ISTE 645

Research Project: Online Research

Dhairya Dutt (dd8053)

Data Hiding using Chess

1. Page 1: Introduction

a. About

- The use of games as a cover medium for steganography techniques has grown in popularity recently. Several research have used games as a cover medium to hide information [2]. Gaming is a popular source of entertainment. People of all ages enjoy this. Chess is among the most Popular board games around the world. Serving as a simulation of a Battle between two kingdoms, chess grabs the brains of two. Players engaged in a strategic combat on a checkered gameboard. Known as a chessboard. The chessboard contains 64 squares. structured in an 8 × 8 grid and requires the usage of six unique Each player has 16 moving pieces. Each piece has a unique set of rules and movements [4].

Fig.1 Chess Board [4]

- This approach of steganography involves embedding data throughout chess games to hide the true content. Data can be encoded in a chess game by assigning binary values to each move. A sequence of games, rather than a single match, might represent more and more complicated facts. This work presents a method for encoding and reconstructing whole files, including graphics and text, using chess games. The research examines how this technology can provide secure, low-bandwidth communication. Emphasizing the encryption of secret messages. This method requires translating binary data into a format that allows legal chess moves. It gives an innovative technique for hiding information in plain sight, making it helpful.

b. What is steganography

- To put it simply, steganography is the art and method of hiding data. It can be done both physically and digitally, using techniques ranging from Morse code blinking to data hidiing in.mp3 files.[1]

- Combining steganography and encryption can provide an additional degree of security by hiding the message's existence and scrambling its contents even if detected. This technology is utilized in a variety of sectors, including digital watermarking (to protect intellectual property) and covert communication in cyber espionage.

c. Steganography vs Cryptography

- Steganography aims to conceal the presence of information, whereas cryptography aims to prevent access to that information. When steganography is used correctly, no one, save the intended recipients, should be able to detect any secret communication taking place. This makes it an effective method in situations where obvious contact is dangerous. In contrast, cryptography is typically utilized in cases where the

participants are unconcerned about anyone discovering that they are communicating, but the communication itself must be disguised and inaccessible to third parties. [1]

- Let's look at some examples to better grasp the differences. If you are a political activist who has been imprisoned and needs to communicate with your organization, logistics can be difficult. The authorities may monitor everything that enters and exits your cell, so you will most likely have to mask any communication that occurs. Steganography would be an appropriate solution in this case. It may be difficult given your resources, but you may write a plain-sounding letter with a hidden message concealed using several font kinds or other steganography techniques.

- Another example would be, Diplomats are expected to communicate with officials from their home country in order to avoid suspicion. However, because the conversation's substance is top secret, the diplomat may choose to use cryptography and communicate over an encrypted line. If spies or attackers attempt to intercept the communication, they will only have access to the ciphertext, not what the two parties are saying.

2. Page 2: History

a. History of Steganography

- Herodotus' Histories contains the first known textual example of steganography. He claims that it occurred during the Ionian Revolt, a rebellion of certain Greek cities against Persian control in roughly 500 BC. Histiaeus, the ruler of Miletus, was away from his city serving as an adviser to the Persian monarch. He intended to return to Miletus, which was controlled by his son-in-law, Aristagoras, so he plotted an uprising in Ionia as a pretext for his homecoming. This is where steganography comes in. He shaved a slave's head and tattooed a statement on his scalp. [1]

- Histiaeus then waited for the slave's hair to grow back, hiding the message, before sending him to Aristagoras with instructions to shave the slave's head again and read the letter. The hidden writing instructed him to rise up against Persian rule, igniting the revolt against their invaders. Herodotus recounts another incident with steganography that occurred several years later, when Spartan king Demaratus returned a supposedly blank wax tablet to Sparta. A message was hidden inside the wax, warning the Spartans about Xerxes' impending assault. Herodotus is infamous for his wild tales, so we can't be certain how true these stories are, but they are the oldest recordings of steganography we have.

Fig.2 Null Cipher Example [1]

- It wasn't long before more advanced types of steganography were discovered. In the fourth century BC, Aeneas Tacticus mentioned a hole punching technique. Philo of Byzantium was the first to write about invisible inks, in the third century BC. His recipe involved writing text with gall nuts and revealing it with a copper sulfate solution. Johannes Trithemius coined the

term "steganography" in his book Steganographia. The name is a combination of the Greek words steganos (concealed) and graphein (writing). Steganographia was a brilliant book that claimed to be about magic and the occult but concealed its true subject matter, which was concentrated on cryptography and steganography.[1]

- Steganographia was followed by Polygraphia, which appeared after Trithemius' death in 1518. This was a more straightforward book on steganography and its use. Another significant advancement in steganography occurred in 1605, when Francis Bacon created Bacon's cipher. This method employed two distinct typefaces to encode a secret message into seemingly benign text. Microdots were first invented in the second half of the nineteenth century, although they were not widely utilized for steganography until World War I. They include reducing a message or image to the size of a dot, allowing people to communicate and share information without their adversaries knowing.

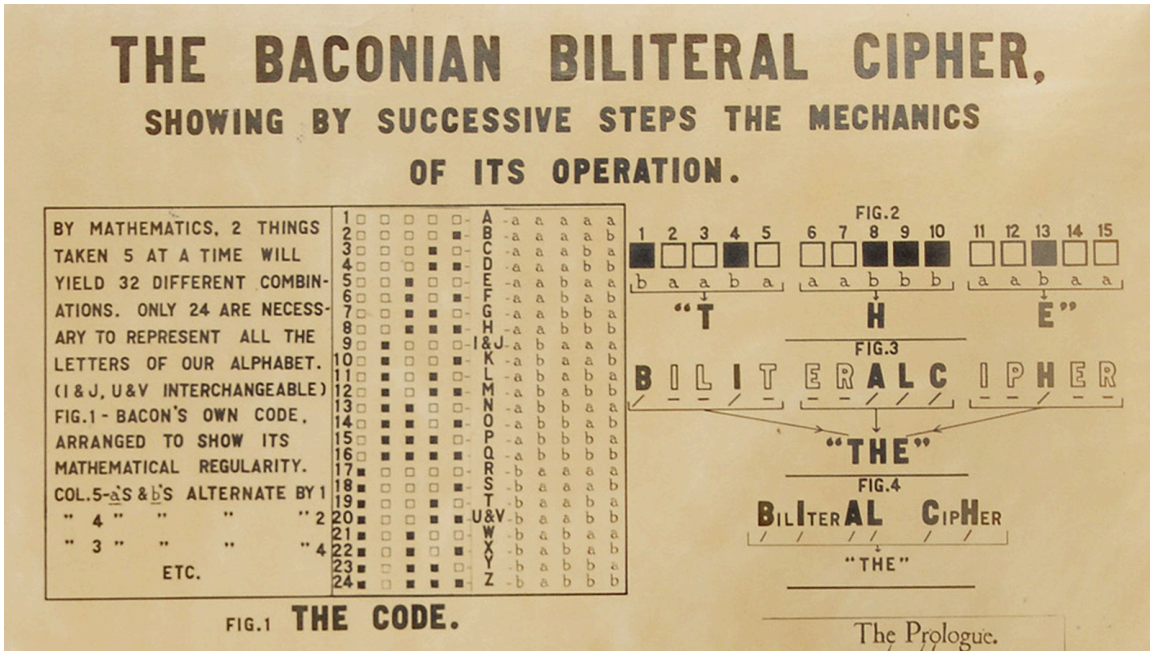

Fig.3 Baconian Cipher [1]

- There have been numerous other steganographic developments and approaches over the years. Steganography is still practiced today, with low-tech variants commonly utilized by prison gangs and digital methods used to hide data in images, sound files, and other media.

b. History of related work

- Game-based steganography has been extensively studied, with several ways being considered. Some solutions use a framework, while others use visuals from a game to hide text. Ou and Chen [3] suggested a steganographic approach using online Tetris games to incorporate secret messages using tetromino sequences. The suggested method creates a unique stegoed tetromino sequence for each game, meeting the criterion of generating a new sequence each time a game is played. The study provides a scenario, simulation, and theoretical proof for the suggested strategy. Experimental results show that the proposed approach is undetectable. However, these solutions have restrictions, including the need for the recipient to share the same Sudoku grid information and the size of the puzzle image.[5]

- Dey et al. [4] suggested an image steganographic approach using the sudoku puzzle. The suggested approach uses an 8x8 sudoku matrix as a key to encrypt and decrypt the secret message. The proposed approach converts the secret message's ASCII value to base-8 numbers, which are then saved in an array. Each sudoku cell's value is translated to binary and represented by the least significant bit of the blue component of each set of 9 pixels in the cover image.

- Hussien et al. [5] suggested a coverless picture steganography method using jigsaw puzzle image generating. The proposed method breaks an image into blocks and produces a jigsaw puzzle stego-picture using secret message bits and a mapping function. To extract the payload, reassemble the puzzle. Our suggested method outperforms

existing coverless image steganography algorithms in terms of hiding capacity, security, and resilience.

- Desoky et al. proposed Chestega [7] in 2009, which hides data by using chessboard position, piece color, game moves and outcomes, tournament name, place, and player name. Chestega produces a chessboard graphic, a written sequence of moves, and a story.

- In 2021, Bansal et al. [8] proposed a steganographic technique inspired by the rook chess piece. The process divides the cover image into n×1 pixel blocks, which are equivalent to 64 bits, similar to chessboard squares. Each block represents black and white rook pieces, with bit values of 0 and 1, respectively. The hidden message is incorporated in the cover image depending on the functional output of each block, which is computed by taking into account the number of rook positions under attack from opponents.

- However, none of the three chess-steganography approaches stated use an image of a chessboard to conceal a hidden message.

3. Page 3: Methodology

a. Method 1: Chess-Based Encryption System

- The suggested chess-based encryption system consists of two main components: an encoder and decoder. The encoder translates binary data to chess moves and generates a Portable Game Notation (PGN) file with one or more full games. The process maps binary chunks to legal chess moves, with the size of each chunk based on the number of potential movements in the current board position. The technique uses the intricacy and unpredictability of chess games to conceal encrypted information, similar to steganography. [2]

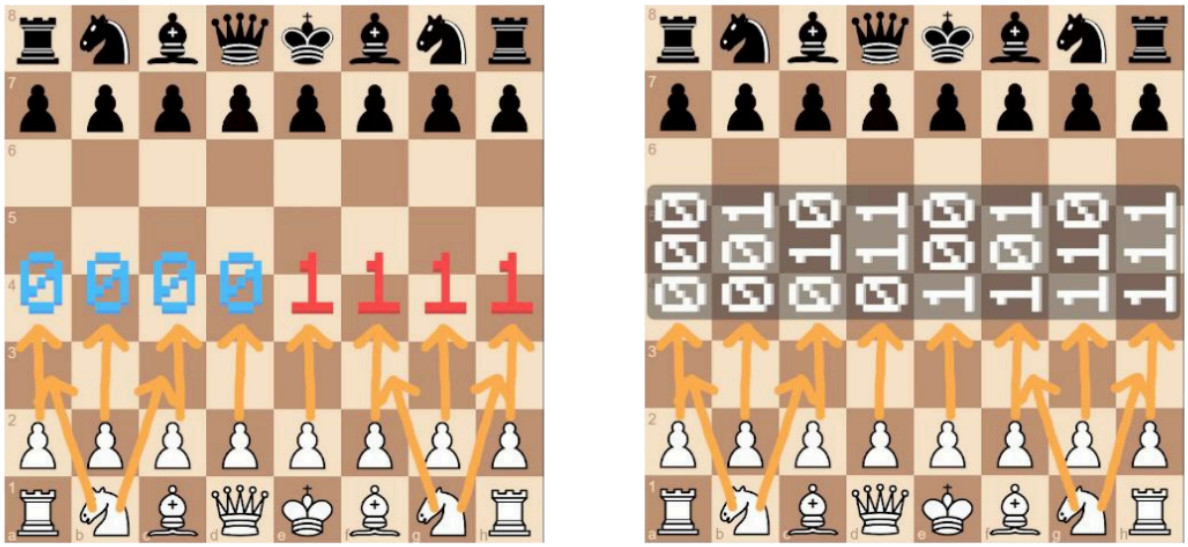

Fig.4 Method 1 [2]

- On the receiving end, the decoder reverses the procedure. The program reads the PGN file, reconstructs the chess games, and turns each move into a binary chunk. The binary chunks are concatenated and written to an output file to reassemble the original data. The system's security is based on the large number of possible chess games and the challenge of discriminating between moves for data encoding and actual gameplay. This technology provides a secure data transmission method that is ideal for situations when typical encryption methods may cause unwanted attention.

b. Method 2: Chess-Based Steganography

- The proposed method for data hiding in chessboard games cleverly incorporates hidden message embedding into the chess framework. Initially, the secret message is compressed by Huffman coding, which optimizes data by assigning shorter binary codes to frequently occurring parts. The message is separated into two sections: the first 24 bits are embedded through pawn placements according to a specified mapping, and the following 16 bits are encoded based on the number of

pieces on the chessboard's columns and rows using special binary representation rules.[3]

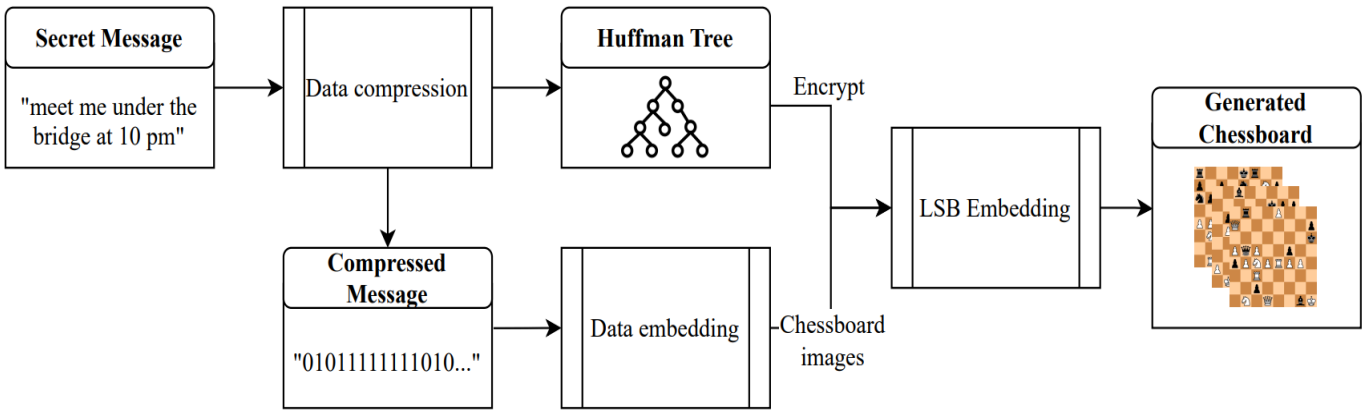

Fig.4 Method 2 [3]

- Validation requirements are followed to ensure that the chess setup remains legitimate following the embedding process. Furthermore, the method uses the Least Significant Bit (LSB) methodology to embed the Huffman tree in the chessboard image, dispersing bits across different squares to reduce visible artifacts. Reconstructing the chessboard, reading the encoded messages, and decoding with the stored Huffman tree are all part of the data extraction process.

- This revolutionary concept not only displays a novel use of steganography, but it also combines cryptographic principles with games strategy to provide safe communication, allowing up to 40 bits of secret information to be hidden within an otherwise normal chess game. This strategy improves the field of secure communications by preserving the chessboard's integrity while concealing critical data.

4. Page 4: Applications and Drawbacks

a. Applications

- **Covert Communication**: This strategy is ideal for hidden communication, particularly in digitally monitored contexts. This approach, which hides data within seemingly harmless chess games, can be utilized by journalists, activists, or spy

organizations for secret messaging. Games can discreetly transmit important information by embedding small text files.

- **Secure File Transmission**: Chess-based encryption may safely transfer small files (e.g., text or photos) using regular chess platforms, making it ideal for high-security contexts such as corporate espionage and military operations. Chess games are a popular form of entertainment and competitiveness, making them a suitable cover for transferring encrypted data.

- **Digital watermarking and DRM**: Another use involves digital watermarking and digital rights management (DRM). Chess games can be used to add ownership or usage rights to media files. Encrypted and communicated through chess games, content providers can show ownership of their creative property during disputes. [9] [10].

- **Secure Messaging for Restricted Networks**: This approach may be useful in dictatorships that prohibit or monitor common encryption technologies. Using a game like chess to transmit data can avoid monitoring devices that cannot detect encrypted communications concealed within game moves.

b. Drawbacks

- However, the system is not without flaws. One potential vulnerability is the predictability of lawful chess moves. Skilled chess players or AI systems may spot patterns in move choices, potentially revealing encoded information. Encryption can be compromised if the encoding mechanism assigns binary values to specified moves in a predictable manner. To address this, use randomization approaches when assigning binary values to each motion.

- Another drawback is the method's limited throughput. Transmission of huge files becomes difficult with an encoding rate of around two bytes per second, limiting the amount of

secure information that can be communicated. Other encryption algorithms may apply to larger data files.

5. Page 5: Conclusion and Future Work

a. Future Work

- **Optimizing Encoding Efficiency**: The performance evaluation shows that encoding speed reduces dramatically while There are fewer legal movements available in the middle and endgame phases. Future work could Investigate approaches to dynamically alter encoding strategies, maybe incorporating Techniques for improving performance include parallelism and multi-threading. This would also. allows for more efficient encoding of larger files.

- **Enhancing Security**: Future iterations may include adding a second layer of security. encryption, such as AES (Advanced Encryption Standard) [11], on top of the existing Chess-based methodology. This hybrid technique will ensure that even if the chess encoding is decoded, the underlying data will still remain safeguarded. Also, introducing More advanced randomness in assigning binary values to chess moves Could make it more resistant to patterns

- **Application for Real-Time Messaging**: One interesting possibility is to use the chess-based encryption method in real-time. Communication platforms. By incorporating it into chat platforms or video conferencing. Users might exchange short secret messages disguised as in-game chess moves. Throughout a chat. This application will make it more difficult for attackers to Detect covert communications in real time.

- **Exploring Game Variants**: Currently, the technique is based on normal chess games, but there may be possibilities for extending the method to variants such as Chess960 (Fischer Random Chess). There are many other games, such as Go and Shogi. These games provide a wider range of move

options, potentially boosting the encoding capacity each game while keeping the Obfuscation can be beneficial.

- Integration of Blockchain Technology A future direction could be to combine this encryption technology with blockchain. technology. Encoding data into chess games and keeping game reports on a blockchain would provide an immutable, decentralized record of the encrypted data, enabling Verifiable storage and retrieval. This could lead to new opportunities for secure and Permanent data storage.

b. Conclusion

- Both methods highlight the unique and innovative nature of using chess as a method for securing data. The first paper emphasizes the method's novelty in combining cryptography with game theory, making it ideal for small files, covert communication, and specific security-conscious applications. While it faces challenges in speed and overhead, it offers strong obfuscation and future potential with optimization. The second paper focuses on steganography, embedding up to 40 bits in chessboard positions using Huffman coding, resulting in millions of possible board variations, enhancing security through increased complexity. Both methods present promising avenues for secure data transmission in specialized contexts

● References

[1] Lake, J. (2023, December 29). What is steganography and how does it differ from cryptography?. Comparitech. https://www.comparitech.com/blog/information-security/what-is-steganography/#The_history_of_steganography

[2] Md Shaheer Ahmed, P MaryAnkitha, P U Anitha et al. Chess Games as a Method for File Encryption and Storage, 17 September 2024, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-5088828/v1]

[3] I. K. Agus Ariesta Putra and T. Ahmad, "Enigma on the Board: Chess-Based Steganography for Secure Communication," 2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri Sarawak, Malaysia, 2024, pp. 287-292, doi: 10.1109/GECOST60902.2024.10474684.

[4] “Chess: Everything You Need to Know - Chess.com.” [Online]. Available: https://www.chess.com/terms/chess.

[5] Shalu and Y. Sharma, “A Review on Game based Steganography,” in 2019 International Conference on Intelligent Sustainable Systems (ICISS). Palladam, Tamilnadu, India: IEEE, Feb. 2019, pp. 286–290.

[6] WintrCat. (n.d.). WintrCat/Chessencryption: Chess Encryption. GitHub. https://github.com/WintrCat/chessencryption

[7] D. Dey, A. Bandyopadhyay, S. Jana, A. K. Maji, and R. K. Pal, “A Novel Image Steganographic Scheme Using 8x8 Sudoku Puzzle,” in Advanced Computing and Systems for Security: Volume Three, R. Chaki, K. Saeed, A. Cortesi, and N. Chaki, Eds. Singapore: Springer Singapore, 2017, pp. 85–100