A Steganographic Data Transmission Framework Using Legal Chess Move Sequences

Yashika Aggarwal
Department of Computer Engineering
Bharati Vidyapeeth's College of Engineering, Lavale
(Affiliated to SPPU)
Pune, India
yashika.aggarwal05@gmail.com

Abhishek Bharajkar
Department of Computer Engineering
Bharati Vidyapeeth's College of Engineering, Lavale
(Affiliated to SPPU)
Pune, India
abhishekbharajkar22@gmail.com

Rohan Ambhore
Department of Computer Engineering
Bharati Vidyapeeth's College of Engineering,Lavale
(Affiliated to SPPU)
Pune, India
rohanambhore7@gmail.com

Siya Shaikh
Department of Computer Engineering
Bharati Vidyapeeth's College of Engineering, Lavale
(Affiliated to SPPU)
Pune, India
Siyashaikh1212@gmail.com

Yogesh Kadam
Department of Computer Engineering
Bharati Vidyapeeth's College of Engineering, Lavale
(Affiliated to SPPU)
Pune, India
yogesh.kadam@bharatividyapeeth.edu

Abstract— **The new data transmission and storage system project is presented in this work. It converts encrypted binary data into a series of legitimate chess moves that may be played between bot accounts on the open-source Lichess.org chess platform. This project uses game logs to facilitate low-profile, decentralized file sharing by utilizing the move structure of a chess game and the public availability of Lichess game records. The system opens up conversations about subversive computing and innovative usage of digital platforms while showcasing the useful intersection of steganography, cryptography, and limited media encoding.**

Keywords—Steganography,Cryptography,LitchessGame, Cloud Storage,Binary Data

I. INTRODUCTION

The need for privacy-preserving and non-traditional data transmission methods has increased due to the development of digital surveillance, censorship, and platform moderation. Conventional steganographic methods frequently use media format redundancy to obfuscate content by embedding data into pictures, movies, or audio files[7][8]. A radically different method is presented in this paper: using structured, rule-constrained systems, namely chess games, as a transmission medium. The project encodes binary data as series of valid chess moves in order to provide a way for embedding and extracting arbitrary files.

The well-known online chess platform Lichess.org provides a low-latency, high-availability environment where users can retrieve previous games using PGN (Portable Game Notation). This makes it the perfect medium for decentralized storage, particularly when combined with bot accounts that can play games that are encoded with data automatically. Files encoded as games can be kept on the platform indefinitely without drawing notice because they are indistinguishable from regular matches.

The design and implementation of such a system are thoroughly examined in this work, together with the automation infrastructure, cryptographic strategy, encoding technique, and possible uses[3]. We also take into account this method's wider ramifications, including its potential for digital activism, censorship resistance, and the conceptual repurposing of play spaces for computational purposes.

II. RELATED WORK

Information concealment in restricted rule-based systems is not a completely novel concept. From antiquated techniques like invisible ink to contemporary digital approaches, steganography has a long history. Digital steganography frequently uses methods like least significant bit (LSB) manipulation to embed data in media like MP3 audio files or JPEG images. Nevertheless, these techniques typically presume redundancy in the exploitable data format. Data concealing in chess games is a special difficulty since each data point (move) has great semantic meaning and little redundancy[10].

Furthermore, encoding data under structural constraints (such DNA storage or modulation in telecommunications) is the focus of the information theory field of restricted encoding. Similar ideas are used by Project, but in the context of game mechanics. The theoretical foundations of this research are informed by the work of Anderson et al. (1998) on "The Steganographic File System" and more current investigations into "network steganography."

Additionally, there is history for the use of games and other structured systems as data conduits in situations such as exfiltration and infection[9]. Chess as a message-hiding medium has been investigated through projects like code-based CTF challenges and ChessSteg, a hypothetical tool that was presented but never made public. None, though, have put in place a full pipeline that integrates with public platforms, has file-size scalability, and is secure by cryptography.

By integrating game integrity, data encryption, multi-game chaining, and live public distribution through bots, Project sets itself apart and pushes the theoretical and practical limits of steganographic systems.

III. METHODOLOGY

By integrating game integrity, data encryption, multi-game chaining, and live public distribution through bots, project sets itself apart and pushes the theoretical and practical limits of steganographic systems.

A. *System Requirements and Architecture Design*

Among the primary design specifications were:

- Absence of a central server for file retrieval or storage.
- Using only Lichess game IDs for stateless transmission.
- Support for the contents of encrypted files
- Completely reversible file-to-game and game-to-file conversion

These served as the foundation for the design of a modular architecture that included a decoder, two Lichess-integrated bot agents, and an encoder. To ensure portability and scalability, each module was constructed using Python 3 as a stand-alone component.

B. *Data Encoding and Encryption*

The technology transforms files in two steps in order to integrate them within a chess game:

- **The Encryption**: Using a user-supplied key, input files are encrypted using AES-256 (with CBC mode). This prevents inference about the nature or structure of the file by guaranteeing that the resultant data cannot be distinguished from random noise.
- **Encoding**: Based on the current board condition, each short, fixed-size chunk of encrypted binary data—usually 4–6 bits—is mapped to a legitimate chess move. At every ply (half-move), a dynamic move dictionary is created instantly, enabling the mapping to change as the game progresses.
- Particular focus was placed on keeping the game legal at all times while maintaining encoding and decoding logic synchronisation.

C. *Game Transmission via Lichess Bots*

The OAuth tokens were used to establish and authenticate two Lichess bot accounts. The Lichess API is used by these bots to:

- Track requests for file uploads.
- Start a match between them.
- Real-time playback of the moves that match to the encoded file.

The OAuth tokens were used to establish and authenticate two Lichess bot accounts. The Lichess API is used by these bots to:

- Change the time of your moves at random.
- Start with "natural-looking" or well-known openings.
- Use legal, non-data-carrying "dummy" motions for obfuscation occasionally.

The Approximately 1-2 KB of data are encoded by each game. The encoder automatically links several games together for larger files, adding metadata to each game's beginning sequence to specify its order and continuation flag.

D. *File Retrieval and Decoding*

A user must supply the original encryption key and the Lichess game ID (or list of IDs for multi-game files) in order to recover a file. The module for decoding:

- Utilizes the Lichess API to download the PGN(s).
- Reconstructs the sequence of moves.
- Extracts the encrypted binary stream by reversing the encoding.
- Uses AES-256 to decrypt the stream and create the original file.

IV. ENCODING TECHNIQUES AND CRYPTOGRAPHIC CONSIDERATIONS

The most important and technically complex feature of Project is its ability to encode binary data into legitimate chess moves. Mapping a stream of binary data onto a dynamic, legally confined place is the main challenge. The set of permitted movements at each ply is determined by the current board state, which serves as the encoding dictionary. There may be 20–40 permissible moves for a typical mid-game position, with optimal circumstances permitting up to 5 bits per move.

To boost dependability and capacity:

- Positions with greater branching factors are given priority by the encoder.
- Early encoding entropy is constructed using opening sequences.
- To keep things consistent, moves are occasionally repeated or padded with no-op equivalent moves (such as back-and-forth bishop shifts).

Before encoding, encryption is used to make sure that a key is needed for decoding and to stop file structures from skewing the distribution of moves. AES-256 is utilized in CBC mode with a random IV that is incorporated into the game's initial moves. The resultant encrypted file generates an unbiased move distribution since it cannot be distinguished from random noise.

By combining encryption, encoding, and legality filtering, a strong data channel is produced that is impervious to compression, tampering, and irregularities in the game.

V. EVALUATION AND LIMITATIONS

Project can be tested using a range of file sizes and types, including text, photos, and zip archives. About 1-2 KB of encrypted data can be encoded in a single standard-length chess game. The encoder automatically divides the payload among several games and connects them using metadata headers for larger files.

The main causes of failures can be Lichess maintenance, move legality issues resulting from mid-game interruptions, and API rate constraints.

Important restrictions consist of:

- Encoding Capacity: The amount of data that may be saved per game is limited by the limited move space in chess. In comparison to image-based steganography, the encoding density is substantially lower.
- Detection Risk: Although the games are lawful, in a well scrutinized setting, statistical irregularities in move selection (such as a lack of captures or subpar play) could cause suspicion.
- Dependency on Platform Stability: System may have disruptions in the future due to modifications made to game rules or API behavior.

VI. BROADER IMPLICATIONS AND ETHICAL CONSIDERATIONS

The project is more than just a technological advancement; it raises significant issues regarding the reuse of digital spaces, particularly those intended for learning or enjoyment. The project makes it difficult to distinguish between subversion and innovation, art and usefulness, and game and tool. It also brings up moral concerns of resource consumption, platform integrity, and user expectations by employing a public platform as a transmission channel.

On the one hand, these technologies can be used for justifiable reasons, such as avoiding censorship, facilitating safe activism, or providing insightful criticism on digital surveillance. However, the same technology might be applied maliciously or illegally. Therefore, it is imperative that such work be combined with responsible disclosure, open dialogue, and transparent documentation.

We suggest that comparable systems ought to:

- Prevent overloading or abusing platform infrastructure, provide fail-safes.
- Provide platforms with opt-out options so they can identify or, if necessary, limit such activity.
- Be assessed according to their capacity for abuse as well as empowerment.

VII. FUTURE SCOPE

The project’s creation and successful presentation offer numerous prospects for further study and useful improvements. There are still a number of avenues for development, improvement, and multidisciplinary research, even if the existing implementation confirms that encoding encrypted data into chess games and using a public platform as a decentralized data conduit are feasible.

A. Encoding Efficiency and Game Semantics

Increasing the bit-density every move without sacrificing game legality is one of the immediate areas for improvement. Potential avenues for future research include:

- Board locations with the highest encoding potential can be found using machine learning models.
- Customising the chess variants where move legality expands the encoding dictionary.
- Types of hybrid encoding that change tactics in the middle of a game to add more entropy.

B. Platform Generalisation

Even though this project was based around Lichess.org, the similar encoding data principle can be used by other platforms[12].

C. Integration with Decentralised Storage and Blockchain

Combining this encoding method with blockchain-based file systems or decentralized identity systems (like IPFS) is a viable approach. Games could reference file shards stored on dispersed networks and serve as lightweight metadata anchors.

These integrations may result in:

- Unchangeable academic records.
- Platforms for the anonymous dissemination of material.
- File recovery from chess game logs using public keys.

As digital ecosystems evolve and filtering grows more sophisticated, the significance of inventive, rule-based steganographic channels like this project will definitely expand. This entertaining yet subversive idea can become a useful tool for privacy, freedom, and creativity with continued multidisciplinary cooperation between cryptographers, game theorists, and digital rights advocates.

VIII. CONCLUSION

Project encrypts data into legitimate chess moves and stores the resulting games on a public chess platform, introducing a new and unusual method of safe, decentralized file transport. In order to transform an open digital playground into a secret data channel, this study crosses several fields, including platform engineering, steganography, cryptography, and restricted encoding. The system effectively illustrates how chess and other organized, rule-constrained environments can be utilized for subversive communication, decentralization, and digital privacy experimentation in addition to play.

With its fully reversible game-based encoding approach, strong encryption pipeline, and modular architecture, the project demonstrates its feasibility as a workable prototype for data embedding and retrieval. The utilization of public bot accounts on Lichess.org for passive file access via game IDs and live data "uploads" illustrates a larger possibility for low-profile, low-cost data storage in unexpected places. Even while the platform places restrictions on things like move legality and encoding limits, these restrictions are incorporated into the creative design rather than being limitations.

Beyond its technological advantages, the initiative sparks fresh discussions on ethical steganography, digital resistance, and the changing function of entertainment platforms as communication layers. Repurposing public, harmless technologies into data conduits could be a potent instrument for privacy and freedom of expression as surveillance and censorship grow more widespread.

In the end, project is a conceptual provocation as well as a technological demonstration, exploring what may happen when systems are repurposed as safe, covert communication tools in plain sight rather than being used as intended.

REFERENCES

[1] Bloisi, D. D., & Iocchi, L. (2007, March). Image based steganography and cryptography. In VISAPP (1) (pp. 127-134).

[2] Kumar, P., & Sharma, V. K. (2014). Information security based on steganography & cryptography techniques: A review. International Journal, 4(10), 246-250.

[3] Gupta, S., Goyal, A., & Bhushan, B. (2012). Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 4(6), 27.

[4] Bukhari, S., Arif, M. S., Anjum, M. R., & Dilbar, S. (2016, August). Enhancing security of images by Steganography and Cryptography techniques. In 2016 Sixth International Conference on Innovative Computing Technology (INTECH) (pp. 531-534). IEEE.

[5] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications, 7(6).

[6] Varghese, F., & Sasikala, P. (2023). A detailed review based on secure data transmission using cryptography and steganography. Wireless Personal Communications, 129(4), 2291-2318.

[7] Abdullah, D. M., Ameen, S. Y., Omar, N., Salih, A. A., Ahmed, D. M., Kak, S. F., & Rashid, Z. N. (2021). Secure data transfer over internet using image steganography. Asian Journal of Research in Computer Science, 10, 33-52.

[8] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73-80.

[9] Abdeihaleem, S. H., Radwan, A. G., & Abd-El-Hafiz, S. K. (2014, June). A chess-based chaotic block cipher. In 2014 IEEE 12th

[10] International New Circuits and Systems Conference (NEWCAS) (pp. 405-408). IEEE.

[11] Ahmed, M. S., MaryAnkitha, P., Anitha, P. U., Raju, M. R., & Kumar, B. P. (2024). Chess Games as a Method for File Encryption and Storage.

[12] Kamat, V. K. (2017). Chessography: A Cryptosystem Based on the Game of Chess. In Computational Intelligence in Data Mining: Proceedings of the International Conference on CIDM, 10-11 December 2016 (pp. 309-324). Springer Singapore.