

Risk Analysis Research on SMS Verification Code and Biometric Recognition Technology

Likun Yu

Information and computer science, University of California, Irvine, 92612, USA

likuny@uci.edu

Abstract. This paper delves into the ongoing transformation in the domain of digital identity security. It specifically focuses on the paradigm shift from traditional methods of authentication, such as passwords and text message verification codes, towards the use of biometric recognition technology. By scrutinizing the inherent weaknesses linked with the utilization of text message verification codes, the paper underlines the demand for more trustworthy and secure solutions for authentication. Following this, biometric authentication is thoroughly examined, with a highlight on its unique features, the convenience it provides to users, and its capacity for ongoing verification. The discussion extends to practical applications of biometrics in a variety of sectors, including healthcare and high-security workplaces, as well as in situations where employing text message verification is unsuitable. A focal point of the discussion is multi-modal biometric authentication. While acknowledging the potential hurdles and future possibilities tied to the adoption of biometric technology, the paper offers an objective perspective. The overall intent of this research is to furnish insights that will enable informed decision-making regarding the deployment and improvement of digital identity verification methods across a wide range of industries.

Keywords: Digital Identity Security, Biometric Recognition Technology, SMS Verification Codes, Multi-modal Biometric Authentication.

1. Introduction

In this age of digital transformation, where the lines between physical and virtual realities are increasingly dissolving, the security of digital identity has emerged as a crucial concern [1]. As an escalating amount of personal, financial, and sensitive information is stored and transacted online, safeguarding it from unauthorized access has become of utmost importance. Traditional security methods such as passwords and text message verification codes have been the primary tools for digital identity verification for a long time. However, as these methods become more susceptible to various security risks, the need to delve into more reliable and secure authentication mechanisms grows stronger.

This paper delves into the domain of biometric recognition technology, investigating its advantages over traditional methods such as text message verification codes and its deployment in various sectors [2]. The discussion begins with a detailed analysis of security risks associated with text message verification codes, touching on vulnerabilities to social engineering and brute-force attacks. Subsequently, the discourse shifts towards the merits of biometric authentication, exploring its potential to provide enhanced security and convenience. Moreover, the study examines how the integration of biometric authentication with traditional methods can amplify security, using banking verification as a pertinent example. However, it is important to note that every technology comes with its challenges, and biometric authentication is no exception. This paper shines a light on potential impediments and future prospects associated with the implementation of biometric technology. By illuminating these aspects, the aim is to offer a comprehensive understanding of biometric recognition technology. This, in turn, can facilitate informed discussions and decisions about the implementation and enhancement of digital identity verification methods across a range of sectors [3].

2. Security Analysis of SMS Verification Code

In the rapidly evolving digital era, the pervasive use of Short Message Service for user authentication has emerged as a standard practice. This seemingly simple and user-friendly method, however, is not without its weaknesses. One of the primary concerns associated with SMS verification codes is the potential for interception during transmission over public telecommunication networks. The risk of various forms of attacks, such as man-in-the-middle (MITM) and phishing attacks, further adds to the security concerns of this method. Furthermore, the dependence on mobile devices - vulnerable to loss, theft, or compromise - contributes to the precariousness of the security infrastructure that underlies the use of SMS verification codes [4].

Delving deeper into the vulnerabilities, social engineering attacks emerge as one of the significant threats to SMS-based authentication. Social engineering, a nefarious technique involving the manipulation of individuals into divulging confidential information, often manifests itself in the guise of a trusted entity. For instance, an attacker might employ a seemingly innocuous text message, claiming to originate from a credible organization, and deceive users into revealing their verification codes. Consequently, the attacker bypasses security measures and gains unauthorized access to the victims' personal accounts [5]. Moreover, another pervasive threat to the security of SMS verification codes is password cracking. Notwithstanding the extra layer of protection SMS verification codes offer, they remain susceptible to brute-force attacks. In such attacks, adversaries employ software that generates and tests an extensive range of code combinations in rapid succession. The vulnerability of SMS verification codes to password cracking is compounded by the fact that these codes often consist of a limited number of digits. This constraint significantly decreases the possible combinations, inadvertently increasing the success rate of brute-force attacks.

Beyond the security risks, the use of SMS verification codes also presents practical challenges for users [6]. The dependence on mobile devices can often become a barrier, particularly when users are unable to receive the required codes. This could be due to a range of issues including, but not limited to, network coverage problems, device malfunctions, or simply when the mobile device is not within the user's reach. Consequently, users may find themselves unable to access their own accounts remotely, leading to significant inconvenience and potential disruption to their activities. The inability to access essential services at critical times underscores the need for more reliable and user-friendly authentication methods, further motivating our exploration into the application of biometric recognition technology.

3. Advantages of Biological Validation

The increased demand for robust and user-friendly security measures in our digital landscape has led to the rise of biometric authentication. This mode of identification, which uses unique biological characteristics such as fingerprints, facial features, iris patterns, or voice profiles, offers several advantages over traditional methods like passwords and SMS verification codes [7].

Firstly, biometric characteristics are inherently unique to each individual, making them difficult to replicate or steal. Unlike passwords or SMS verification codes, which can be easily shared, guessed, or cracked by malicious entities, biometric traits provide a level of security that is intrinsically linked to the individual. This uniqueness provides a significant deterrent to unauthorized access, as it requires physical presence or highly sophisticated techniques to replicate these personal traits.

Secondly, biometric authentication provides convenience for users. Unlike password-based systems that demand users to remember complex strings of characters, or SMS-based verification that depends on the availability of mobile devices and network connectivity, biometric authentication is readily accessible. A user simply needs to present their biometric trait - a fingerprint, a face scan, or a voice command - to gain access to their accounts. This method reduces the likelihood of being locked out due to forgotten passwords or inaccessible SMS codes [8].

Finally, biometric authentication supports continuous authentication. Traditional authentication methods authenticate users at the point of login, but they cannot detect if someone else takes over the

session after the initial login. In contrast, biometric systems can continuously monitor the authenticated user, thereby increasing security by providing real-time detection of unauthorized users.

While biometric authentication brings substantial improvements, it is not without its challenges, including privacy concerns and potential technical issues. The subsequent sections of this paper will further explore these considerations and propose ways to optimize the use of biometrics for user authentication.

4. Research on Biological Validation Application Scenarios

As we dive deeper into the realm of biometric authentication, it's essential to analyze real-world scenarios where biometric authentication can effectively replace traditional methods like SMS verification [9]. A deeper understanding of these scenarios will shed light on the practical applications of this technology and how it can be effectively deployed to enhance user security and convenience.

Biometric authentication's ability to reliably confirm the presence of an individual is a standout advantage, especially when considering scenarios in sectors such as healthcare and workplaces. By nature, biometric traits can't be transferred or misplaced, unlike passwords or verification codes, providing an unmistakable indication of the individual's presence.

In the context of healthcare, patient identification is a crucial aspect that impacts patient safety and the quality of care delivered. Relying on traditional methods such as patient ID cards or verification codes sent to registered phone numbers presents a host of challenges. They can be easily misplaced, stolen, or misused, leading to potential misidentification and associated consequences. With biometric authentication, these concerns are significantly alleviated. A patient can be accurately identified by their unique biometric traits, ensuring the right care is provided to the right person. This can be particularly critical in high-stress situations, such as emergency medical cases where swift and accurate identification can save lives [10].

Workplaces, particularly those dealing with sensitive data or operating in high-security areas, can also benefit greatly from the adoption of biometric authentication. Traditional access methods, such as ID cards or passcodes, can be shared, lost, or stolen, making them a potential security risk. Moreover, they cannot provide definitive proof of the individual's presence. However, biometric authentication such as fingerprint scanning or facial recognition offers a more secure alternative. An employee's access to sensitive areas or confidential data can be effectively managed through biometrics, ensuring that only authorized individuals have access and that their presence is accurately recorded.

In both these scenarios, biometric authentication offers a higher level of assurance regarding the individual's presence compared to traditional verification codes. Not only does it bolster security by reducing the chances of misidentification or unauthorized access, but it also significantly enhances operational efficiency and the overall user experience. The deployment of biometric authentication in such critical sectors underscores its value as a robust, reliable, and convenient alternative to conventional authentication methods.

Another crucial application scenario of biometric authentication arises in situations where traditional means like SMS verification are infeasible. Consider a situation where a user is in a region with poor network coverage or the mobile device is lost or stolen. In these circumstances, receiving an SMS verification code would be impossible, leaving the user unable to access their accounts. This is where multi-modal biometric authentication can play a pivotal role.

Multi-modal biometric authentication refers to the use of more than one biometric trait for verification. For example, a system might require both fingerprint and facial recognition to authenticate a user. Such a system would be highly beneficial in situations where SMS verification is unviable. The user simply needs to scan their fingerprint and face using the biometric reader, circumventing the need for network coverage or the specific mobile device tied to the account.

From a security standpoint, multi-modal biometric authentication outstrips SMS verification. The SMS verification process is susceptible to several security risks, including code interception and

social engineering attacks. In contrast, multi-modal biometric systems significantly heighten security. Since the system uses two or more biometric traits, even if one trait is somehow compromised, the other trait(s) provide an additional layer of security. This means the attacker would need to forge multiple biometric traits simultaneously, a task considerably more challenging than intercepting an SMS code or guessing a password.

Aside from superior security, multi-modal biometric authentication offers improved user convenience. Users no longer need to remember complex passwords or wait for SMS codes to arrive. Nor do they have to worry about network coverage or the availability of their mobile device. They just present their biometric traits - as simple as looking into a camera or touching a fingerprint sensor - to gain access to their accounts. This ability to authenticate in a few quick and easy steps enhances the user experience, making biometric systems not just more secure, but also more user-friendly than traditional methods.

In sum, in scenarios where SMS verification falls short, multi-modal biometric authentication emerges as a robust and convenient alternative. It provides superior security by leveraging the inherent uniqueness and complexity of multiple biometric traits and offers users a smooth and effortless authentication experience. These advantages reaffirm the tremendous potential of biometric authentication in transforming digital security paradigms.

Integrating biometric authentication with traditional verification methods can create a robust multi-factor authentication system that significantly enhances security. This approach combines the strengths of different authentication methods, providing a more comprehensive and effective security solution. Let's explore this idea further using the example of banking verification.

Banks often deal with highly sensitive data and high-stakes transactions, making robust security an absolute necessity. However, sole reliance on traditional methods like passwords or SMS verification codes can expose users to potential risks. For instance, passwords can be easily forgotten, guessed, or stolen, while SMS verification codes can be intercepted or even socially engineered.

On the other hand, biometric authentication, which utilizes unique biological traits, offers a robust solution to these problems. Yet, while biometrics provide a high level of security and user convenience, they are not infallible. Environmental factors or technical errors can sometimes affect the system's accuracy.

To mitigate the limitations of both methods, banks can implement a multi-factor authentication system that combines traditional verification codes with biometric authentication. For instance, a user could be asked to input a password and also authenticate their identity using a fingerprint scan or facial recognition. This approach ensures that even if one factor is compromised, the other factor still protects the user's account.

From a security perspective, this combination provides an additional layer of protection. Although multiple authentications are more time consuming for the user, it is very effective for protecting important information such as finances, secrets, etc. A potential attacker would need to overcome multiple hurdles - cracking the password, intercepting the SMS code, and forging the biometric trait - to gain unauthorized access. The difficulty level of breaching such a system is considerably higher, making it a significant deterrent for potential attacks.

In conclusion, while both traditional verification codes and biometric authentication have their respective strengths and weaknesses, their integration in a multi-factor authentication system can provide a highly effective solution. Such a system capitalizes on the strengths of each method and mitigates their weaknesses, creating a significantly more secure and reliable system for user authentication.

5. Challenges and Future Prospects for Biological Validation

While biometric authentication has numerous advantages and wide-ranging applications, it is not without its challenges. Acknowledging these issues and seeking solutions is crucial for the continued

development and adoption of biometric technology. This section will explore the primary challenges associated with biometric authentication and consider the future prospects for this exciting field.

One of the main concerns with biometric authentication is the privacy and data security of the users. Biometric data, being unique and unchangeable, can have serious implications if compromised. Unlike passwords or PINs, biometric traits cannot be reset or changed. A significant risk arises from the potential for companies holding biometric data to suffer data breaches. If hackers manage to infiltrate these databases, they could gain access to sensitive biometric information of numerous individuals. Given the irrevocable nature of biometric data, a breach of this sort could have far-reaching and lasting implications. It could compromise not only the affected individual's accounts where the biometric data was used but potentially any future accounts as well, given the unchangeable nature of biometric data.

False positives and negatives present another challenge for biometric systems. A false positive, where an unauthorized individual is mistakenly granted access, can lead to security breaches. Conversely, a false negative, where an authorized individual is wrongly denied access, can impede user experience. These errors can occur due to a variety of factors, such as poor quality sensors, environmental conditions, or changes in the biometric trait due to injury or aging. Continued advancements in technology and machine learning algorithms can help improve the accuracy and reliability of biometric systems.

Another potential hurdle is the initial cost of setting up biometric systems. High-quality sensors and the necessary infrastructure for safe data storage and processing can entail significant investment. However, it is important to note that these costs are likely to decrease over time due to advancements in technology and increased market competition. In the long run, the enhanced security and improved user experience offered by biometric systems may outweigh the initial setup costs.

6. Conclusion

This paper offers an exhaustive exploration of the importance of risk analysis for text message verification codes and the role of biometric recognition technology in today's digital landscape. The discussion commences by dissecting the security risks associated with text message verification codes. This includes threats from social engineering and brute-force attacks, as well as limitations experienced by users under certain circumstances.

Subsequently, the advantages of biometric authentication are probed, emphasizing its superior security, convenience, and inherent uniqueness. Various real-world scenarios, including healthcare and workplaces, illustrate the effectiveness of biometrics in establishing secure and convenient authentication. This is particularly noteworthy when contrasted with text message verification. In addition, the amalgamation of biometrics with traditional verification techniques, exemplified in the banking industry, accentuates the potential of multi-factor authentication in fortifying overall security. By merging different authentication techniques into a cohesive system, the strengths of each method can be harnessed while mitigating their individual shortcomings, resulting in a robust and secure solution.

While acknowledging the challenges intrinsic to biometric authentication, such as privacy concerns, data security, and the costs of initial setup, the future prospects of this technology appear promising. Technological advancements, ongoing research, and evolving regulatory landscapes contribute to its continuous development. Considering the increasing dependence on digital platforms across various sectors, the requirement for sturdy, reliable, and user-friendly authentication methods is of utmost importance. In this context, biometric authentication exhibits significant potential. Despite the challenges, the undeniable benefits and continuing advancements in the field posit it as an integral component of future digital security solutions. Through sustained research and development, the application of biometric authentication has the potential to transcend current limitations, revolutionizing identity verification and access control in the digital age.

Reference

- [1] Yong, Y. (2020). Research on Technology of Finger Vein Pattern Recognition Based on FPGA. *Journal of Physics Conference Series*, 1453, 012037.
- [2] Hui, Y. (2018). Research on fingerprint image sensor technology and follow-up development. *Electronic Test*.
- [3] Oh, J., Choi, J., Moon, K., et al. (2020). Research on Implementation of User Authentication Based on Gesture Recognition of Human. In *International Semi-Cirtual Workshop on Data Science and Digital Transformation in the Industrial Revolution*.
- [4] Campione, G., Giudice, E. L., Cannella, F. (2020). Risk of failure for the salso river railroad steel bridge. *Engineering Failure Analysis*, 118, 104887.
- [5] Aidong, F., Zhiwei, Z., Lin, C., et al. (2019). Research on Speech Recognition System Based on Artificial Intelligence and Its Application. *Journal of Suzhou University*.
- [6] Ali, A. E. D. A. (2019). Research on Analysis Method of Cascading Tripping in Power Network Based on Pattern Recognition Technology. (Doctoral dissertation).
- [7] Wenxi, L., Jingjing, W., Jianqin, Z., et al. (2019). Research on high precision laser detection and recognition technology and the large passenger flow monitoring application. *Bulletin of Surveying and Mapping*, (5).
- [8] Xiang, B. I., Cunchen, T., University, W. (2019). Research on Electronic Signature Verification Based on Image Recognition Technology. *Computer & Digital Engineering*.
- [9] Xiaosong, W., Zhiqing, Z. (2018). send orders for reprints to reprints benthamscience.ae open access research on multimode biometric features recognition system adopting neural network.
- [10] Yu, Y., He, J., Zhu, N., et al. (2018). A new method for identity authentication using mobile terminals. *Procedia computer science*, 131, 771-778