standard is published
1998	FBI launches DNA database
2002	ISO Standards Committee established on Biometrics
2004	Introduce personal identification card for all federal employees and contractors
2005	Iris on the Move is announced at Biometrics Consortium Conference
2008	U.S. Government begin coordinating biometric database use
2013	Apple includes fingerprint scanners into consumer-targed smartphones

5. CURRENTLY AT THE FOREFRONT OF THE RESEARCH AREA

Privacy and Personalization are the forefront issue in the society. As everyone consider biometrics technology as a safe tool of security. But there are several issues with Biometrics identification system. The first is unimodal

biometrics is fail to reach the performance level. Researcher have been the forefront of developing screen system and imaging system custom fit clothing using holographic radar imaging techniques. In this system radar signal are used which can easily penetrate into the body and reflect of the water in skin. This system implemented on the security check points.

6. FUTURE WORK AREAS

Biometrics system developers start working on multimodal biometrics authentication system, to provide a high level of security. Now a day Hitachi's progress toward the multimodal biometrics system named "Advance Digital Person Authentication System"[45]. Biometrics system developer further develops "3-D infrared facial recognition" and "Visitor management System" [46].

In future there are also some standard that are defined for the growth of biometric technology so this will guide the vendors and developers to develop the standard product [46].

7. RESEARCHER PIONEERS IN THE AREA

M.Trauring was the pioneer who publish very first research paper in this area in 1963 at "Hughes Research Laboratory".

8. RESEARCHER ACTIVE TODAY

Well number of researcher who currently working on the biometrics technology and there issues. In my research I found some of the researcher who is actively working in this field. Some of them Anil K Jain and David Zhang.

Anil K Jain is a university professor in the department of computer science at Michigan State University. He researched on pattern recognition, computer vision and biometric recognition. His articles or papers related to biometrics are published in Scientific American, Nature, IEEE Spectrum, Comm.ACM, IEEE Computer and MIT Technology Review [47].

David Zhang is the director of biometrics technology center supported in 1998. He is the founder and editor in chief of 'International Journal of Image and Graphics' and also book editor of 'Springer International Series on Biometrics'. He is the first organizer of 'International Conference on Biometrics Authentication'. He is the author of more than 10 books and 200 journals [48].

9. CONFERENCES AND JOURNALS WHERE YOUR ARTICLES HAVE BEEN PUBLISHED

Table 3: Conferences and Journal articles

Ref	Date	Article /Paper Type	Conference/Journal Name
[1]	2004	JA	Biometric Technology Today
[2]	2003	JA	IEEE Security and Privacy
[3]	2006	JA	Information Security Technical Report
[4]	2007	JA	Computers & Security
[5]	2002		Logistics Information Management
[6]	2004		An economics view of biometrics
[7]	2008	JA	Marketing
[8]	2006	JA	Sensor Review
[9]	2004	JA	Biometric Technology Today
[10]	1994	JA	Information Technology & people
[11]	1995	JA	Computers & Security
[12]	2003	JA	Computer Fraud & Security
[13]	2007	JA	Computer Fraud & Security
[14]	2009	JA	Journal on Multi model user interface
[15]	2005	CA	ITHET 6th International conference
[16]	2001	JA	Computer Law & Security Report
[17]	2008	JA	Computer Law & Security Report
[18]	2006	JA	Managing Service Quality
[19]	2009	JA	Management
[20]	2004	CA	Proc. International Conference on Pattern Recognition
[21]	2004	JA	Communications of the ACM
[22]	2006	JA	IEEE transactions on information forensics and security
[23]	2004	JA	Sensor Review
[24]	2005	JA	DOI=etdindividuals.dlib.vt. edu
[25]	2006	JA	DOI=drdavidlease. com
[26]	2001	JA	IT Professional
[27]	2009	JA	Computer Law and Security Review: The International Journal of Technology and Practice
[28]	2000	JA	Biometric Technology Today
[29]	2007	CA	SPIE - The International Society for Optical Engineering
[30]	2006	JA	IEEE internet computing
[31]	2009	JA	International Journal of Contemporary Hospitality Management
[32]	2000	JA	Computer
[33]	2005	JA	Information management and computer security

[34]	2003	JA	Pattern recognition letter
[35]	2004	CA	Citeseer
[36]	2008	JA	Kybernetes
[37]	2002	JA	Information security technical report
[38]	2008	JA	Information and management and computer security
[39]	2000	JA	Computer
[40]	1997	CA	Lecture note in computer science
[41]	2004	JA	Information management and computer security
[49]	2011	JA	Intention to Use Biometric Systems
[50]	2011	JA	Customers' Adoption of Biometric Systems in Restaurants: An Extension of the Technology Acceptance Model
[51]	2013	JA	Secure Biometrics: Concepts, Authentication Architectures, and Challenges
[52]	2017	JA	Evolution of Biotechnology and Information Technology and Its Impact on Human Security
[53]	2018	JA	BIOMETRIC TECHNOLOGY: SECURITY AND PRIVACY CONCERNS
[54]	2018	JA	Biometric template security: an overview
[55]	2020	JA	The latest evolution of biometrics
[56]	2020	JA	A review on performance,security and various biometric template protection schemes for biometric authentication systems
[57]	2020	JA	Addressing biometrics security and privacy related challenges in China

*JA: Journal Article
*CA: Conference Article

10. CONCLUSION

This paper describes the stages for selecting, searching and refining the valid material for the specified research area. It also helps for assessing the quality of the searched material. We adopted self-created search strategy such as (→Define Keyword→ Choose sources→ Search technique →Evaluate the search results →Document selection→ Reference Management →Formulate Information Problem^)

ACKNOWLEDGEMENT

The author would like to express his deep sense of gratitude to Professor Dr. Ali bin Ibrahim alahdam, and Professor Dr. Yasir bin Muhammad bin Saleh Alghafeeli who led all the research stages and provided insight and invaluable expertise that greatly assisted the research. My thanks are due to Dr. Awad bin Dhawi Al-Harbi for constant inspiration and valuable advices.

REFERENCES

[1] Ashbourn, J. 2004.Where we really are with biometrics. Biometric Technology Today 12, 4 (2004), 7-9. DOI=http://www.sciencedirect.com/science/article/B6W70 -4C1C7SW-H/2/38ffc75944909cfb490a7a4e9111a844

[2] Bernecker, O.2006. Biometrics security: An end user perspective. Information Security Technical Report 11, 3 (2006), 111-118. DOI= http://www.sciencedirect.com/science/article/B6VJC-4KPGS0Y-2/2/393610dc3668a241b2c8b32d5d7b4805

[3] Bolle, R.M., Connell, J.H., and Ratha, N.K.2002. Biometric perils and patches. Pattern Recognition 35, 12 (2002), 2727-2738. DOI=http://www.sciencedirect.com/science/article/B6V14-4502W33-1/2/11a1f87771b2e8ccd37420c32a9aa07a

[4] Roberts, C. 2007. Biometric attack vectors and defences. Computers & Security 26, 1 (2007), 14-25. DOI=http://www.sciencedirect.com/science/article/B6V8G -4MNYYTW-3/2/1ffddfaf7b1b87d854d5706d9e2ebf13

[5] Brooks, W.J., Warren, M.J., and Hutchinson, W.2002. A security evaluation criteria. Logistics Information Management 15, 5/6 (2002), 377-384. DOI=http://www.emeraldinsight.com/Insight/ViewContent Servlet?Filename=Published/EmeraldFullTextArticle/Artic les/0880150506.html

[6] Cave, J. 2005. An economics view of biometrics. Biometric Technology Today 13, 5 (2005), 8-11 DOI=http://www.sciencedirect.com/science/article/B6W70 -4GD43Y8-N/2/90b79d2dc8407822571dca3e47e9c545

[7] Chandra, A., Durand, R., and Weaver, S. 2008. The uses and potential of biometrics in health care. Marketing 2, 1 (2008), 22-34. DOI=http ://assets. emeraldinsight.com/Insight/ viewC ontent Item.do?contentType=Article&hdAction=lnkhtml &a mp;contentId= 1718605&history=false

[8] Connolly, C. 2006. Performance testing of commercial biometric systems. Sensor Review 26, 1 (2006), 33-37 DOI=http://www.emeraldinsight.com/Insight/ViewContent Servlet?Filename=Published/EmeraldFullTextArticle/Artic les/0870260105.html

[9] Coventry, L. 2004. Biometrics, self-service and the user. Biometric Technology Today 12, 10 (2004), 7-9. DOI=http://linkinghub.elsevier.com/retrieve/pii/S09694765 04002292

[10] Davies, S.G. 1994.Touching Big Brother. Information Technology & People 7, 4 (1994), 38-47.

[11] Deane, F., Barrelle, K., Henderson, R., and Mahar, D. 1995. Perceived acceptability of biometric security systems. Computers & Security 14, 3 (1995), 225-231.

DOI=http://www.sciencedirect.com/science/article/B6V8G
-3Y45THW-5Y/2/819d7b68cc954f0d0906686463e1a421

[12] Forte, D.2003. Biometrics: future abuses. Computer Fraud & Security 2003, 10 (2003), 12-14. DOI=http://www.sciencedirect.com/science/article/B6VN T-49V9RY2-8/2/2dec7ad4e4c40192db0210c2d08728b9

[13] Furnell, S. and Evangelatos, K. 2007. Public awareness and perceptions of biometrics. Computer Fraud & Security 2007, 1 (2007), 8-13.

DOI=http://www.sciencedirect.com/science/article/B6VNT -4MY2019-6/2/90f8b7fe0c3 5 5b10be523192e8e13134

[14] Goudelis, G., Tefas, A., and Pitas, I. Emerging biometric modalities: a survey. Journal on Multimodal User Interfaces, , 1 -19.DOI=http://www.springerlink.com/content/44m74418u58k

l895/fulltext.pdf

[15] Green, N. and Romney, G.W. 2005.Establishing public confidence in the security of fingerprint biometrics. Information Technology Based Higher Education and Training, 2005. ITHET 2005. 6th International Conference on, (2005), S3C.

DOI=http ://ieeexplore .ieee.org/stamp/stamp. jsp?arnumber= 1560332&isnumber=33131

[16] Grijpink, J. 2001. Privacy Law Biometrics and privacy. Computer Law & Security Report 17, 3 (2001), 154-160. DOI=http://www.sciencedirect.com/science/article/B6VB3 -43GH45H-4/2/a6c547b54ccf1537fc283a4868b3be82

[17] Grijpink, J.2008. Trend report on biometrics: Some new insights, experiences and developments. Computer Law & Security Report 24, 3 (2008).

[18] Heracleous, L. and Wirtz, J. Biometrics: the next frontier in service excellence, productivity and security in the service sector. Managing Service Quality 16, 1 (2006), 12.

[19] Jackson, L.A. 2009.Biometric technology: the future of identity assurance and authentication in the lodging industry. Management 21, 7 (2009), 892-905.

[20] Jain, A.K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., and Wayman, J.L.2004. Biometrics: a grand challenge. Proc. Interntaional Conference on Pattern Recognition, (2004), 935-942

[21] Jain, A.K. and Ross, A. 2004. Multibiometric systems. Communications of the ACM 47, 1 (2004), 40.

DOI= http://doi.acm.org/10.1145/962081.962102

[22] Jain, A.K., Ross, A., Pankanti, S., and others. 2006.Biometrics: a tool for information security. IEEE transactions on information forensics and security 1, 2 (2006), 125-143.

[23] Kochan, A.2004. Breakthrough in Biometrics. Sensor Review 24, 2 (2004), 125-128.

[24] Lease, D.R.2005. Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information Technology and Security Managers. (2005).

[25] Lease, D.R. 2007.Enhancing Security in the Private Sector with Biometric Technologies: Problems and Prospects. October 5, (2006), 2007.

[26] Liu, S. and Silverman, M. 2001. A practical guide to biometric security technology. IT Professional 3, 1 (2001), 27-32.

[27] Liu, Y. 2009 The principle of proportionality in biometrics: Case studies from Norway. Computer Law and Security Review: The International Journal of Technology and Practice 25, 3 (2009), 237-250.

[28] Loranger, P.2000. US Army formulates its future biometric strategy. Biometric Technology Today 8, 5 (2000), 3-3.

[29] McMakin, D.L., Sheen, D.M., Hall, T.E., Kennedy, M.O., and Foote, H.P. 2007. Biometric identification using holographic radar imaging techniques. Proceedings of SPIE, (2007), 65380C.

DOI Link: http://dx.doi.org/10.1117/12.729636

[30] Mills, J.E. and Byun, S.2006. Cybercrimes against Consumers: Could Biometric Technology Be the Solution? IEEE internet computing 10, 4 (2006), 64-71.

[31] Murphy, H.C. and Rottet, D. 2009. An exploration of the key hotel processes implicated in biometric adoption. International Journal of Contemporary Hospitality Management 21, (2009).

[32] Phillips, P.J., Martin, A., Wilson, C.L., and Przybocki, M. 2000. An introduction to evaluating biometric systems. Computer, (2000), 56-63.

[33] Riley Jr, R.A. and Kleist, V.F. 2005. The biometric technologies business case: a systematic approach. Information Management & Computer Security 13, 2 (2005), 89-105.

[34] Ross, A. and Jain, A. 2003. Information fusion in biometrics. Pattern Recognition Letters 24, 13. (2003), 2115-2125.

DOI=http://www.sciencedirect.com/science/article/B6V15-

48N31PN-8/2/4296d07cfa90500427b755758bdeb1be

[35] Ross, A. and Jain, A.K. 2004. Multimodal biometrics: An overview. Proceedings of 12th European Signal Processing Conference, (2004), 1221-1224.

[36] Rudall, B.H. and Mann, C.J.H. 2008. New initiatives for new technologies. Kybernetes 37, 7 (2008), 1059-1065.

[37] Schuckers, S.A.2002 Spoofing and anti-spoofing measures. Information Security technical report 7, 4 (2002), 56-62.

[38] Venkatraman, S. and Delpachitra, I.2008. Biometrics in banking security: a case study. Information Management & Computer Security 16, 4 (2008), 415-430.

[39] Wayman, J.L. 2000.Federal biometric technology legislation. Computer, (2000), 76-80.

[40] Wirtz, B. 1997. Technical evaluation of biometric systems. Lecture notes in computer science, (1997).

[41] Zorkadis, V. and Donos, P. 2004. On biometrics-based authentication and identification from a privacy-protection perspective. Information Management and Computer Security 12, 1 (2004), 125-137.

[42] Harzing 2009. Publish or Perish, version (2.73),

available at www.harzing.com/pop.htm

[43] Science Daily. (Nov. 16, 2009). DOI= http://www.sciencedaily.com/releases/2009711/0911111213 58.htm

[44] Biometric History.2006. National Science and Technology Council. August 2006 DOI=http://www.biometrics.gov/Documents

[45] Isobe, Y.2005. Multimodal Biometrics System. “Personal Authentication Infrastructure for the Ubiquitous Information Age” .July 2005. DOI= http://www.hitachi.com/rd/sdl/people

[46] Osborn, A. 2005. The future of biometrics, “Trends and emerging uses for biometric technology” August 2005. DOI= http://www.video-surveillance-guide.com/future-of- biometrics.htm

[47] DOI=http://www.cse.msu.edu/~jain/

[48] DOI=http://www4.comp.polyu.edu.hk/~csdzhang

[49] Ngugi, B., et al. (2011). "Intention to Use Biometric Systems." e-Service Journal **7**(3): 20-46.

[50] Morosan, C. (2011). "Customers' Adoption of Biometric Systems in Restaurants: An Extension of the Technology Acceptance Model." Journal of Hospitality Marketing & Management **20**(6): 661-690.

[51] Rane, S., et al. (2013). "Secure Biometrics: Concepts, Authentication Architectures, and Challenges." IEEE Signal Processing Magazine, Signal Processing Magazine, IEEE, IEEE Signal Process. Mag. **30**(5): 51-64.

[52] Zinovieva, E. S. and Y. I. Vojtenko (2017). "Evolution of Biotechnology and Information Technology and Its Impact on Human Security." Vestnik MGIMO-Universiteta(5(44)): 154-161.

[53] Krishan, R. and R. Mostafavi (2018). "BIOMETRIC TECHNOLOGY: SECURITY AND PRIVACY CONCERNS." Journal of Internet Law **22**(1): 19-23.

[54] Naveed, R., et al. (2018). "Biometric template security: an overview." Sensor Review **38**(1): 120-127.

[55] Bhalla, A. (2020). "The latest evolution of biometrics." Biometric Technology Today **2020**(8): 5-8.

[56] Sarkar, A. and B. K. Singh (2020). "A review on performance,security and various biometric template protection schemes for biometric authentication systems." Multimedia Tools & Applications **79**(37/38): 27721-27776.

[57] SumYu, M. and A. Kumar (2012). Addressing biometrics security and privacy related challenges in China, IEEE**:** 1-8.