When the Past Technology Comes to the Future Wearable Technology: Speculative Art Project *Lock at First Sight* (2020)

Minso Kim
University of Colorado Boulder
Boulder, CO, U.S.A.
minso.kim@colorado.edu

Abstract

To protect information—both individuals' and corporations'—we use locks in both the real world and the digital environment. Due to the non-physicality in the digital environment, digital locks have appeared, such as numeric and letter-based combinations, the most common and secure way to perform any online activity. For additional security purposes, passwords have to be updated every few months. Clearly, it is true that there is no way to avoid using those passwords as long as we connect to the digital world. In other words, users easily get overwhelmed by the plethora of passwords regarding secure combinations, security questions, and regulations. Biometric data is permanent and cannot be changed—you cannot change your biologically innate iris or fingerprint. To lessen the burden, digital authentication systems apply biometrics technologies, such as iris scanners or fingerprint sensors on smartphones. Inspired by ancient signet rings (seals), the author proposes a speculative art object, *Lock at First Sight* (2020), a soft contact lens with a unique marker as a wearable security lock, which highlights lesser-known vulnerabilities in biometrics. This object is intended as social and artistic commentary, not as a functional product proposal for a commercial marketplace.

Keywords

Speculative practice, artistic practice, biological human bodies in the digital world, historical artifacts in the future technologies, contact lenses.

Introduction

It has been more than twenty years since the release of the film, *Minority Report* (2002). Those who watched the movie as teenagers have now grown into adults watching it at home. Digital platforms have evolved into new community spaces for sharing thoughts, generating discussions, and creating new auras around subjects within popular culture. [1] [2] In 2020, on Reddit—a social news aggregation, content rating, and discussion website—a user named 'FireLiesWithin' posted that the movie *Minority Report* "is eerily accurate in regard to technology and law enforcement. (…) the arguing couple who stop screaming at each other midsentence to allow the spiders to scan their retina, then continue the brawl like nothing happened. I could see something similar becoming a part of our 'normal' life in the future." [3]

In the movie, people use their biometrics, such as their irises, to verify their identities. The protagonist in the movie steals another person's actual eye and implants it into his eyehole to disguise his social identity from digital authentication systems. This illustrates how our biological bodies become not only valuable living organisms but also living keys to access digital information in the virtual world. In a scenario like *Minority Report*, can our eyes be safe from theft in both the physical and digital realms? In 2023, in the reality we inhabit, how can we effectively utilize our iris biometrics?

To protect information—both individuals' and corporations'—we use locks in both the real world and the digital environment. Due to the non-physicality in the digital environment, digital locks have appeared, such as numeric and letter-based combinations, the most common and secure way to perform any online activity.

For additional security purposes, passwords have to be updated every few months. Clearly, it is true that there is no way to avoid using those passwords as long as we connect to the digital world. In other words, users easily get overwhelmed by the plethora of passwords regarding secure combinations, security questions, and regulations. Biometric data is permanent and cannot be changed—you cannot change your biologically innate iris or fingerprint. To lessen the burden, digital authentication systems apply biometrics technologies, such as iris scanners or fingerprint sensors on smartphones.

This paper highlights lesser-known vulnerabilities in biometrics through my speculative art object, *Lock at First Sight* (2020), which proposes the idea of a soft contact lens with a unique marker as a wearable security lock.

What is Biometrics?

To highlight the role of wearable temporary biometrics, such as *Lock at first sight*, in the near future, it is crucial to comprehend the characteristics of biometrics. Biometrics is based on the concept of "oneness (uniqueness)" of an individual's body, meaning we all "carry" biometrics as passwords in our bodies. Such unique physical characteristics in bodies can be used for automated recognition systems in the present.

The first biometric information was collected in 1891 by anthropologist and police official Juan Vucetich who collected fingerprints from criminals in Argentina. Since this first collection of fingerprints, types of biometrics have been advanced and categorized: physiological and behavioral biometrics. Physiological biometrics means information about an individual's physical body, including iris, retina,

voice, ears, faces, fingerprints, hand gestures, veins, and DNA. Behavioral biometrics, on the other hand, involves signatures, gaits, and keystroke dynamics. With all those types of biometrics, the physical human body now becomes a collection of varying mobile passwords for digital identification. Due to debates over individual rights and bodily integrity, or informational self-determination [1] the discrepancy between privacy and security has been a hot topic. To illustrate, once one of an individual's physical or behavioral biometrics is registered in any digital authentication system, then the registered biometrics information is no longer a secret. In other words, the registered biometrics is shared with and becomes an asset to a company that hosts and saves the information to apply it to automated recognition systems. This means when an individual's registered bio information is in a recognition system, it is no longer secret, and it is impossible to remove or revoke from the companies' systems.

One discrepancy example is that if one of an individual's physiological biometrics, such as iris patterns, is compromised, then the compromised data can no longer function as a secret password because anyone can exploit the leaked biometrics' information.

Another example is that the registered biometrics cannot be canceled, revoked, or changed. Despite the use of signals and templates that disguise biometrics through differentlooking algorithms, the embedded biometric information remains consistent after being decoded. [4] To resolve such issues, information technologists and cyber security experts study, develop, and recommend encryptions in the digital space.[5][6][7][8][9] Encryption is the process of converting original information into an alternative form, which can be unlocked by a specific digital key. These technologists' research focuses on how to advance digital authentication systems to protect digitized individuals' biometrics. [10][11]

Furthermore, there are relevant scholars who give attention to the technical limitations of biometrics authentication systems in the physical world.[12][13] For instance, Matsumoto and his colleagues made artificial fingers with gummy material either by pressing their fingers against it or by processing fingerprint images from prints on glass surfaces. According to their research, the ways in such systems can fail and be fooled.

Particularly, regarding iris recognition systems, information and forensic scholars found that while transparent soft contact lenses on user's eyes do not modify the iris texture, standard prescription contact lenses can interfere with the accuracy of iris biometrics [14] due to the lenses' effect on the reflection value of the iris location.[15] Thus, biometric system scholars have attempted to reduce errors that come from transparent soft contact lens users.[16][17] Furthermore, iris biometric systems are susceptible to a variety of attacks. In 2001, Ratha and their colleagues identified eight vulnerable spots. To counter the attacks on biometric recognition systems, several hardware or data-driven based solutions have been suggested.[18] In other words, biometric authentication systems are not infallible despite the complex algorithms that are supposed to protect data. In the light of the information presented above, a pertinent question arises: Could a contact lens be used as a medium to effectively function as an identifier rather than a medium that introduces false information and errors?

Adversarial and Speculative Design

Adversarial Design

We live with contentious issues in our daily lives. As science studies scholar Bruno Latour suggested, the contemporary world runs through matters of concern rather than matters of fact. Matters of concern include but are not limited to social, political, environmental, ethical, and religious issues. Addressing power dynamics between such conflicting arguments, adversarial design illustrates how design can represent and enact the political conditions of contemporary society, and functions in objects that challenge and offer alternatives to the present's dominant practices and agenda.[19] Carl DiSalvo suggests examples from social robots to umbrellas, websites, data visualization, and more.[19][20] Such adversarial design in the public space has been explored as public design [21], particularly in regard to surveillance issues.

Although the digital environment is open to everybody, cyber security systems in the digital space are hard to define as the public domain because such digital systems have to be private and inaccessible to the general public. Only professionals (hackers, or trespassers) can intrude. Designers suggest diverse types of wearables to promote awareness of surveillance issues at the accessible and public levels. For instance, facial recognition systems in surveillance cameras can trace certain citizens' contacts and walks. Many visual designers propose wearables that potentially confuse the facial recognition systems. Those examples include a wearable face projector [22], a privacy visor [23], and a makeup technique known as CV Dazzle [24].

In short, the recent adversarial design highlights the dominant issue of the biometrics security system by offering alternatives, particularly wearables that trick visual recognition systems.

Speculative Design

Speculative design is a branch of critical design that shares a critical perspective or encourages debate while increasing awareness of certain issues through proposing the role

[1] Informational self-determination was first coined by Germans, regarding personal information collected during the 1983 census, which is now enclosed as a right into their constitution.

objects play in everyday life. Bill Gaver and Heather Martin extend a branch of critical design to speculative design by providing conceptual design proposals. [25] In speculative design, science fiction is valued due to its futuristic vision that highlights new values that may appear with/within new technology in the future.

In the Human-Computer Interaction (HCI) design community, researchers categorize such fiction-based designs as diegetic prototypes rather than prototypes. Film scholar David Kirby defined a diegetic prototype as a cinematic depiction of future technologies that demonstrate the technology's usefulness, benevolence, and viability to the audiences.[26] Therefore, lending narratives and insights about the possible scenarios to audiences is a key element in speculative design.

Selfish Ledger (2016), filmed by Google, is a good example of a diegetic prototype about a speculative design. *Selfish Ledger* was distributed as an internal campaign video to the Google community—later it was opened to the public in 2018. The main idea in the campaign video was about Google's future application technology called 'ledger', which can shepherd individuals' activities/thoughts to overcome current or situated societal issues through Google's algorithms. Putting the intention embedded in the ledger aside, the narrative about the ledger presents that the company plans to form societal betterment via their future technological systems through a campaign video. In short, speculative design proposes objects that address potential societal, cultural, or ethical issues of near-future technology by broadening the scope of design and systems. This speculative design process is as follows: identify signals of emerging technologies and trends, ideate future products, storify the products, and share them to generate discussion. Pro-speculative design thinks that speculative design helps designers to be a more imaginative group than problem-solving thinkers. This enables them to develop boundary-pushing prototypes for the future. In contrast, counterparts say that due to the lack of functionality and marketability, speculative design is useless object-making. In such a sense, speculative design is established upon critical insights that go beyond an agenda of consumer culture and instead embody cultural critique in designed artifacts.
[26]

Thus, speculative design is about highlighting little-discussed issues in the present by storifying them into imaginative narratives about the near future in forms of new media, such as films and design objects.

Lock at First Sight (2020)

In *Lock at First Sight* (2020), I introduce a concept for a wearable firewall designed to address contemporary biometric concerns, specifically focusing on iris patterns. This proposed artifact takes the form of a pair of contact lenses featuring a custom-designed iris pattern on their surface. My approach involves merging adversarial design principles with speculative design methods to create a design that could potentially benefit both users and biometric authentication systems in the near future.

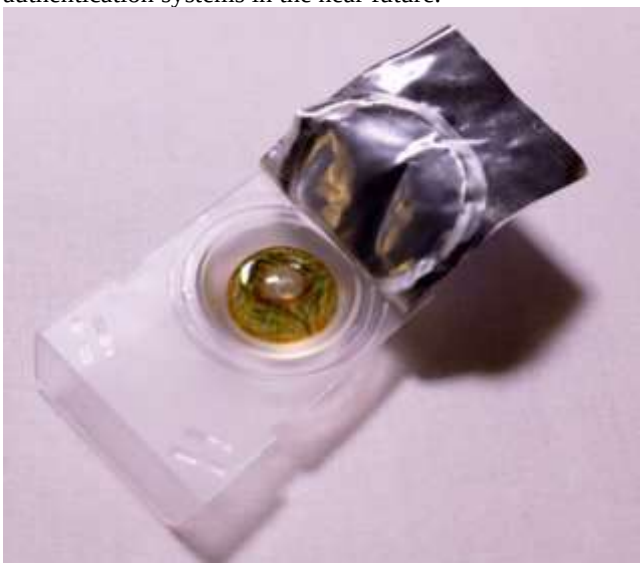

Figure 1. A picture of Lock at First Sight (2020). ©Author.

First of all, this design proposal is inspired by combining invisible technology, particularly wearable technology, with autographic authentication tools. Invisible technology embodies the concept of invisibility applied to technology. This notion was popularized by Donald Norman's 1999 book, *The Invisible Computer: Why Good Products Can Fail, the Personal Computer is So Complex, and Information Appliances are the Solution*. Norman proposed that personal computers were overly complicated to use and should be replaced by what we now refer to as the Internet of Things (IoT) and wearable devices. Invisible technology is a use case where individuals deploy technology without necessarily realizing that they are doing so.

In fact, wearable technology has a longer history than we generally think. There are historical records about a signet ring that was presented to the holder of an office as the seal and badge of authority in Genesis 41: 41-43. [27][28] Additionally, as early as the 17th century in China, merchants used an abacus ring to solve mathematical tasks, without using any writing tools.[29]

In East Asia, people use both seals and handwritten signatures for important documents, such as legal warranties and agreements. Scholars and scientists have studied and verified how the digital environment can use the images of seal imprints as digital verification by recognition systems [30][31][32][33]. The combined concept of wearability with handwritten signatures in digital verification systems promotes me to suggest the design proposal for alternative digital authentication tool, *Lock at First Sight*.

From the adversarial design aspect, I propose my designed artifact as an alternative that can transform the recognition system issues today. The following are the issues that are highlighted in this proposed designed artifact: If a person has a custom-designed iris contact lens that verifies their identity

in digital systems, they can bypass the need to trust the security of the company's data storage and avoid disputes over their ownership of biological information (data privacy); Furthermore, if a person lost their custom-designed iris contact lens, they could easily cancel the lens's data (cancelability); If a person can easily change their contact lens design, they will become more responsible biometric-users who are aware of the importance of their digital identifiers because they actively participate in the process of designing their iris contact lens (changeability). From the speculative design approach, I demonstrate how *Lock at First Sight* can be designed via a form of contact lens. To dramatize how the lens could be operated, I propose to use a soft contact lens with a custom-designed image as a medium to identify its user instead of using natural iris biometrics. As mentioned above, researchers in biometrics find that when a user wears soft contact lenses, the lenses interfere with iris recognition systems causing them to produce errors or false data instead of accurate outputs. Accordingly, the researchers try to solve the error issue by developing better algorithms for better iris recognition data results. However, my reversed way of using a soft contact lens will promote a new approach to iris biometrics and underscore the significance of embracing alternative perspectives. Additionally, it will address concerns surrounding iris recognition systems, prompting a comprehensive reevaluation of the subject matter.

In short, *Lock at First Sight* is a design proposal to use a custom-designed iris pattern on a soft contact lens as a wearable digital firewall and an alternative marker for biometrics authentication systems.

Wearable Hand-written Autograph

To create a unique identifier, I think about a behavioral biometrics' method, which has been effectively used for historically longer periods: hand-written signatures as in signet rings and seals.

The ability to write letter formations varies from one person to another because the act of handwriting is based on each writer's visual perception of images when they first learn how to write letters. And the repetitive practice of writing forms habitual features in an individual's writings which are distinguishable from another's.

Although there is controversy around the consistency of handwriting document examination, published research demonstrates the validity of analysis in handwriting documents and has developed the standards of handwriting individuality.[34] To clarify rationality of handwriting's uniqueness, the Scientific Working Group for Forensic Document Examination develop and publish over 20 criteria that are used to evaluate handwriting as evidence for criminal cases and more for 15 years.[35] When a person's anatomy and physiology of the bones and muscles get used to writing, then the writer's writing skill becomes consistent and retains its features throughout adulthood.[36] Handwriting examination is based on the assumption that no two people likely produce the same habits and features in their handwriting.

To sum up, a person's hand-written autograph presents a unique pattern image, which cannot be duplicated. Furthermore, scientists have developed image recognition systems that read and utilize such inimitable imprints for securing digital documents. Because only one person can generate autographs that reflect their writing habits and features, each autograph looks slightly different.

When an image of a hand-written autograph is imprinted on the surface of a contact lens, then the contact lens becomes to have similar features in a physical seal in a form of wearables. By doing so, users can potentially preserve an individual's natural body biometrics and create temporal identifications, which are cancelable and revocable.

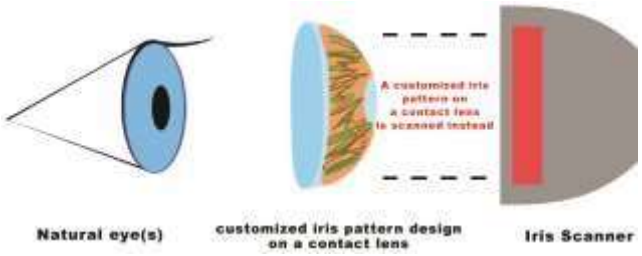

Figure 2. An idea about a wearable physical firewall in a form of contact lens ©Author

Design Process

Let us think about a speculative moment in the near future like this: One day you get an alarming text message. It is from a company that stores your biometrics for digital authentications. The text message tells you that iris pattern data have been compromised by anonymous hackers. If you used your own (natural) iris patterns, then you have no other option but cannot use your iris for authentication for the rest of your life. What if, instead you had registered a temporary iris pattern? If you had registered an alternative iris pattern by wearing a contact lens, then you have an option: you can throw out the current contact lens and register a new contact lens with a new pattern.

To design the *Lock at first sight*, the author practiced their autographs on numerous sticky notes: one autograph per a sticky note. Then, they chose one to three exemplary signatures that had precise lines and patterns. Then, they scanned the images to digitize the autographs.

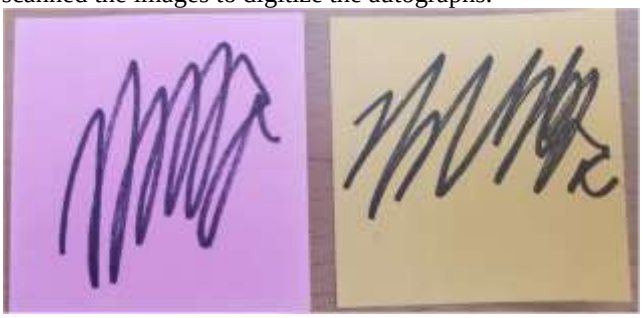

Figure 3. Signature samples for iris pattern designs ©Author

Next, the author chose colors that would be applied to the digitized images. They preferably chose the colors that could contrast with their natural iris color.

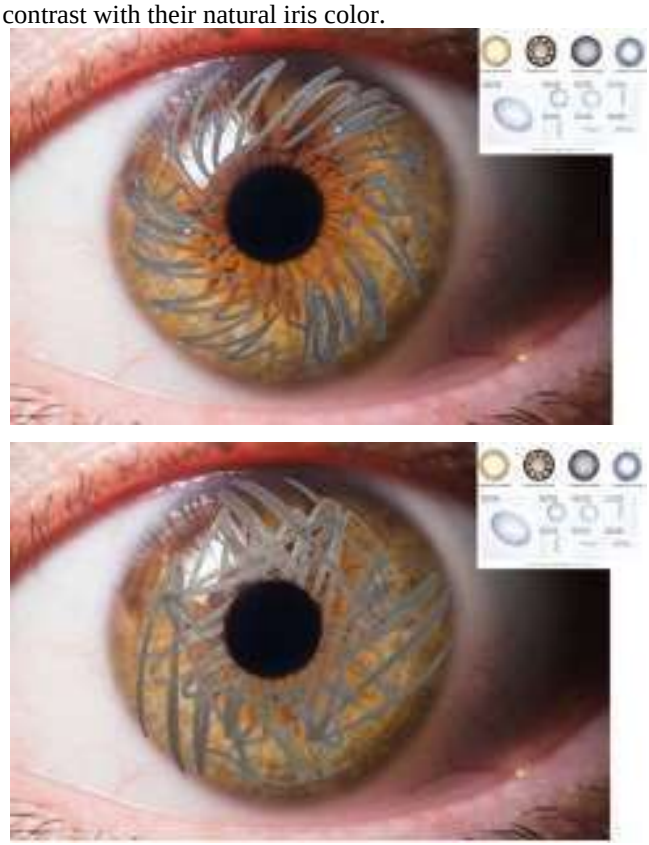

Figure 4. Examples of the autograph sequence design on the surface of a contact lens. ©Author

Then, the author tried to find a preferred sequence or layout of autograph images, for instance, putting a signature image on the half surface of a lens, or arranging the same four signature images in a cross shape. The author kept in mind that the center of the lens surface should have a small empty space because if any image goes into the center, then it would block light that goes into a user's pupil. Finally, the author sent her iris pattern design to a contact lens company to make customized contact lenses.

The final speculative art object has been displayed in a round-bottom plastic container with an aluminum cover. The container is big enough to hold one contact lens and solution to soak the lens.

Discussion

The proposed creative artifact, *Lock at First Sight*, synthesizes adversarial and speculative design practices. This discussion aims to contextualize *Lock at First Sight* within the broader landscape of wearable technology, mainly focusing on its connection to soft contact lenses. By delving into the current state and historical trajectory of smart contact lens development, we can better appreciate the innovative potential and societal implications of *Lock at First Sight*.

Figure 5. A detailed picture of *Lock at First Sight* ©Author.

In the contemporary realm of wearable technology, the concept of smart contact lenses has garnered attention for its potential to revolutionize healthcare and augment daily living experiences. Notably, in 2014, Verily (formerly Google Lift Sciences) unveiled its ambitious project to create a smart contact lens capable of monitoring glucose levels in diabetes patients. This initiative marked a significant intersection of technology and healthcare, with a micro-size wireless chip and a glucose monitor integrated into the lens. [37] However, despite initial enthusiasm, the project faced a notable hiatus, as observed by its apparent silence in 2016 [38] The trajectory of smart contact lens development did. not remain stagnant, as Mojo Vision presented working prototypes of Augmented Reality (AR) contact lenses at the Consumer Electronics Show (CES) in the early 2020s.[39] The collaboration with Amazon to develop the Alexa Shopping List app for the Mojo Vision's AR contact lens added a layer of functionality and utility to the technology.[40] However, the subsequent announcement of Mojo Vision's pivot away from smart contact lens technology[41] underscores this field's dynamic and evolving nature. In light of these historical developments, *Lock at First Sight* emerges as a speculative art object that reflects the current landscape of wearable technology and speculates on its future possibilities. The proposed design's exploration of soft contact lenses as more than mere medical devices positions it within a broader discourse on integrating technology into our daily lives. *Lock at First Sight* prompts us to consider the socio-technical aspects of wearable devices, encouraging discussions on user experiences, ethical considerations, and the evolving role of technology in shaping our interactions with the world.

In a nutshell, the exploration of *Lock at First Sight* transcends its immediate temporal context, inviting a profound reflection on the ever-evolving trajectory of smart contact lens technology and its enduring impact on society. In other words, the art project provides a social commentary and can be contextualized within the continuum of past initiatives and industry shifts, to unearth insights into the multifaceted nature of wearable technology and the intricate interplay between creative artifact, functionality, and societal dynamics across the present and the future. While this project seems functional, it is not the project's primary focus; rather it is a speculative art object, meant to encourage discourses.

Additional research

After the *Lock at First Sight* project, the author created a photography series, *Citizen X* in 2022. *Citizen X* (Figure 6) is a visualization of how people would look if they wore *Lock at First Sight* in daily life. *Citizen X* reveals the expected pros and cons of *Lock at First Fight* if the contact lens became a norm in the near future. For example, *Citizen X* shows that if *Lock at First Sight* became a norm, it would contribute convenience to personal style as well as security. On the other hand, the need for frequent cleaning of the contact lens may be a downside to widespread adoption.

Figure 6. 4 photos of *Citizen X* (2022) series. ©Author.

Conclusion

The author suggests a speculative art object, *Lock at First Sight*, a soft contact lens that can be worn and used for the purpose of authenticating the user's identity. It is based on the author's artistic vision about alternative iris patterns in emerging technology. The author shows that traditional hand-written autograph (drawing) method can be applied to invisible technology in the form of soft contact lenses. This design proposal highlights three issues: One is the potential of combinations of traditional seals (signet) with handwriting methods in today's technology. Another is the current status quo of soft contact lenses in digital technology. The last one is raising the awareness of biometric authentication, particularly the fact that registered bio information is neither cancelable nor revocable. By exhibiting her idea in the form of *Lock at First Sight*, the author encourages ethical questions about the equitable uses of an individual's biodata within biometrics authentication systems. In summary, the author mediates her artistic vision on the interactions between the human bodies and the digital environment by exploring both the past and the future technologies. By incorporating the author's artistic vision with wearable technology, the proposed speculative art object serves multiple purposes. It 1) highlights a flaw in current iris recognition interactions associated with soft contact lenses, 2) recognizes an opportunity to redefine the role of soft contact lenses in future recognition interactions, 3) introduces wearable hand-written autographs as an alternative for digital interactive authentication systems, supplanting the use of natural iris patterns, and 4) integrates the concepts of drawings, design methods, and biometrics into a cohesive artifact, *Lock at First Sight*.

Acknowledgements

I would like to thank all of the participants in my study, who generously shared their time and experiences with me. I am grateful to the anonymous reviewers, who provided constructive feedback and helpful comments that allowed me to refine this paper. This research has been partly funded by Beverly Sears Graduate Student Grant 2019 from the Graduate School at the University of Colorado Boulder (CU-Boulder), and Creative Research Grant 2020 from the Department of Critical Media Practices at the CU-Boulder. Special thanks to professor Tara Knight's and professor Laura Devendorf's advice and encouragement.

References

[1] Minso Kim. "Does Ritual Disappear as Walter Benjamin Describes in 'The Work of Art in the Age of Mechanical Reproduction' in the Age of Digital Technology?". In the proceedigns of the *23rd International Symposium on Electronic Art (ISEA) 2017*.

[2] Minso Kim. "Newly generated ritual in the age of digital technology" *Virtual Creativity*, vol. 8, no. 2, pp.179-188.

[3] FireLiesWithin. "Minority Report is scary accurate for being ~20years old" *Reddit*, 2020. https://www.reddit.com/r/movies/comments/gpzqt4/minority_report_is_scary_accurate_for_being/

[4] Christian Rathgeb and Andreas Uhl. "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security* 2011 (2011), 1–25.

[5] Sanaul Hoque, M Fairhurst, Gareth Howells, Farzin Deravi,. 2005. "Feasibility of generating biometric encryption keys," *Electronics Letters* 41, 6 (2005), 309–311.
[6] Ann Cavoukian and Alex Stoianov. "Biometric encryption: a positive-sum technology that achieves strong authentication, security, and privacy," *Information and Privacy Commissioner of Ontario* (2007).
[7] Alex Stoianove, Ann Cavoukian, Michelle Chibba. "Advances in biometric encryption: taking privacy by design from academic research to deployment," *Review of Policy Research* 29, 1 (2012)
[8] Ratha N. K., Patel V. M., and Chellappa R. "Cancelable Biometrics: A review," *Signal Processing Magazine* 32, 5 (2015), 54– 65
[9] M, V. K., Venkatachalam, K., P, P., Almutairi, A., and Abouhawwash, M. "Secure biometric authentication with de-duplication on distributed cloud storage," *Peer Journal Computer science*, 7, e569. (2021) https://doi.org/10.7717/peerj-cs.569
[10] Nalini K. Ratha. "Privacy Protection in High Security Biometrics Applications," *Ethics and Policy of Biometrics* (2010), 62–69.
[11] Javier Galbally, Patrizio Campisi, Julian Fierrez, Marta Gomez-Barrero, and Emanuele Maiorana. "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognition* 67 (2017), 149–163.
[12] van der Putte, T. and Keuning, J. (2000). "Biometrical Fingerprint Recognition: Don't get your Fingers Burned," *The International Federation for Information Processing* 52. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35528-3_17
[13] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada Satoshi Hoshino "Impact of artificial "gummy" fingers on fingerprint systems," *Proceedings of SPIE* 4677, optical Security and counterfeit deterrence techniques IV (2002).
[14] Baker S, Bowyer KW, Flynn PJ. Contact lenses: handle with care for iris recognition. Proceedings of the Third Int Conf on Biometrics: Theory, Applications and Systems (BTAS 09), September (2009)
[15] Hugo Proença,and Luís A. Alexandre (2012) Toward Covert Iris Biometric Recognition: Experimental Results From the NICE Contests, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2 , 798-807.
[16] D.Yadav,N.Kohli,J.S.Doyle,R.Singh,M.Vatsa,K.W.Bowyer, "Unraveling the effect to textured contact lenses on iris recognition, IEEE Trans. Inf. ForensicsSecur.9(5)(2014)851–862.
[17] Meenakshi Choudhary, Vivek Riwari, Venkanna U. (2019) "An approach for iris contact lens detection and classification using ensemble of customized DenseNet and SVM" Future Generation Computer Systems. vol.101 p.1259-1270.
[18] Verma, P., Selwal, A. & Sharma, D. A survey on data-driven iris spoof detectors: state-of-the-art, open issues and future perspectives. *Multimed Tools Appl* 82, 19745–19792 (2023). https://doi.org/10.1007/s11042-022-14014-4
[19] Carl DiSalvo. *Adversarial Design as Inquiry and Practice*. MIT Press, Chapter 5 (2012) 115–125.
[20] Tom Jenkins, Jonathan Lukens, Tanyoung Kim, Carl DiSalvo, and Thomas Lodato. "Making Public Things: How HCI Design Can Express Matters of Concern," *Computer Human Interaction 2014*, 2397–2406.
[21] Jing-Cai Jiu. "Wearable face projector (2017)", http://jingcailiu.com/wearable-face-projector/
[22] Isao Echizen. "Privacy Visor (2013)", https://research.nii.ac.jp/~iechizen/official/research/research2-e.html
[23] Adam Harvey. "CV Dazzle (2010)", https://cvdazzle.com/
[24] Heather Martin and William W. Gaver. "Alternatives: exploring information appliances through conceptual design proposals," *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (2000)., Vol. 1, No. 1, Article. Publication date: October 2022.
[25] David Kirby. "The future is now: Diegetic prototypes and the role of popular films in generating real-world technological development," *Social Studies of Science* 40, 1 (2010) 41-70.
[26] Fiona Raby and Anthony Dunne. *Speculative Everything: Design, fiction, and social dreaming*. (2013) The MIT Press.
[27] New international Version (2011) NIV online: https://www.biblegateway.com/passage/?search=Genesis%2041%3A41-43&version=NIV
[28] Herbert E. Winlock (1922) "A gift of Egyptian antiquities" The Metropolitan Museum of Art Bulletin. Vol. 17, no. 8, pp.169173.
[29] Tom Page (2015) "Barriers to the adoption of wearable technology" i-manager's Journal on Information Technology, vol.4, no.3.
[30] Shengfu Dong, Wen Gao, and Xilin Chen. "A system for automatic Chinese seal imprint verification," *In Proceedings of 3rd International Conference on Document Analysis and Recog-nition* (1995) Vol. 2, 660–664.
[31] H. Leung. "Analysis of traditional Chinese seals and synthesis of personalized seals," In 2004 *IEEE International Conference on Multimedia and Expo* (ICME) (IEEE Cat. No.04TH8763), Vol. 2. 1283–1286.
[32] P. P. Roy, U. Pal and J. Lladós, "Seal Detection and Recognition: An Approach for Document Indexing," *2009 10th International Conference on Document Analysis and Recognition*, 2009, pp. 101-105, doi: 10.1109/ICDAR.2009.128.
[33] Bin Sun, Shaojun Hua, Shutao Li, and Jun Sun. "Graphmatching-based character recognition for Chinese seal images," *Science China Information Sciences* 62 (2019).
[34] Diana Harrison, Ted M Burkes, and Danielle P Seiger. "Handwriting examination: Meeting the challenges of science and the law," *Forensic Science Communications* 11, 4 (2009), 1–13.
[35] Rigo Vargas. "Standards in forensic document examination" In *Forensic document examination in the 21st century* (CRC Press, 2020), 7–8.
[36] Marie E. Durina and Lisa M. Hanson. "Development of habitual handwriting characteristics in elementary school studies" In *Forensic document examination in the 21st century* (CRC Press, 2020), 73–79.
[37] Brian Otis, Babak Parviz (Jan. 16, 2014) "Introducing our smart contact lens project" ALPHABET. https://blog.google/alphabet/introducing-our-smart-contact-lens/
[38] Angela Chen (Nov. 16, 2018) "Verily pauses research on glucose-sensing contact lens" Verge. https://www.theverge.com/2018/11/16/18099193/verily-novartis-glucose-contactlens-science-health
[39] Tekla S. Perry (Jan. 16, 2020) "Augmented Reality in a contact lens: It's the real deal" IEEE Spectrum. https://spectrum.ieee.org/ar-in-a-contact-lens-its-the-real-deal

[40] Carol Boyko. “Mojo vision announces test integration with Alexa Shopping List on smart contact lens” *Business wire*, Nov. 3, 2022. https://www.businesswire.com/news/home/20221103005395/en/Mojo-Vision-Announces-Test-Integration-With-Alexa-Shopping-List-on-Smart-Contact-Lens
[41] Drew Perkins (Jan. 6, 2023) "A new direction for Mojo Vision's groundbreaking technology" The Mojo Blog. https://www.mojo.vision/news/a-new-direction

Bibliography

Claus Vielhauer. *Biometric user authentication for IT security: from fundamentals to handwriting*. Springer Science & Busi-ness Media (2005)

Dourish, Paul. “Embodied interaction: Exploring the foundations of a new approach to HCI” (1999) https://www.researchgate.net/publication/228934732_Embodied_interaction_Exploring_the_foundations_of_a_new_approach_to_HCI

Erik Parens. “Authenticity and Ambivalence: Toward Understanding the Enhancement Debate.” *The Hastings Center Report* 35, no. 3 (2005): 34–41. https://doi.org/10.2307/3528804.

Erik Stolterman and Anna Croon Fors. “Information technology and the good life,” In *International Federation for Information Processing* 143 (2004) 687-692.

Galbally Javier, A. A. Ross, Marta Gomez-Barrero, Julian Fierrez and Javier Ortega-Garcia. “From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems.” (2012).

Harumi Kimoto. “Japan’s official seal culture an obstacle to fullscale teleworking amid virus fears”, *Mainichi Japan* (April 3, 2020) https://mainichi.jp/english/articles/20200402/p2a/00m/0na/020000c

James I. Novak (2020) “Awareables: Beyond wearable technology” TEI’ 20, p.5-16.

K.W. Bowyer, S.E. Baker, A. Hentz, *et al.* Factors that degrade the match distribution in iris biometrics. *IDIS* **2**, 327–343 (2009).

Mark Weiser and John Seely Brown (1996) “The coming age of calm technology”, a revised version of “designing calm technology” PowerGrid Journal, v 1.01 (1996) https://people.eng.unimelb.edu.au/vkostakos/courses/ubicomp10S/papers/visions/weiser-96.pdf
Vlad Savov. “Google’s Selfish Ledger is an unsettling vision of Silicon Valley social engineering” The Verge (May 17, 2018) https://www.theverge.com/2018/5/17/17344250/google-x-selfishledger-video-data-privacy

Author(s) Biography(ies)

Minso Kim is an international artist, educator, and researcher whose practice explores the relationship between analogue and digital worlds through human interaction. Together, her creative and academic works not only consider the sensorial experiences of art, but they meditate on human life infused with diverse categories, from the environment to computational systems, to popular culture. Kim’s artwork and writing have been shown and published in various countries: Minnesota State University, Universidad de Caldas, Short Film Festival Budapest, (Buk-)Seoul Museum of Art, and more. She graduated from the School of the Art Institute of Chicago, with a master’s degree in art and technology studies in 2013. Minso has taught contemporary art practices and theory at universities from 2011 to 2017. Recently, Kim completed her doctoral degree in Emergent Technology and Media Art Practices at the University of Colorado Boulder.