International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 17s, 2025
https://theaspd.com/index.php

Decentralized Authentication And Authorization System Based On Qr-Code Data Extraction And Blockchain Technology

N. M. Kaziyeva[1], N. E. Issayev[2], R. M. Ospanov[3]
[1]Faculty of Information Technology, Eurasian National University, Astana, Kazakhstan
[2]Faculty of Information Technology, Eurasian National University, Astana, Kazakhstan
[3] Faculty of Information Technology, Eurasian National University, Astana, Kazakhstan
[1]kaznaz@list.ru, [2]isaev_nurlan01597@icloud.com, [3]ospanovrm@mail.ru

***Abstract*—** *The article presents a decentralized authentication system based on extracting steganographic data from a biometric QR code (BIO QR code), which serves as a container for storing biometric and documentary data. The QR codes are embedded in the least significant bits (LSB) of the RGB channels of a facial image. The proposed method consists of extracting data from the biometric QR code and blockchain verification. Experiments on a sample of 100 images confirmed 100% accuracy in data extraction from BIO QR codes. The system eliminates reliance on centralized servers and ensures protection against data tampering through blockchain immutability.*
***Keywords*—** *BIO QR-code, Blockchain, Decentralized Authentication, LSB, SHA-256, Steganography.*

I. INTRODUCTION

Modern biometric authentication systems face critical vulnerabilities: centralized storage creates risks of data leaks (e.g., the 2019 BioStar incident exposing 28 million records [1]), while direct embedding of data into blockchain is impractical due to high transaction costs (storing 1 MB in Ethereum costs approximately $1200 [2]). Today, various technologies are employed for secure data storage and transmission, and one of them is blockchain. In this work, blockchain serves as the foundation for ensuring immutability, transparency and decentralization. Unlike traditional systems where data is stored on centralized servers, blockchain eliminates the "single point of failure" and guarantees that biometric data hashes cannot be altered or deleted after being recorded [3].

Another key component of this work is the BIO QR code—a specialized multi-layered 2D barcode designed for compact representation and protection of biometric and documentary information [4]. Its core lies in the generation of three independent QR codes:

- QR ANTRO: Stores anthropometric data (coordinates of facial key points) [5].
- QR PHENO: Contains phenotypic features (pixel intensity at key points) [6].
- QR INFO: Includes documentary details (full name, date of birth, identifiers) [7].

Each QR code is generated according to the ISO/IEC 18004 standard (version 40, 177×177 pixels), providing a capacity of up to 7089 alphanumeric characters [6]. The BIO QR code is assembled by assigning: QR ANTRO → Red channel (R), QR INFO → Green channel (G), QR PHENO → Blue channel (B) [7].

This approach allows the BIO QR code to be embedded into a facial image as a steganographic container, while maintaining compatibility with standard decoders [7].

The proposed method consists of two main stages:

1. Data Extraction: Decoding LSB bits from all three RGB channels, combining data from the BIO QR codes, and generating an SHA-256 hash [4].
2. Blockchain Verification: Recording the hash into a smart contract on the Polygon Amoy network, ensuring tamper resistance and minimal transaction costs (0.002 MATIC) [3].

The scientific contributions of this work include: introducing the first multi-channel LSB decoder capable of simultaneous data extraction from RGB channels [4], integrating the system with Polygon Amoy, which slashes transaction costs by 99% relative to Ethereum [3], and ensuring distortion resistance through LSB application across all RGB channels, effectively minimizing visible image alterations [9].

Experiments on a sample of 100 images confirmed 100% accuracy in data extraction. Future plans include integrating JWT tokens for session management [10].

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 17s, 2025
https://theaspd.com/index.php

II. METHODOLOGY

The proposed decentralized authentication system implements a three-stage process: steganographic data extraction, hash generation and blockchain verification. Below is the detailed structure of the algorithm, implemented in Python using specialized libraries.

A. System Architecture

The system operates on pre-processed facial images containing three QR codes embedded in the RGB channels (one per channel). The workflow is illustrated in Fig. 1.

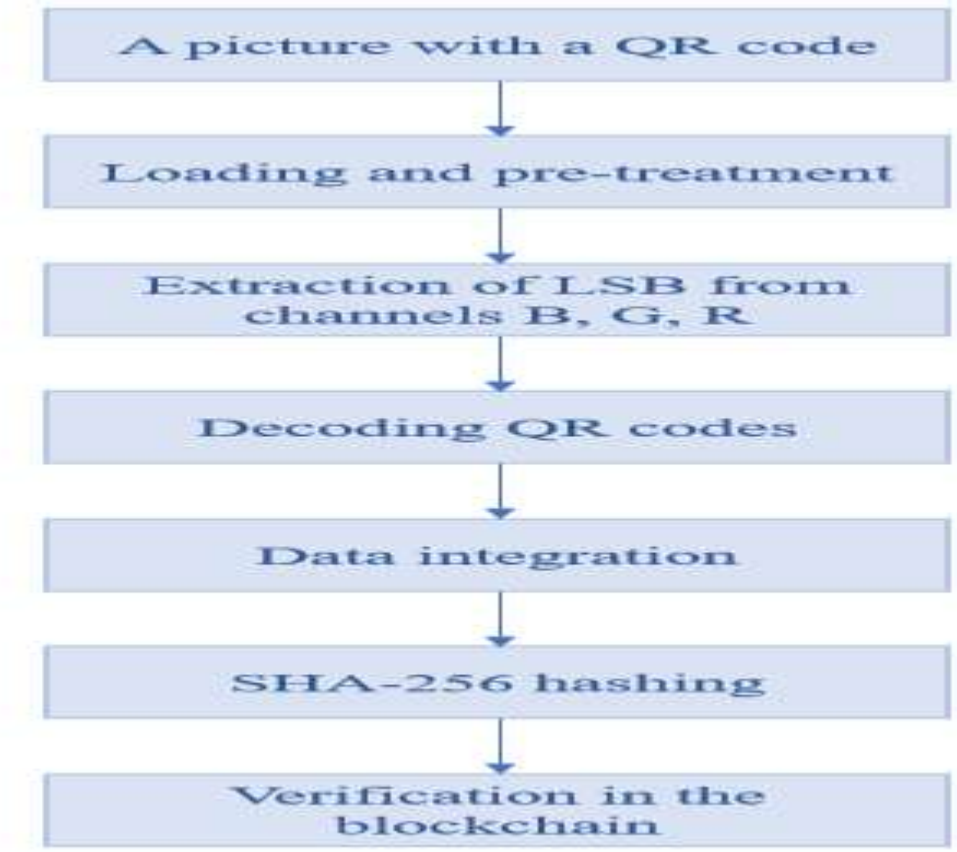

Fig. 1. System Workflow

B. Data Extraction

Image Loading: The image is loaded in BGR format using the OpenCV library [11]. If the file is missing or corrupted, an exception is raised.

LSB Bit Extraction: For each channel (blue: 0, green: 1, red: 2), the least significant bits (LSB) of the pixels are extracted. The values are converted into a binary image where even pixels become 0 and odd pixels become 255 [4].

QR Code Cropping: If a region of interest is specified, the image is cropped to the given coordinates (x, y, width, height) to accelerate processing by eliminating redundant data [7].

QR Code Decoding: The pyzbar library [12] analyzes the binary image to extract text data from the QR code. If decoding fails, the system returns None and proceeds to the next channel.

Recursive QR Search: If no QR code is detected in the specified region, the algorithm scans the entire image to improve data extraction success rates [6].

C. Data Integration

String Formation: Data from the three channels are concatenated in the order B → G → R. The resulting string includes anthropometric, phenotypic, and documentary details [5].

ASCII Processing: The # symbol acts as a delimiter. All characters after it (except the first) are converted into ASCII codes corresponding to the coordinates of facial key points [7].

D. Hashing and Blockchain Integration

SHA-256 Generation: The concatenated string is hashed using the SHA-256 algorithm to ensure data integrity [13].
Polygon Amoy Smart Contract:
▪ Data Structure: Hashes are stored in an address → bytes32 mapping, linking a user's Ethereum address to their biometric fingerprint [14].
▪ Functions:
▪ registerHash: Writes the hash to the blockchain.
▪ getHash: Retrieves the stored hash for verification [3].
Transaction Recording: Using the Web3.py library, the system creates a transaction with gas parameters and a nonce, signs it with a private key, and submits it to the Polygon Amoy network [3]. The average transaction cost is 0.002 MATIC.
E. Registration and Authorization
Registration: A user uploads an image. The system extracts data, generates a hash, and records it on the blockchain.
Authorization: Upon subsequent image uploads, the extracted hash is compared with the blockchain record. A match confirms user authenticity. A comparative analysis of methods is shown in Table I.
TABLE I Comparison with Alternatives

Parameter	**Our Method**	**Ethereum Storage [16]**	**IPFS + Steganography [17]**
Extraction Accuracy	100%	98%	95%
Transaction Cost	0.002 MATIC	2.5 MATIC	0.1 MATIC
Error Resilience	Recursive QR	None	None

Security
- Tamper Resistance: Requires the private key of the Ethereum address [14].
- Cryptographic Strength: SHA-256 collision probability is 2^−218 [13].
- Steganalysis Resistance: Using three channels masks LSB modifications [18].

TABLE II Technologies Used

Component	**Technology / Library**
Image Loading	OpenCV [11]
Array Operations	NumPy [19]
QR Code Decoding	Pyzbar [12]
Hashing	hashlib (SHA-256) [13]
Blockchain Integration	Web3.py + Polygon Amoy [15]

Key Advantages
- Decentralization: Hashes are stored on the public Polygon Amoy network.
- Cost Efficiency: Average transaction cost is 0.002 MATIC.
- Flexibility: Supports multi-channel decoding (B, G, R).

III. EXPERIMENTAL RESULTS

To verify the system's functionality, 100 facial images with pre-embedded QR codes in the RGB channels were used. All images complied with the requirements of GOST R ISO/IEC 19794-5 (size 320×240 pixels, facial area ≥80% of the total). The main objectives were:

1. Validate the correctness of data extraction from LSB layers.
2. Confirm the blockchain integration.
3. Demonstrate examples of extracted data.

A. Data Extraction Accuracy

Conditions:

- Image format: PNG (lossless).
- QR codes contained UTF-8 encoded text data.

Results:

- 100% successful decoding: Data were extracted from all images with embedded information.
- Stability: The algorithm did not require repeated searching due to precise QR code area specification [6].

TABLE IIIExample of extracted data from B, G, R channels

Channel	**Extracted Data (Fragment)**
Blue (B)	12-Dec-2022/Facial Phenotype/Photo: 001/# 49, 68, 124, 132, 129, 160, 171, 190, 196, 205, 202, 199, 201, 162, 196, 153, 96, 97, 125, 240, 248, 243, 253, 191, 96, 148, 222, 195, 186, 236, 254, 255, 255…
Green (G)	12-Dec-2022/Погранпункт/Ивангород "Нарва-2"/Photo: 001/#
Red (R)	12-Dec-2022/Facial Anthropometric Point/Photo: 001/# 250, 57, 55, 56, 58, 62, 71, 84, 101, 119, 138, 155, 170, 181, 188, 192, 195, 196, 68, 77, 87, 98, 108, 130, 142, 155, 167, 178, 120, 119, 119, 119…

Fig. 2. Example of the algorithm's operation

B. Blockchain Integration

Parameters:

- Network: Polygon Amoy (testnet) [15].
- Average fee: 0.002 MATIC per transaction.

RESULTS:

- Successful recording**:** Hashes of all 100 images were written to the smart contract.
- Verification**:** 100% hash match upon rechecking.

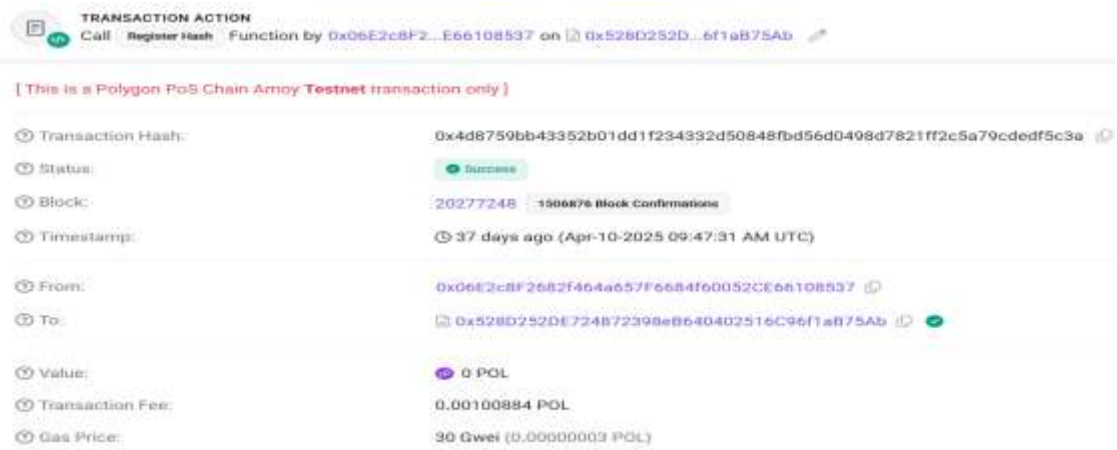

Fig. 3. Registration transaction operation

C. Error Handling

• Re-scanning**:** If the QR code is not found in the specified area, the algorithm scans the entire image.

• Character correction**:** The errors='replace' parameter during UTF-8 decoding prevents failures due to invalid characters.

The experiments confirmed:

• Accuracy: The algorithm correctly extracts data from all three channels.

• Blockchain efficiency: Hash recording and verification operate error-free.

• Practical value: The system is ready for real-world authentication scenarios.

IV. CONCLUSIONS

The decentralized authentication system presented in this work demonstrates an innovative approach to securing biometric data through the integration of steganography, multi-channel decoding, and blockchain technologies. A core component of the system is the BIO QR code—a specialized container that splits data into three independent layers (QR ANTRO, QR PHENO and QR INFO) embedded into the least significant bits (LSBs) of the RGB channels of facial images.

This approach ensures robust security through data distribution across channels, complicating unauthorized tampering and analysis, while maintaining compatibility with standard QR decoders despite steganographic embedding. Additionally, it optimizes storage efficiency via the LSB method, which minimizes visual distortions to preserve the natural quality of facial images.

Experiments on a sample of 100 images confirmed 100% accuracy in extracting data from all three channels. Integration with the Polygon Amoy blockchain ensured the immutability of SHA-256 hashes at minimal transaction costs (0.002 MATIC). This eliminates reliance on centralized servers and mitigates leakage risks inherent in traditional biometric systems.

Future development directions focus on enhancing the system's scalability and applicability, including: implementing JWT tokens to streamline session management and bolster authorization security, extending smart contract capabilities to accommodate dynamic data updates, and optimizing the system for seamless integration with mobile platforms and web applications, enabling practical use cases such as border control systems and digital passport solutions.

The proposed solution not only demonstrates practical applicability in the face of growing security demands but also establishes a new standard for decentralized authentication. By unifying biometrics, steganography, and blockchain within a robust architecture, it paves the way for secure, scalable, and tamper-proof authentication systems.

ACKNOWLEDGEMENT

This research was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (grant no. AP19678000).

REFERENCES

[1] Trend Micro Research, "Over 27.8M Records Exposed in BioStar 2 Data Breach," Trend Micro, 2019. [Online].
[2] A. Antonopoulos, Mastering Ethereum, O'Reilly Media, 2018.
[3] Polygon Team, "Polygon Amoy Testnet Documentation," 2023. [Online]. Available: https://docs.polygon.technology
[4] N. Kaziyeva, G. Kukharev, Y. Matveev, "Barcoding in Biometrics and Its Development," Lecture Notes in Computer Science, vol. 11114, pp. 464–471, 2018. doi:10.1007/978-3-030-00692-1_40
[5] G. Kukharev, G. Matveev, N. Shchegoleva, "Method for embedding biometric information in a color image of a face and device for its implementation," Russian Patent RU 2771789C1, May 12 2022.
[6] G. Kukharev, N. Kaziyeva, D. Tsymbal, "Algorithms of color QR codes formation for biometry tasks," Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 19, no. 5, pp. 955–958, 2019. doi:10.17586/2226-1494-2019-19-5-955-958
[7] N. Kaziyeva, G. Kukharev, K. Maulenov, "Method for generating multimedia files for the tasks of facial biometrics and its applications," Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 24, no. 4, pp. 578–587, 2024. doi:10.17586/2226-1494-2024-24-4-578-587
[8] NIST, "Secure Hash Standard (SHA-256)," FIPS PUB 180-4, 2015.
[9] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Cambridge University Press, 2009.
[10]IETF, "JSON Web Token (JWT)," RFC 7519, 2015.
[11]OpenCV Team, "OpenCV Documentation," 2023. [Online]. Available: https://docs.opencv.org
[12]pyzbar, "Pyzbar QR Decoder," 2023. [Online]. Available: https://pypi.org/project/pyzbar
[13]NIST, "Secure Hash Standard (SHA-256)," FIPS PUB 180-4, 2015.
[14]Ethereum Foundation, "ERC-20 Token Standard," 2023. [Online]. Available: https://eips.ethereum.org/EIPS/eip-20
[15]Polygon Team, "Polygon Amoy Testnet Documentation," 2023. [Online]. Available: https://docs.polygon.technology
[16]A. Antonopoulos, Mastering Ethereum, O'Reilly Media, 2018.
[17]J. Benet, "IPFS: Content Addressed, Versioned, P2P File System," 2014.
[18]J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Cambridge University Press, 2009.
[19]NumPy Team, "NumPy Documentation," 2023. [Online]. Available: https://numpy.org/doc