Experiments on the Cyrillic handwritten dataset show that the proposed method is better than the original model in a number of key indicators: lower training and validation losses, faster learning, and stronger generalization ability. The recognition accuracy is higher, which verifies the effectiveness of data enhancement and targeted training. Although the initial time is increased due to pretreatment, the overall training efficiency is better.

References

1. Very deep convolutional networks for large-scale image recognition / K. Simonyan, A. Zisserman. – 2015.

2. Baek, J. Dataset and Model Analysis. – 2019.

3. Graves, A. IEEE transactions on pattern analysis and machine intelligence. – 2008.

УДК 004, 656.8, 336.7

SECURITY METRICS AND COUNTERMEASURES FOR NFC PAYMENT TECHNOLOGY

Liu W., Balukho I. N., Kolchevsky N. N.
Belarusian State University
E-mail: weil48384@gmail.com, iren.balukho@gmail.com, kolchevsky@gmail.com

Summary. *In recent years, Near Field Communication (NFC) technology has been widely applied in the field of modern payment systems. However, in practical applications, NFC technology is vulnerable to attacks such as eavesdropping, data tampering, data corruption, cloning, and phishing, which can lead to the leakage of users' private data and pose serious threats to financial information and the security of users' assets. This article outlines the potential information security risks faced by NFC payment technology and the future technological developments aimed at ensuring information security.*

With the surge in the number of people using mobile payments, its security vulnerabilities are continuously being discovered, while new viruses and technical fraud methods are constantly emerging. Given the characteristics of mobile payments, the threats they face are also unique, including the following:

Data Confidentiality. During the transmission of user information, if no encryption measures are taken, unauthorized attackers may intercept the transmitted data and access the legitimate user's confidential information, such as bank account numbers and payment passwords.

Data Integrity. It ensures that authentic information remains complete and unaltered when transmitted from the sender to the legitimate recipient. This prevents the data exchanged between buyers, sellers, and the payment processing platform from being tampered with, inserted, deleted, or otherwise compromised.

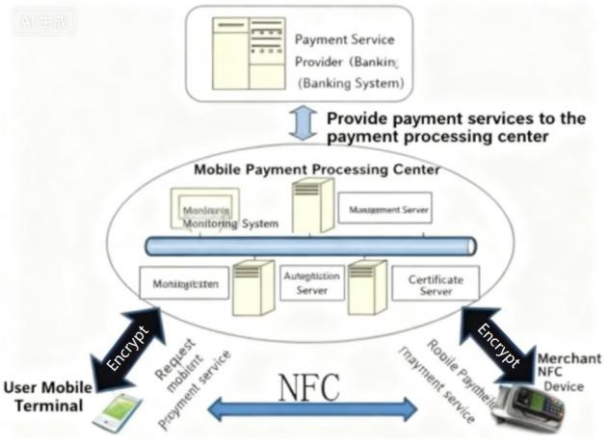

Figure 1 – Simple Architecture of an NFC Mobile Payment Processing Security System

Non-repudiation of Data. It ensures that all information exchanged during the transaction process between buyers and sellers is supported by irrefutable records, preventing either party from denying the information they have sent or received.

To safeguard data security during the NFC mobile payment process and authenticate the identities of different modules, devices, or roles involved in the transaction, it is essential to address the security threats within NFC systems and meet the safety requirements of the payment ecosystem. The following security technologies are primarily adopted in authentication schemes:

Public and Private Key Cryptography System: This system utilizes encryption algorithms to generate a key pair – a public key and a private key. The public key is openly accessible and can be viewed by anyone, while the private key remains confidential and is known only to its owner. The public key is typically used for encrypting session data and verifying digital signatures.

Digital Signature: A digital signature is the digital equivalent of a handwritten signature, representing the identity of the signer. Its key characteristics are that generating a signature is straightforward, while forging one is extremely difficult.

Anonymization: During transactions, customers use pseudonyms or virtual IDs, while their real identity information is known only to the bank or a trusted authentication platform.

Hybrid AES and ECC encryption algorithm: The AES algorithm offers relatively fast data encryption and decryption processes, making it more efficient for payment systems with smaller data volumes. In contrast, the ECC algorithm provides stronger security but operates at a slower encryption speed. By combining the strengths and weaknesses of both algorithms, a hybrid encryption approach integrating AES and ECC is adopted. During data transmission, the data in NFC mobile payments is encrypted using the AES algorithm, while the AES key is encrypted and managed using the ECC algorithm. During decryption, the AES key is first retrieved by decrypting the ECC-encrypted key, after which the data is decrypted using the obtained AES key.

References

1. NFC Reader/Writer Reference Design (TIDM-NFC-RW): pat. TI DM-NFC-RW / Texas Instruments (TI). – TRF7970A Transceiver Development Team. – Publ. date 12.11.2025.

2. Near Field Communication Interface and Protocol (NFCIP-1): pat. ISO/IEC 18092:2023 / International Organization for Standardization (ISO). – International Electrotechnical Commission (IEC). – Publ. date 2023 (Replaces ISO/IEC 18092:2004).

3. The NFC Forum's Latest Usage and Adoption Survey Conducted by ABI Research Reveals Growing Reliance on Mobile Payment Wallets and Priorities for Future Innovation: rep. ABI Research. – ABI Research Team (Lead Researchers: Sarah Quinlan, Andrew Zignani). – Publ. date 17.04.2024.

4. NFC technologies for identification and contactless payment / W. Liu, I. N. Balukho, N. N. Kolchevsky // Applied Problems of Optics, Computer Science, Radiophysics, Aerospace Technologies, and Condensed Matter Physics: Proceedings of the 8th International Scientific and Practical Conference, May 22–23, 2025, Minsk / Ministry of Education of the Republic of Belarus, A. N. Sevchenko Research Institute of Applied Physical Problems, BSU; P. V. Kuchinsky (Chief Editor) [et al.]. – Minsk: StroyMediaProekt, 2025. – P. 296–297.

УДК 004.932.2

COMPARISON OF ORB AND SIFT METHODS UNDER THE SLAM FRAMEWORK

Qiyao Yang, Qinghan Yu, Jun Ma
Belarusian State University of Informatics and Radioelectronics
E-mail: a1002112732@gmail.com

***Summary**. This paper presents a comparative study of ORB and SIFT feature matching methods under the SLAM framework. Both algorithms were implemented and tested on identical image sets to evaluate their performance from multiple classical perspectives, including feature distribution, robustness to illumination and rotation, matching accuracy, and computational efficiency. By analyzing both qualitative and quantitative results, this study aims to provide insights into algorithm selection and optimization for real-time visual SLAM systems.*

In visual SLAM [1] (Simultaneous Localization and Mapping), feature extraction and matching algorithms play a vital role in determining the overall accuracy, robustness, and computational speed of the system. Feature-based methods rely on keypoint detection and descriptor matching to track the motion of the camera across frames. Among the many feature detectors available, ORB (Oriented FAST and Rotated BRIEF) [2] and SIFT (Scale-Invariant Feature Transform) [3] represent two of the most widely used approaches. SIFT is known for its robustness and invariance to scale, rotation, and illumination changes, while ORB is a fast, binary alternative optimized for real-time applications. This study aims to provide a systematic comparison between ORB and SIFT in the context of SLAM front-end feature processing.