CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 2
October 2024
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

Consumer Acceptance of Biometric Credit Cards as an Identify Proofing Mechanism

Laura Poe
laurapoe@verizon.net
Longwood University
Farmville, VA 23909

Abstract

Biometric credit cards have entered the marketplace as an enhancement to the chip card technology for authenticating consumers when making a purchase at a credit card terminal. Consumers using a physical credit card have the capability to provide authentication using a pre-registered fingerprint stored on the card that is compared with the fingerprint used at the time of purchase. The success of the biometric advancement will be impacted by marketplace user acceptance. Cyber vulnerabilities on biometrics through similarity-based attacks and other methods are explored in relation to the impact on consumers' data privacy. After making purchases with a test product of a biometric credit card, consumer attitudes and reactions were measured using a survey instrument to determine the acceptance of biometric credit cards in the marketplace. The results of the research indicated that overall, consumers find the biometric credit card to add to the financial security of physical credit card transactions and are not a privacy concern. This research provides a quantitative analysis of user attitudes towards fraud, reaction to biometric credit cards, and predictive analysis of consumer acceptance of biometric cards for identity proofing.

Keywords: biometrics, identity proofing, consumer attitudes, fraud.

Recommended Citation: Poe, L., (2024). Consumer Acceptance of Biometric Credit Cards as an Identify Proofing Mechanism. *Cybersecurity Pedagogy and Practice Journal;* v3 (n2) pp 4-11. https://doi.org/10.62273/JUPA7528

Consumer Acceptance of Biometric Credit Cards as an Identify Proofing Mechanism

Laura Poe

1. INTRODUCTION

Behavior-driven algorithms are commonly used for fraud detection in the financial services industry. Credit card fraud losses will total approximately $165.1 billion by 2033, impacting all age groups across the United States (Nilson, 2023). Numerous fraud detection and prevention methods exist to detect fraudulent transactions before they occur, but fraud detection models are generally considered company proprietary information, making the analysis of the various methods challenging. Regardless of the fraud detection model used, the consumer is typically blind to the process until a purchase triggers a fraud alert.

An alternative to fraud detection models are biometric credit cards that are embedded with a registered fingerprint, providing real-time authentication and identity proofing. Studies indicate a reduction in physical card fraud from 31.5% of card transactions to less than 2% when using biometric cards (Poe, 2021). While this is a significant reduction in projected fraud, the success of biometric cards will be impacted by consumers' willingness to provide biometrics on a transactional basis. Consumer-facing methods, such as signature-based purchases are not widely leveraged. The most widely used physical card authentication method was the introduction of the (Europay, Mastercard, Visa) EMV chip card, which added the additional element of security by generating a unique code for the transaction that replaces the actual card number. However, the EMV chip can be combined with additional user authentication to prevent unauthorized users from initializing the transaction. Given most credit card purchases are made with physical credit cards, the lack of adequate identity proofing is a known security gap. Leveraging biometric cards provides the benefit of both the EMV chip and a strong identity proofing mechanism. This research evaluates the user response and attitudes to biometric credit cards after using a biometric credit card for a purchase.

2. BACKGROUND AND RELATED WORK

Despite the efforts to prevent fraud through EMV chip cards and back-end fraud detection models, verifying the identity of a person at transaction initiation remains the most difficult but most important step in preventing fraud. The introduction of the iPhone 5 and the capability to lock and unlock the phone using a fingerprint was instrumental in cultural changes and the way biometric fingerprint authentication was viewed. Google Wallet and ApplePay capitalized on this feature, providing a way for financial transactions to be secured by using the fingerprint in the phone for authorization. ApplePay's growth in the marketplace shows rapidly growing consumer demand in using biometrics when performing financial transactions. Since the release of the iPhone 8, facial recognition is used to authenticate the consumer. Facebook's DeepFace, which uses a neural network approach with a high-capacity model, obtained an accuracy of 97.35% on LFW benchmark (Taigman, 2014). However, in-store purchases require a less bulky system for purchase transactions.

Financial institutions have the opportunity to capitalize on the culture shift and utilize a biometric-enabled physical credit card device to enhance the current physical card, leading to significant reductions in the amount of fraud related to counterfeit and lost/stolen cards. Mobile payments, both in-apps and in-retail stores, have been a major contributor to the adoption of biometrics. The need for authentication speed coupled with the ability to include payment authentication to contactless payments has resulted in fingerprint biometrics becoming the standard (Goode Intelligence 2015).

Leveraging biometrics for credit card purchase authentication is achieved by embedding the fingerprint into the credit card. A study previously conducted on biometric credit cards indicated 0.71% lower error rates than indicated in previous studies of fingerprint accuracy, and an overall the biometric card yielded a flat reduction in fraud of 30.5% of physical credit card fraud (Poe, 2021). While various types of

fraud detection models attempt to catch fraud as it occurs, successful identity proofing prevents the ability for a lost/stolen card to be used by an unauthorized user. The effectiveness of the biometric-enabled credit card must be greater than the overall concerns of consumers and must demonstrate the ability to prove the identity of the card holder at the time of purchase.

Digital forensics and the use of fingerprints impact the individual's privacy beyond the consumer standpoint (Kaye, 2003). The concern of privacy is further impacted by the ability to protect the fingerprint from cyberattacks during the comparison of the live fingerprint with the stored template. Similarity-based attacks, leveraging Kerckhoff's principle of public knowledge of both the function and template, the template itself is not protected and is vulnerable to attack. Based on the similarity index used in the comparison of the stored template and the actual fingerprint, a determination of authenticity is established. If the similarity index is too broad, the digital biometric can be reverse engineered, revealing the original template.

Corporate Responsibility to Consumers

Privacy protection of the data is the responsibility of the party collecting the information from the individual/consumer and are a serious concern in the design of biometric identity proofing and authentication systems. The uniqueness of the traits increases the criticality of protecting the data. When considering privacy, the value of security and convenience typically supersedes the value in safeguarding biometric data. During the authentication process, a user claims an identity by providing biometric information to a system for comparison against the stored references. In the case of surveillance applications, the process differs only that the system initiates the comparison rather than the user (Krishnan, 2012).

Companies, such as Busch Gardens and Disney Theme Parks, collect biometric data for entrance to the park in effort to track members and limit the membership fraud resulting from sharing of annual membership cards. The membership systems store the member's fingerprint data as well as photographs. Upon park entry, a member must scan the same finger each time, which is compared to the fingerprint in the system for a match. If authenticated successfully, the member gains entry into the park. Additionally, photographs of the members are stored to ensure the photograph on the account record matches the person entering the park. In these cases, the theme parks have the responsibility for storing and protecting the biometric data of their members. Their cybersecurity measures become critical components in the protection of this data.

Numerous governmental programs utilize biometric data, specifically fingerprint data, such as First Capture. First Capture is a multi-agency governmental program working to develop technology designed to capture ten rolled-equivalent fingerprints in less than 15 seconds. The focus is to ensure high quality of the fingerprint image with a device that is portable. The Integrated Automatic Fingerprint Identification System (IAFIS) contains over 47 million fingerprints and includes the electronic exchanges of fingerprints (Melodia, 2015). Governments have equal responsibility in maintaining and protecting biometric data.

3. CASE STUDY AND RESEARCH OBJECTIVES

The purpose of this study was to determine the user perception of consumers using a biometric card as a means for reducing credit card fraud and the applicability of a biometric card for the general credit card market. The study will provide specific data related to the survey of users after using a biometric credit card.

Research Methods

The study was performed by conducting a survey of 200 participants after their first-time use of a biometric credit card. The survey instrument was designed to measure the following categories: consumer perceptions of credit card fraud, ease of use of the biometric card, consumer attitudes towards risk, consumer attitudes towards identity proofing, and consumers attitudes towards privacy. The questions were divided based on these categories, but the question sequence was inconsequential and deemed to have no impact on the outcome of the responses based on the utilization of Likert scale-based questions (Weng and Cheng, 2000).

Performing the survey simultaneously with the biometric card experiment facilitated the timely capture of information while, also, providing the same participant base for both the experiment and the survey. The chances of survey participation were nearly 100%, since the survey was completed immediately following the credit card experiment. The goal of the survey was to find correlations among the categories. The survey was self-administered immediately following the successful registration of the fingerprint to the biometric credit card, a

successful purchase, and an attempted fraudulent purchase.

Each participant completed the survey, but three percent of participants were unable to successfully register their biometric card during the initial card experiment, which could result in a negative experience, reflected in the survey results.

Population and Sample

The population completing the survey consisted of a convenience sample of 200 people from a shopping mall located in Glen Allen, Virginia without regard to demographic criteria. Participants in the study were selected to use a biometric credit card and take a survey following the use of the card. The shopping location provided a strong sample of the population who would be using a physical credit or debit card and could be potential users of the biometric card.

Survey Instrument & Criteria

The survey instrument was created following Creswell's (2013) strategy for the development of a mixed methods study to incorporate the qualitative analysis with the quantitative analysis. This study focused on the consumer's attitudes towards fraud and the use of biometrics as a means to prevent credit card fraud in conjunction with the actual fraud detection rate when using the biometric card. The survey instrument was designed to measure the following categories: consumer perceptions of credit card fraud, ease of use of the biometric card, consumer attitudes towards risk, consumer attitudes towards identity proofing, and consumers attitudes towards privacy. The questions were divided based on these categories, but the question sequence was inconsequential and deemed to have no impact on the outcome of the responses based on the utilization of Likert scale-based questions (Weng and Cheng, 2000).

Performing the survey simultaneously with the biometric card experiment facilitated the timely capture of information while, also, providing the same participant base for both the experiment and the survey. The chances of survey participation were nearly 100%, since the survey was completed immediately following the credit card experiment. The goal of the survey was to find correlations among the categories. The survey was self-administered immediately following the successful registration of the fingerprint to the biometric credit card, a successful purchase, and an attempted fraudulent purchase.

The survey was categorized into five main areas to support the research objectives, Table 1: fraud perceptions, ease of use, attitude toward identity proofing, attitudes towards risk, and attitudes towards privacy. Using this criteria, previous individuals who identified as victims of fraud were evaluated as well as age categories.

Variable Name	Variable Type
Positive Fraud Experience	Dependent
Age Category	Dependent
Credit Card Ownership	Dependent
Biometric Card Device False Positive Result	Dependent
Attitude Toward Identity Proofing	Independent
Fraud Perceptions	Independent
Ease of Use	Independent
Consumers' Attitudes Toward Data Privacy	Independent

Table 1: List of Variables

Data Analysis Methods & Design

A convenience sample was used for both the biometric card experiment and the survey instrument in order to maximize participation and target brick and mortar shoppers. The results of the study may limit the transferability of results to other geographic locations. However, based on the cost of obtaining the biometric cards and the coordination with the registration of those cards by an industry subject matter expert, the convenience sample provided the most feasible solution for obtaining the data. The data analysis is unaffected by the convenience sample, although noted for informational purposes. The study was guided by research questions employing quantitative analyses through the experiment followed by survey results. External reporting provided sustainable comparisons of existing successful fraud rates for the prior two years.

The following research question was evaluated as part of the study.

RQ: Are consumers attitudes towards biometric credit cards supportive in order to reduce credit card fraud?

RO1 Evaluate the consumers' attitudes towards corporate responsibility in reducing fraud.

RO2: Evaluate the consumers' attitudes towards using a biometric credit card for purchases

4. RESULTS

Research Question: Are consumers attitudes towards biometric credit cards supportive to reduce credit card fraud?

In addition to the results of the physical biometric card experiment, the consumer perception of fraud and the biometric card is important to explore the themes and issues to be addressed by financial institutions seeking to utilize biometric credit cards as a future product. The use of closed questions, indicated by selecting a response provided by the researcher, were applied to determine categorical variables. In order to measure the consumer attitudes towards cards, the following categories were measured: attitude towards identity proofing, fraud perceptions, ease of use, and consumers' attitudes towards data privacy. These were evaluated against the following dependent variables: previous positive fraud experience, age category, credit card ownership, and the corresponding biometric card device false positive result for the participant.

A three-way ANOVA was used to determine the relationship between previous fraud experience, age, and the biometric card device false positive result from the experiment to the consumers' attitudes towards identity proofing, fraud perception, and ease of use of the biometric card. Additionally, descriptive statistics were analyzed, comparing the ease of use scores to the participants' age. Age was evaluated for statistical significance in ease of use and the perceived reduction of fraud.

Each of these data points provided quantitative evidence of the viability of biometric credit cards to provide high authenticity identity proofing and the expected future impact on the rate of successful credit card fraud transactions for lost/stolen physical cards. Additionally, the data provides statistical evaluation of the consumers' perceptions of fraud and prospective use of biometric cards.

Categorical questions were included in the survey instrument to gain the consumer's perspectives on fraud, biometrics, privacy, and corporate responsibility. Participants were asked to designate a score for each question based on the levels 1-5, as follows: 1 – mostly disagree, 2 – disagree, 3 – neutral, 4 – agree, and 5 – mostly agree. Additional demographic data, such as gender and nationality, was captured to determine a relationship to age and previous fraud victims.

In each of the five categories, the mean results were calculated based on the total participant pool of 200. The mean score was further evaluated against age and victim identity. In the first category of fraud perceptions, Table 2, the overall majority found that fraud is a growing problem but did not feel confident that current strategies in the financial services industry are successful in preventing fraud. Participants seem to be somewhat neutral when determining if banks should use biometric identity proofing for fighting fraud. The majority agreed that successful prevention of fraud increases their trust in the financial institution. Evaluating successful prevention is difficult, since most consumers are unaware of the percentage of fraud attempts blocked by financial institutions. The theme of the first section is the participants held the belief that fraud is a problem, and prevention is expected from financial institutions to earn the consumer's business.

The second category, ease of use, Table 3, demonstrated that biometrics were not cumbersome, and a slight majority found them both easy and safe. The third category focused on how the consumer views biometrics as a form of identity proofing. Most participants believe that biometrics make it more difficult for fraudsters to steal identities. At the time of this study, fingerprint and facial recognition were a method for cell phone users to make purchases using ApplePay or GooglePay. This is reflected in the comfort level of using a mobile phone's biometric for making purchases. The overall attitude towards biometrics is slightly positive.

The last two categories focused on risk and privacy. More participants believed there is increased risk in credit card fraud as compared to risk in providing biometric data in a transaction, Table 4. Participants did not find the collection of biometric data to be invasive or a violation to their privacy.

FRAUD PERCEPTIONS						EASE OF USE	
Fraud Growing Problem	Successful Strategies	Bank Selection	Use Biometrics	Fraud Trust	Prevention Trust	Biometric Cumbersome	Biometric Easy Safe
4.25	2.56	3.67	3.18	3.84	4.13	2.49	3.81

Table 2. Fraud perceptions and ease of use

ATTITUDE TOWARD IDENTITY PROOFING						
Financial Security	Biometric Decreases Fraud	Mobile	Biometric Identity	Biometric Deters	Biometric Increases Identity Theft	Biometrics Use Stolen Identities
3.59	3.60	3.90	3.84	3.40	2.57	3.85

Table 3. Consumer attitudes towards biometrics

ATTITUDE TOWARD RISK						ATTITUDE TOWARD PRIVACY
Consumer Comfort	Consumer Comfort Mobile	institution Trust Bio Data	Biometric Risks	Bio Less Risk Fraud	Back-Up Verification	Biometric Invasive
3.71	3.59	2.27	3.35	2.93	3.97	2.63

Table 4. Consumer attitudes towards risk and privacy

To evaluate the consumers' attitudes towards corporate responsibility in reducing fraud, a multivariate analysis of variance (MANOVA) test was performed to determine the relationships between age, victims of fraud, attitudes towards credit card bank selection based on a company's ability to combat fraud, and attitudes towards recommending that companies use biometrics as a means of identity proofing for preventing fraud. The solid distribution between age categories and fraud victims allowed for an analysis by each age group and victim category.

Further analysis through Box's test of equality of covariance proves statistical significance of age and victims of fraud with corporate responsibility for fraud prevention and utilizing biometrics. Levene's test, Table 3, supports the results of Box's test with statistically significant results. Ages 18-24 and 45-54 had the highest scores of Agree to Strongly Agree that fraud prevention tactics by a company were crucial in selecting a bank. Regardless of fraud victimization, the outcomes of the analysis postulate that a bank's ability to prevent fraud is important in the selection of a financial institution for obtaining a credit card. However, the lack of a statistical relationship between age and selection of a financial institution ruled out any predictive relationship. The overall results remain an indicator that nearly all age groups found fraud prevention a consideration in credit card company selection.

RO2: Evaluate the consumers' attitudes towards using a biometric credit card for purchases.

The majority of participants who were victims of fraud held a positive attitude towards using biometrics for identity proof during credit card purchases. A linear regression analysis was performed to analyze only the relationship between fraud victims and attitudes towards using biometrics for identity proof during credit card purchases. The relationship between those who think fraud is a growing problem to biometrics as a deterrent was statistically significant. Removing the variable fraud victim allowed for more targeted calculations to determine if a predictor relationship exists. The R square of fraud victims was not high enough to substantiate a predictor relationship.

Nearly unanimously, respondents believed that biometric cards are easy and safe to use for making a purchase transaction. However, respondents were not as agreeable to requiring biometric data as part of a credit card application. The resistance was not in providing biometric data but more focused on capturing the biometrics during the application process. In this study, no credit card application was required to register and use the card.

The majority of the participants responded in disagreement that requiring the biometric print during the application process would be too cumbersome. Recognizing the user's perception of the level of difficulty using the biometric card is essential to determine the influence between the user's perception and the marketability of the card. As a sample population of credit card holders, the level of resistance to using credit cards based on any complexity with capturing fingerprints seems minimal in impact. Organizations can, however, focus on reducing the impact to card holders by developing a seamless registration process and potentially utilizing devices that allow consumers to register cards from their own homes.

More than half of respondents had experienced some form of credit card fraud. However, recommendations to use biometrics as a means for fraud prevention remained neutral, eliminating a causal relationship between the two variables. When evaluating demographics, age was a significant factor in relation to biometrics as an invasion of privacy. Participants over the age of 45 had privacy concerns on the collection of biometric data, though they felt that fraud was a growing problem, and the requirement of a fingerprint would lead to reduced numbers of fraud occurrences.

Concerns over personal privacy were addressed as part of the survey, and overall, participants did not feel that a biometric credit card violated their privacy. The 35-44 age group were neutral on privacy, and the age categories of 18-24, 25-34, and 45-54 equally disagreed on the question addressing "requiring biometric fingerprint data is invasive and violates the right to privacy". While ages 35-44 were neutral on privacy, they disagreed that risks involved in providing fingerprint data are less than the risks of fraud. The 45-54 age group felt different and agreed that risks of using biometric data were less than the risk of fraud. The younger group, from 18-34 were neutral, indicating they did not believe the biometrics were any riskier than existing chances of fraud.

5. CONCLUSIONS

The purpose of this study was to evaluate the viability of the biometric credit card by exploring the perceptions and attitudes of consumers towards using biometrics for identity proofing during a credit card transaction. The study provided evidence of consumer's acceptance of the biometric credit card. In general, consumers feel that fraud is a growing problem and believe that using biometrics will result in credit card fraud reduction. Biometric cards were found to be easy to use and more secure than current means of authentication. Numerous statistical analyses were performed to determine the relationship between fraud victims and biometrics as well as age and biometrics. Linear regression analyses were performed as well as a multivariate analysis to determine predictability associations.

The survey conducted gathered data for understanding consumers' attitudes towards fraud and using biometrics to combat fraud. The study was further evaluated based on age group and consumers who had or had not experienced credit card fraud. Fraud victims believe fraud is a growing problem and are more likely to believe that biometrics should be used to combat fraud. Consumer perceptions were measured based on age category for fraud prevention tactics. Ages 18-24 and 45-54 had the highest scores of Agree to Strongly Agree that fraud prevention tactics by a company were crucial in selecting a bank. Those who believe fraud is a growing problem believe biometrics reduce fraud. Little resistance to biometrics could be found, as nearly all participants responded in favor of biometrics for identity proofing and declared a biometric card as easy to use. All age groups found a company's approach to and guarantee of fraud protection and prevention important when selecting a credit card. The ease of use with the biometric card was reflected in the survey responses by the participants.

The results of this study are applicable to biometric card industry in determining user acceptance and usability for implementing biometric credit cards into the marketplace. Additionally, the results provide further evidence of the market demand for enhanced security measures for the banking and financial industry.

6. RECOMMENDATIONS FOR FURTHER STUDY

The survey was conducted as a joint experiment with the biometric credit card. The conjoining of these two aspects of the study did not allow for survey respondents who had never seen or experienced a biometric credit card and could have concluded differing results. Additionally, the participants in the study opted to take part based on their interest in biometrics. Those uninterested in utilizing biometric cards were more unlikely to participate, creating some level of bias. The bias created an inherent limitation to the survey results. Future research could be conducted from a random sample of participants with no knowledge or experience using biometric credit cards. Place before the references.

7. REFERENCES

Goode Intelligence. 2015. Biometrics for Banking; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020. Retrieved from http://www.goodeintelligence.com/report-store/view/biometrics-for-banking-market-technology-analysis-adoption-strategies-forecasts-20152020

Kaye, D. (2003). *The Nonscience of Fingerprinting: United States v. Llera-Plaza*. Retrieved from Law Review Library: https://www.qu.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/43_21QLR1073(2001-2003).pdf

Krishnan, A. P., & Sy, B. K. (2012). SIPPA-2.0 – Secure Information Processing with Privacy Assurance (version 2.0). *Tenth Annual International Conference on Privacy, Security and Trust*, 25-34.

Melodia, M., Bond, P., & Angelovska-Wilson, A. (2015). Legal Risks and Rules of the Move to Biometrics. *New York Law Journal*, 1-2.

Nilson Report. (2023, April) *Acquisitions and Financing Deals in Payment Cards—2022.* Retrieved April 18, 2023, from https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1239#

Papadimitriou, O. (2015, October 17). *Where Does Apple Pay Stand On Its First Birthday*. Retrieved from Tech Crunch: http://techcrunch.com/2015/10/17/where-does-apple-pay-stand-on-its-first-birthday/

Poe, Laura F. (2021) Case Study: Empirical Evaluation of a Biometric Credit Card for Fraud Reduction, *Cybernetics and Systems*, DOI: 10.1080/01969722.2021.2005873

Spraggs, D. (2007, February 1). *How to Lift Fingerprints*. Retrieved March 27, 2018, from

http://www.policemag.com/channel/patrol/articles/2007/02/how-to-lift-fingerprints.aspx

United States Census Bureau. (2017, July 1). *Quick Facts United States.* Retrieved 17 November, 2018, from https://www.census.gov/quickfacts/fact/table/US/PST045217.

Weng. L-J., & Cheng, C-P. (2000). Effects of Response Order on Likert-Type Scales.

Educational and Psychological Measurement, 60 (6). 908-924.

Y. Taigman, M. Yang, M. A. Ranzato and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification", *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1701-1708, 2014.

X. Dong, Z. Jin and A. T. B. Jin, "A Genetic Algorithm Enabled Similarity-Based Attack on Cancellable Biometrics," *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Tampa, FL, USA, 2019, pp. 1-8, doi: 10.1109/BTAS46853.2019.9185997.