Cryptographic Image Distribution

[1] Mr P. Rajapandian, [2] A.Puvviyarasi, [3] R.Thirshalakshmi

[1]Associate Professor, Department of Computer Applications, Sri Manakula Vinayagar Engineering college (Autonomous), Puducherry 605008, India.

[2]Post Graduate Student, Department of Computer Applications, Sri Manakula Vinayagar Engineering college (Autonomous), Puducherry 605008, India.

[3]Post Graduate Student, Department of Computer Applications, Sri Manakula Vinayagar Engineering college (Autonomous), Puducherry 605008, India.

*Corresponding author's email address: puvviyarasi@gmail.com

Abstract- Cryptographic Image Distribution (CID) scheme, which integrates the Cellular Automata algorithm to address potential security vulnerabilities in existing fractal sharing matrices, presents a comprehensive and innovative approach to enhancing the security of confidential information distribution. The Cellular Automata algorithm introduces a dynamic and rule-based computational paradigm, adding an extra layer of complexity and unpredictability to the fortification of secret data before distribution. This strategy not only provides robust protection against unauthorized access but also contributes to the adaptability and resilience of the scheme in the face of evolving cyber threats. The incorporation of Cellular Automata not only enhances security but also introduces a versatile cryptographic technique that can be tailored to specific requirements and threat landscapes. Cybersecurity is a domain focused on protecting systems, networks, and data from cyber threats, unauthorized access, and other digital risks. It involves a range of practices, technologies, and processes designed to safeguard digital assets, maintain data integrity, and ensure secure communications. It Protects computer networks from intruders, including both targeted attackers and opportunistic malware attackes. The simplification of the authentication process is a noteworthy aspect of the proposed scheme, making it user-friendly.

Keywords: Cryptographic Image Distribution, cryptographic technique, Cellular Automata encryption.

1. INTRODUCTION

Cryptographic Image Distribution is a cryptographic technique that allows for the distribution of images in such a way that they can only be reconstructed when a certain threshold of shares is combined. In this mechanism, an image is classified into multiple shares, each containing partial information about the original image. However, individual shares reveal no discernible details about the image itself. Only when a predetermined number of shares are combined using a specific algorithm can the original image be reconstructed. This technique is often used for secure image transmission and storage, ensuring confidentiality and integrity by dispersing the image's information across multiple shares, making it extremely difficult for unauthorized parties to access or decipher the original image. Organizations necessary for developing a deeper understanding of the technologies and threats that exist in the cyber domain to be successful. There basically are 5 cyber domain parts, they are:

- *The physical domain*
- *The logical domain*
- *The data domain*
- *The application domain*

- *The user domain*

The Physical domain and Logical domain comprise the hardware and software, respectively that onto the computer system. The physical domain such as I/O devices, networking components, processors, memory, storage, and other physical parts of a computer system.

Software that runs on a computer system, such as BIOS, operating systems, applications, and data forms the logical domain. It defines how data is accessed and manipulated in the System. All the data stored on a computer comes under Data domain.

The Application domain contains various the applications available in the computer system while the user domain is the domain that contains the user information. Securing it requires including PINs, passwords, security phrases, and so on.

The User domain refers to individuals or entities who generate, distribute, or reconstruct shares of an image, controlling access to the original image by combining a specified number of shares using cryptographic techniques.

2. PROPOSED SYSTEM

A scheme is crucial for safeguarding sensitive digitized images from unauthorized access and tampering. The current reliance on a fractal matrix in the existing system poses security drawbacks, motivating the proposed integration of the Cellular Automata algorithm as an alternative to the fractal matrix approach. The Cellular Automata algorithm enhances the security of the secret image sharing scheme by introducing dynamic computational rules. Unlike the fractal matrix, Cellular Automata offers adaptability and unpredictability, fortifying the protection of distributed shares against unauthorized access and tampering.

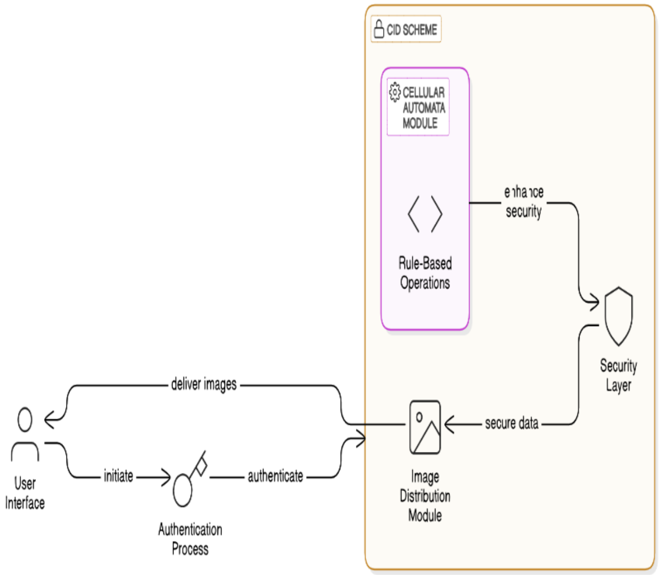

Figure 1: Cellular Automata-Based Secure Image Distribution Architecture

2.2 PROPOSED TECHNIQUE WORKS

1. Random Initialization:

***CA*(*x*,*y*)={0,1},for0≤*x*<*N*and0≤*y*<*M* –[1]**

Where:

- *N is the number of rows of the CA grid.*
- *MM is the number of columns of the CA grid.*
- *{0,1}{0,1} represents random binary values assigned to each cell at the start.*

2. Fixed Pattern Initialization:

***C A*(*x*,*y*)={0 otherwise -[2]**
1 if *x*=*v*

This could be a specific pattern based on the nature of the data or an initial seed pattern.

3. Image-Based Initialization:

$CA(x,y)$=binary_image(x,y),wherebinary_image(x, y)∈{0,1} – [3]

Here, the input image is first converted into a binary form (e.g., grayscale pixel values thresholded to 0 or 1).

2.3 ADVANTAGE OF THE PROPOSED SYSTEM

The Cellular Automata algorithm presents a significant advantage in its ability to provide dynamic and rule based computations, introducing an element of adaptability and unpredictability to cryptographic processes. Unlike traditional methods, Cellular Automata offers a versatile approach to encryption, enhancing the security of secret image sharing schemes. This adaptability is particularly advantageous in scenarios where complex and evolving security challenges need to be addressed. By leveraging Cellular Automata, the cryptographic system gains a higher level of resilience against unauthorized access and tampering, making it a valuable tool for safeguarding sensitive digitized images in applications such as medical imaging or secure document sharing.

3. CONCLUSION AND FUTURE ENHANCEMENTS

the proposed Secret Image Sharing system demonstrates a robust and secure approach to safeguarding sensitive digital assets, leveraging the Cellular Automata algorithm to address the limitations of traditional fractal matrix methods. This dynamic, rule-based mechanism enhances the system's security, adaptability, and unpredictability, making it resilient against unauthorized access and tampering. Comprehensive testing, including unit, integration, validation, and security testing, has validated the system's reliability and alignment with security requirements. Looking to the future, several enhancements are envisioned to further strengthen the system. Advanced encryption techniques will be explored to ensure resilience against evolving threats, while machine learning integration could introduce intelligent detection and response capabilities for potential security breaches. Incorporating blockchain technology may enhance data integrity and transparency, leveraging its decentralized, tamper-resistant architecture. Sophisticated user access management, such as role-based controls, will improve permissions handling, ensuring users access only relevant functionalities. Performance optimization and scalability will also be prioritized, enabling the system to handle larger data volumes and user loads seamlessly. Additionally, the development of mobile-compatible versions will enhance accessibility and flexibility for users. These advancements position the system as a future-ready solution for secure image sharing, with significant potential applications in critical domains such as medical imaging and secure document sharing.

4. REFERENCES

[1] G.R. Blakley, Safeguarding cryptographic keys, in: Proc. of the National Computer Conference1979, Vol. 48, 1979, pp. 313–317.

[2] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[3] M. Naor, A. Shamir, Visual cryptography, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 1–12.

[4] C.-C. Thien, J.-C. Lin, Secret image sharing, Comput. Graph. 26 (5) (2002) 765–770.

[5] Y.-S. Wu, C.-C. Thien, J.-C. Lin, Sharing and hiding secret images with size constraint, Pattern Recognit. 37 (7) (2004) 1377–1385.

[6] C.-C. Chang, Y.-P. Hsieh, C.-H. Lin, Sharing secrets in stego images with authentication, Pattern Recognit. 41 (10) (2008) 3130–3137.

[7] Y.-Y. Lin, R.-Z. Wang, Scalable secret image sharing with smaller shadow images, IEEE Signal Process. Lett. 17 (3) (2010) 316–319.

[8] C.-C. Wu, S.-J. Kao, M.-S. Hwang, A high quality image sharing with steganography and adaptive authentication scheme, J. Syst. Softw. 84 (12) (2011) 2196–2207.

[9] Z. Eslami, J.Z. Ahmadabadi, Secret image sharing with authentication-chaining and dynamic embedding, J. Syst. Softw. 84 (5) (2011) 803–809.

[10] G. Ulutas, M. Ulutas, V.V. Nabiyev, Secret image sharing scheme with adaptive authentication strength, Pattern Recognit. Lett. 34 (3) (2013) 283–291.

[11] M.J. Khosravi, A.R. Naghsh-Nilchi, A novel joint secret image sharing and robust steganography method using wavelet, Multimedia Syst 20 (2) (2014) 215–226.

[12] J. He, W. Lan, S. Tang, A secure image sharing scheme with high quality stegoimages based on steganography, Multimedia Tools Appl. (2016) 1–22.

[13] P. Li, Q. Kong, Y. Ma, Image secret sharing and hiding with authentication based on psnr estimation, J. Inf. Hiding Multimedia Signal Process. 5 (2) (2014) 353–366.

[14] G. Ulutas, M. Ulutas, V. Nabiyev, Distortion free geometry based secret image sharing, Procedia Comput. Sci. 3 (2011) 721–726.

[15] C. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inf. Theory 29 (2) (1983) 208–210.

[16] M. Ulutas, V.V. Nabiyev, G. Ulutas, A new secret image sharing technique based on asmuth bloom's scheme, in: Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on, IEEE, 2009, pp. 1–5.

[17] G. Alvarez, A.H. Encinas, L.H. Encinas, A.M. del Rey, A secure scheme to share secret color images, Comput. Phys. Commun. 173 (1) (2005) 9–16.

[18] Z. Eslami, S. Razzaghi, J.Z. Ahmadabadi, Secret image sharing based on cellular automata and steganography, Pattern Recognit. 43 (1) (2010) 397–404.

[19] J. Zarepour-Ahmadabadi, M.S. Ahmadabadi, A. Latif, An adaptive secret image sharing with a new bitwise steganographic property, Inform. Sci. 369 (2016) 467– 480.

[20] C.-C. Lin, W.-H. Tsai, Secret image sharing with steganography and authentication, J. Syst. Software 73 (3) (2004) 405–414.

[21] C.-N. Yang, T.-S. Chen, K.H. Yu, C.-C. Wang, Improvements of image sharing with steganography and authentication, J. Syst. Software 80 (7) (2007) 1070–1076.

[22] P.-Y. Lin, J.-S. Lee, C.-C. Chang, Distortion-free secret image sharing mechanism using modulus operator, Pattern Recognit. 42 (5) (2009) 886–895.

[23] A.M. Ahmadian, M. Amirmazlaghani, Computationally secure secret image sharing, in: Electrical Engineering (ICEE), 2017 Iranian Conference on, IEEE, 2017, pp. 2217–2222.