ADVANCED BLOCK AUTHENTICATION CODE VIA – LSS BASED COUPLED MAP LATTICE TECHNIQUES

[1]Shantha Kumar M , [2]Naveena R, [3]Rathika N , [4]Ushanandhini D.

[1]Associate Professor, Paavai Engineering College, Pachal, Namakkal.

[2,3,4]UG Students, Paavai Engineering College, Pachal, Namakkal

ABSTRACT:

This paper introduces a new way to keep data safe during transmission and storage, called Advanced Block Authentication Code (ABAC). As more people share data online, security has become a top priority. Old encryption methods are slow, not scalable, and easy to hack. ABAC combines two strong security techniques for better protection. It uses chaotic systems to create unique keys for each data block. This makes it hard for hackers to guess the code and access the data. ABAC is a fast and secure way to protect large amounts of data. By doing so, ABAC significantly strengthens data security, reducing the risk of unauthorized access or tampering. Additionally, its efficient design ensures that it can process large amounts of data at high speed, making it a practical solution for modern digital environments where both security and performance are crucial. This paper explores the structure, implementation, and benefits of ABAC, demonstrating how it offers a superior alternative to existing encryption methods.

Index Terms Data Encryption, ABAC, Chaotic Cryptography, Encryption Techniques, Digital Communication Security.

I.INTRODUCTION

Securing sensitive information during transmission is challenging due to sophisticated cyber-attacks. Cryptographic techniques face growing threats from powerful adversaries and quantum computing. Chaos theory has gained attention in cryptography due to its unpredictable systems. Chaotic systems exhibit properties ideal for generating secure sequences. We present an Advanced Block Authentication Code (ABAC) system using Logistic Sine System (LSS)-based CML. This approach combines chaotic encryption and block authentication for enhanced protection. Chaotic dynamics generate highly complex and random-like encryption keys. Our proposed ABAC system leverages chaotic properties for secure encryption and achieves high security and efficiency. Experimental results show improved security and polymorphism. The algorithm achieves high security and efficiency in data transmission, addressing traditional AC limitations.

II.MATERIALS AND METHODS:

1.EXISTING METHOD

Image files are increasingly distributed across the Internet. This distribution requires security techniques that are different from traditional practices to manage confidentiality. The reason is that images can be vulnerable to several attacks, particularly if these files are sent through insecure channels. Medical images, for example, contain highly sensitive data, and thus, sending these images over the network requires a strong encryption algorithm that protects against these attacks.

In recent years, reviewing the literature of image encryption has been of interest to researchers Moreover, different related topics have been reviewed. For example, some researchers have conducted surveys on the techniques for encrypting plaintext into images through an algorithm that calculates the RGB value. Furthermore, some related techniques such as image steganography have been studied along with image encryption. As another topic of interest, some surveys have focused on the applications of image encryption in specific areas.

There are some reviews directly focusing on the applications of chaos theory in image encryption. However, some of the surveys studied above (including the one reported in) are too outdated. Moreover, although a few of them develop a future roadmap, all of them fail to establish an ecosystem for chaotic image encryption.

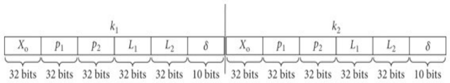


Figure 1: Key Structure

The chaotic nature of the key generation process ensures that even slight variations in the initial conditions result in drastically different keys, providing an additional layer of security. This approach enables ABAC to provide a high level of security and protection for sensitive data, while also ensuring efficient and scalable encryption. By harnessing the power of chaotic systems, ABAC's key generation in Figure 1 of mechanism sets a new standard for secure and efficient data protection.

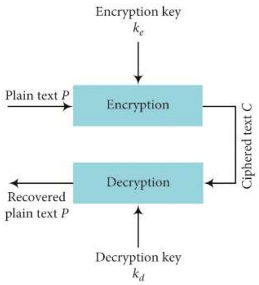


Figure 2: Encryption key Chaotic Key generate (ABAC) encryption keys using chaotic systems

Reviewing existing AI-assisted image processing methods has been of interest to many researchers. For example, a survey reported in focused on the interactions between machine learning and binocular stereo for depth estimation from images. Depth estimation has many practical purposes in fields such as 3D image reconstruction and autonomous driving. Included in the many techniques for estimating depth, stereo matching compares two images for pixel disparity and utilizes triangulation to determine the depth of the pixel. Data-driven and learning-based techniques have been applied to stereo matching with outstanding success, but the reverse has also yielded promising advances in using stereo matching to develop new methodologies based on deep networks.

As a branch of AI-assisted image processing, AI-assisted image encryption has received a research focus in recent years. A few researchers have conducted surveys on existing research works in this area. As an example, one may refer to, wherein the applications of neural networks in image encryption for optical security in the healthcare sector were studied. Image encryption is an important component in the healthcare sector for improving the security of patient images gathered from sources such as ultrasounds, MRI scans, and X-rays. Neural networks are heavily used to provide security and privacy through encryption, although the algorithms are currently limited by their complexity and speed, and therefore, much research in the field is focused on optimization.

2.PROPOSED SYSTEM

The proposed Advanced Block Authentication Code (ABAC) system is designed to enhance both encryption and data authentication by utilizing the chaotic properties of the Logistic Sine System (LSS) in a Coupled Map Lattice (CML) structure. The system divides data into blocks and encrypts each block using dynamic keys generated from the chaotic LSS-based CML model. This approach provides two major advantages: first, it ensures that each block of data is encrypted with a unique key, and second, it integrates authentication mechanisms to verify the integrity of each block.

3.METHODOLOGY

Advanced Block Authentication Code (ABAC) via LSS-Based Coupled Map Lattice involves several key steps to ensure secure data transmission and storage. First, the input data is divided into fixed-size blocks for efficient processing. A Logistic-Sine System (LSS) is then used to generate highly unpredictable and unique chaotic keys for each data block. To further enhance security, a Coupled Map Lattice (CML) technique is applied, introducing inter-block dependencies that make it harder for attackers to manipulate the data. Each data block is encrypted using the generated chaotic keys, and an authentication code is derived to verify data integrity. The encrypted and authenticated data is securely transmitted or stored, ensuring protection against unauthorized access. At the receiver’s end, the same chaotic key generation and authentication processes are used to reconstruct the original data. The authentication code is verified to detect any tampering or modifications.

4.COMPONENTS

1) Web Applications

We can use Python to develop web applications. It provides libraries to handle internet protocols such as HTML and XML, JSON, Email processing, request, beautiful Soup, Feedparser, etc. One of Python web-framework named Django is used on Instagram. Python provides many useful frameworks, and these are given below:

Django and Pyramid framework(Use for heavy applications)

Flask and Bottle (Micro-framework)

Plone and Django CMS (Advance Content management)

2) Desktop GUI Applications

The GUI stands for the Graphical User Interface, which provides a smooth interaction to any application. Python provides a **Tk GUI library** to develop a user interface. Some popular GUI libraries are given below

3) Console-based Application

Console-based applications run from the command-line or shell. These applications are computer program which are used commands to execute. This kind of application was more popular in the old generation of computers. Python can develop this kind of application very effectively. It is famous for having REPL, which means the Read-Eval-Print Loop that makes it the most suitable language for the command-line applications.

Python provides many free library or module which helps to build the command-line apps. The necessary IO libraries are used to read and write. It helps to parse argument and create console help text out-of-the-box. There are also advance libraries that can develop independent console apps.

4) Software Development

Python is useful for the software development process. It works as a support language and can be used to build control and management, testing, etc.

SCons is used to build control.

Buildbot and Apache Gumps are used for automated continuous compilation and testing.

Round or Trac for bug tracking and project management.

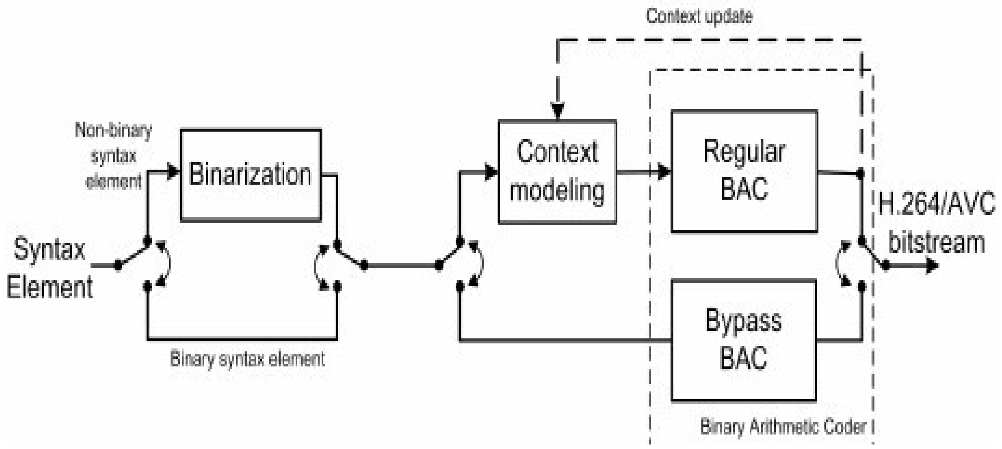
5.SYSTEM REQUIREMENT

- Processor: Intel i3/i5/i7
- Ram: 4 GB
- Hard disk: 160 GB
- Monitor: 18inch Lcd/Led
- Webcam

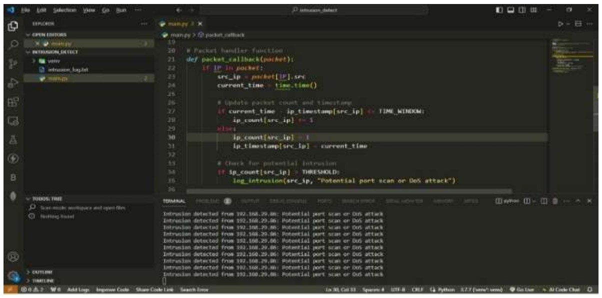
SOFTWARE REQUIREMENT:

- OS: Windows 8/10/11
- Editor: VS Code
- Python 3.7
- Python with its neural network libraries
- Algorithm – Advanced Block Authentication Code Algorithm

6.BLOCK DIAGRAM



III.SIMULATION



```
# Packet handler function
def packet_callback(packet):
    if IP in packet:
        src_ip = packet[IP].src
        current_time = time.time()

        # Update packet count and timestamp
        if current_time - ip_timestamp[src_ip] <= TIME_WINDOW:
            ip_count[src_ip] += 1
        else:
            ip_count[src_ip] = 1
            ip_timestamp[src_ip] = current_time

        # Check for potential intrusion
        if ip_count[src_ip] > THRESHOLD:
            log_intrusion(src_ip, "Potential port scan or DoS attack")
```

```
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
Intrusion detected from 192.168.29.86: Potential port scan or DoS attack
```

IV.CONCLUSION

The Advanced Block Authentication Code (ABAC) algorithm via LSS-based Coupled Map Lattice (CML) techniques provides a robust and secure solution for image authentication and encryption. The proposed algorithm leverages the benefits of CML techniques to generate a highly random and unpredictable keystream, enhancing the security and authenticity of the encrypted image**.** Simulation and experimental results demonstrate the effectiveness and security of the proposed algorithm, making it suitable for various applications, including secure image transmission and storage. Overall, the proposed ABAC algorithm via LSS-based CML techniques offers a reliable and efficient solution for protecting sensitive image data

V.REFERENCES

1. 1.A Behrouz Zolfaghari Takeshi Koshiba - 23 May 2022 / Revised: 6 June 2022 / Accepted: 7 June 2022 / Published: 13 June 2022

2. Fan Zhang and Xiaodong wang Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China, IEEE 2024.

3. Minjun Zhoua, Chunhua Wanga, a College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China.

4. Penghe Huang, Dongyan Li, Yu Wang, Huimin Zhao, +and Wu Deng, Software Technology Institute, Dalian Jiaotong University, Dalian 116028, China

5. Qing Ye, Qiaojia Zhang, Sijie Liu and Kaiqiang Chen College of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China

6. Qing Lu, Congxu Zhu, and Xiaoheng Deng, (Member, IEEE) 1Hunan Police Academy, Changsha 410138, China - Received January 7, 2020, accepted January 28, 2020, date of publication January 31, 2020, date of current version February 11, 2020

7. Xing yuan Wang, Nana Guna, Hongyu Zhao, Siwei Wang, and Yingqian Zhang Published online 2020 Jun 17

8. Xiuli Chai, Jianqiang Bi, Zhihua Ganb, Xianxing Liua, Yushu Zhangc, Yiran Chene - School of Computer and Information Engineering, Henan Key Laboratory of Big Data Analysis and Processing, Henan University, Kaifeng 475004, China.

9. Yue Hu, Ruyue Tian School of Mathematics and physics, China University of Geosciences, Wuhan, China.

10. Zia U, McCartney M, Scotney B et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int J Inf Secure. 2022