International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Integrated AES Encryption and Image Steganography with Multi-Factor Authentication for Secure Data Handling in Government Orders

Amgoth Ashok Kumar, Gugulothu Kalyan[2], Anumala Shravya[2], Boinapally Mounika[2], Gudur Harshavardhan[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

Public service departments handle a significant volume of Government Orders (GO) and administrative documents that often contain highly confidential information. With the rapid adoption of digital governance, ensuring secure storage and controlled sharing of such data has become critical. Existing approaches rely on manual handling or unsecured digital methods such as emails and shared repositories, which lack centralized control, proper authorization, and data protection mechanisms. These limitations lead to risks such as unauthorized access, data leakage, lack of traceability, and operational inefficiencies. To overcome these challenges, this work presents a secure web-based system for managing and sharing administrative documents using Multi-Level Access Control (MLAC). The system is developed using Python and the Flask framework, supporting three distinct user roles: Government, Collector, and Local Body, each with predefined access permissions. Sensitive documents are protected using Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode to ensure confidentiality during storage and controlled access. Tiny Database (TinyDB) is utilized as a lightweight database to manage user credentials, encrypted document metadata, permissions, and notifications in a structured manner. In addition to encryption, the system incorporates steganography to enable secure hidden communication through image-based message embedding. Role-Based Access Control (RBAC), secure session management, and Multi-Factor Authentication (MFA) further strengthen system security.

Key words: Multi-Level Access Control (MLAC), Advanced Encryption Standard (AES), Digital Governance, Steganography, Government Order (GO) Management.

1. INTRODUCTION

Electronic government (e-government) refers to a comprehensive digital ecosystem that integrates individuals, processes, communication subsystems, software applications, and organizational data to enable efficient governance. These components operate under well-defined policies and protocols to collect, process, store, and disseminate information securely within and across organizational boundaries. The effectiveness of such systems depends on the precise coordination and interaction among their elements, ensuring consistency, reliability, and controlled information flow [1]. E-government leverages digital technologies and web-based platforms to enhance communication, streamline administrative processes, and improve the delivery of public services. It encompasses a wide range of applications designed to increase operational efficiency, accessibility, transparency, and responsiveness of government functions [2]. The primary objective is to provide seamless access to government services while optimizing internal workflows, thereby enabling transparent governance and empowering citizens through better access to public information [3].

The implementation of e-government involves multiple interconnected components that collectively support modern digital governance frameworks. Digital service delivery allows citizens to access

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

essential services online, including applying for licenses, paying taxes, and accessing healthcare or welfare programs, reducing the need for physical interaction. Centralized portals and web platforms serve as unified access points where users can interact with various government departments, submit forms, and retrieve information efficiently. Digital identity and authentication systems ensure secure access to these services by providing reliable user verification mechanisms, replacing traditional identity validation with secure digital credentials [4]. Open data initiatives further enhance transparency by making government datasets publicly available in standardized and accessible formats, encouraging accountability and data-driven decision-making.

Figure 1: Digital Government Order

Digital communication platforms enable governments to engage with citizens, gather feedback, and improve policy formulation through participatory approaches. The supporting infrastructure, including secure networks, cloud computing environments, and data centers, ensures scalability, availability, and performance of services. Additionally, cybersecurity and data protection mechanisms play a critical role in safeguarding sensitive information, preventing unauthorized access, and maintaining system integrity against cyber threats [4]. The adoption of public key cryptographic techniques is widespread in securing communications and enabling digital signatures, although challenges related to computational overhead and key management still persist [5].

2. LITERATURE SURVEY

Jun-Hyung Park et, al. [6] proposed an enhanced security model that integrates the concepts of Multi-Level Security (MLS) and Zero Trust (ZT). The proposed model classifies data into the following three sensitivity levels: “Classified”, “Sensitive”, and “Open”. It applies tailored security requirements and dynamic controls to each level, enhancing both data security and usability. Furthermore, the model overcomes the static access control limitations of MLS by incorporating ZT’s automated dynamic access capabilities, significantly improving responsiveness to anomalous behaviors. Constantin Viorel Marian et, al. [7] presented a solution that oversees the auditing and monitoring of document circulation between different public institutions or within a single institution. The system is based on blockchain technology that stores data and preserves history, making every action traceable and auditable. The process of document creation involves the encryption, timestamping, and addition of the document to the blockchain, the access to which is restricted only to authorized stakeholders.

Owen Lo et, al. [8] aimed at administrative efficiency and the reduction of bureaucratic processes. It can also improve government capabilities, and enhances trust and security, which brings confidence

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

in governmental transactions. However, solid implementations of a distributed data sharing model within an e-governance architecture is far from a reality; hence, citizens of European countries often go through the tedious process of having their confidential information verified. Ioannis Lykidis et, al. [9] conducted a literature review on the use of blockchain technology in e-government applications to identify e-government services that can benefit from the use of blockchains, types of technologies that are chosen for the proposed solutions, and their corresponding maturity levels. Jin Han et, al. [10] discussed the application of cloud computing technology in the construction of electronic file management systems, proposed an architecture of electronic file management systems based on cloud computing, and made a more detailed discussion on key technologies and implementation. The electronic file management system is built on the cloud architecture to enable users to upload, download, share, set security roles, audit, and retrieve files based on multiple modes. An electronic file management system based on cloud computing can make full use of cloud storage, cloud security, and cloud computing technologies to achieve unified, reliable, and secure management of electronic files. Saba Rehman et, al. [11] proposed a secure and optimized scheme for sharing data while maintaining data security and integrity over the cloud. The proposed system mainly functions by combining the Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) method to ensure authentication and data integrity. The experimental results show that the proposed approach is efficient and yields better results when compared with existing approaches.

Sana Fatima et, al. [12] analyzed the well-known symmetric algorithm of the Advanced Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) asymmetric algorithm based on time complexity, space, resource and power consumption, and suggest a new hybrid encryption process that is a combination of symmetric and asymmetric cryptographic methods. Based on experimental analysis, they proposed that AES cryptographic method as a first choice for data encryption processes for cloud applications and data storage. Dian Anggraini et, al. [13] reviewed evidence-based insights for practitioners, researchers, and policymakers, addressing gaps in knowledge and advancing understanding of electronic document management systems (EDMS) in modern information management. Additionally, it presented a detailed breakdown of publication distribution across sectors, highlighting significant research areas like companies and businesses, education, and information technology and software. Simona Sternad et, al. [14] proposed a framework that can contribute to a better implementation and a higher level of use of Document management systems (DMS), which both lead to a greener digital transformation of the organization, representing an organization's maturity. We used the Process and Enterprise Maturity Model (PEMM) to assess the organization's maturity level concerning the DMS' life cycle.

3. PROPOSED SYSTEM

The system architecture is designed as a secure, role-based web application that integrates authentication, encryption, steganography, and controlled data sharing within a unified platform, as illustrated in Fig. 2. The Flask application acts as the central controller, managing user requests, routing, and session handling across all modules to ensure seamless coordination. User authentication is strengthened using multi-factor mechanisms, including OTP and biometric verification, which enhances access security and prevents unauthorized entry. TinyDB is utilized as a lightweight database to store user credentials, encrypted document metadata, notifications, and steganographic message records efficiently. AES-based encryption is applied to protect file contents during both storage and transmission, ensuring confidentiality and safeguarding sensitive information from potential threats. Role-based access control mechanisms ensure that only authorized users can retrieve

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

or decrypt data, enforcing strict permission policies. The system supports three primary roles—government, collector, and localbody—each with dedicated dashboards tailored to their specific functionalities. Upon successful authentication, users are redirected to their respective dashboards, where middleware continuously validates permissions to prevent unauthorized actions. During file upload, data is encrypted using AES, generating ciphertext and an initialization vector, which are securely stored along with metadata in structured directories. Controlled data sharing allows only authorized users to access and download encrypted files, with decryption permitted under predefined conditions after verifying data integrity. In addition to encryption, the system incorporates steganography techniques, enabling hidden communication by embedding secret messages into images using LSB methods. These stego-images facilitate secure cross-role communication without revealing the presence of sensitive data.

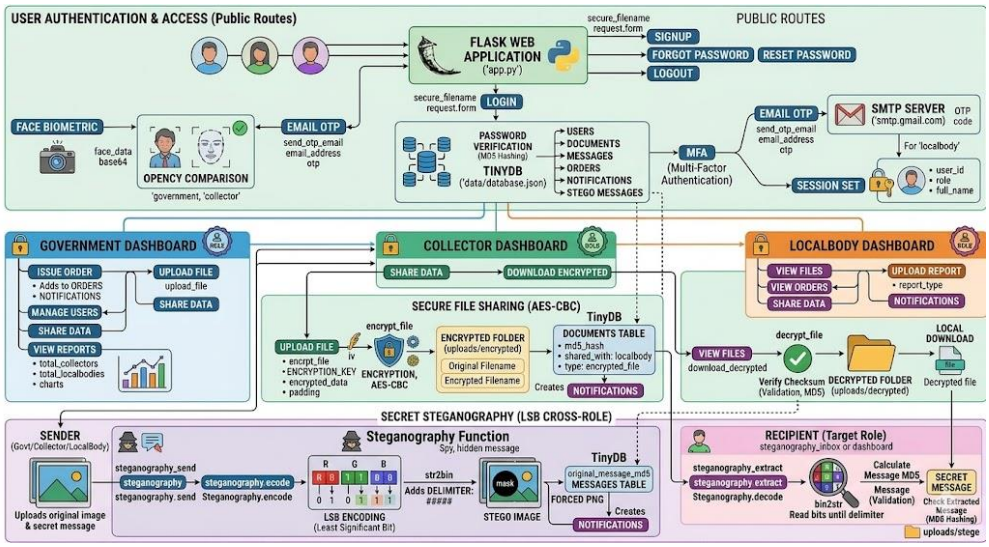

Figure 2: Proposed System Architecture

Upon retrieval, embedded messages are decoded to reconstruct the original information accurately. The system also includes a notification mechanism that generates alerts for events such as file uploads, order issuance, and message sharing, ensuring real-time communication among users. Notifications are stored and delivered based on user roles, maintaining relevance and efficiency. Furthermore, activity logging is implemented to track system operations and user interactions, enabling effective monitoring and traceability. This comprehensive architecture ensures data confidentiality, secure communication, controlled access, and system transparency while maintaining high reliability and scalability.

3.1 Steganography

The steganography module enables secure and covert communication by embedding secret messages inside digital images using LSB encoding as illustrated in Fig. 3. The process ensures that the visual quality of the image remains unchanged while carrying hidden information. A delimiter is appended to the message to enable accurate extraction during decoding. The system enforces role-based access so that only intended recipients can retrieve the hidden content. Stego-images are stored in a lossless format to prevent distortion of embedded data. Notifications are used to inform recipients about new hidden messages. The workflow forms a continuous loop where data is securely embedded, transmitted, and extracted.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

1. Image Selection and Message Input: The process begins when the user selects a valid image and provides a secret message to be hidden. The system also captures the intended recipient to ensure controlled communication. The selected image is stored safely before any modification to preserve the original version. This step prepares both the carrier medium and the hidden data for further processing.

2. Message Preparation and Encoding: The secret message is appended with a unique delimiter to indicate the termination point during extraction. The complete message is then converted into a binary format using 8-bit encoding for each character. This binary stream represents the actual data that will be embedded into the image. Proper encoding ensures that the message can be accurately reconstructed later.

3. LSB-Based Data Embedding: The system iterates through the image pixel by pixel and modifies the least significant bits of RGB channels. Each bit of the binary message is embedded sequentially into these pixel values without causing noticeable visual distortion. The embedding process continues until the entire message is stored inside the image. This technique ensures invisibility while maintaining data integrity.

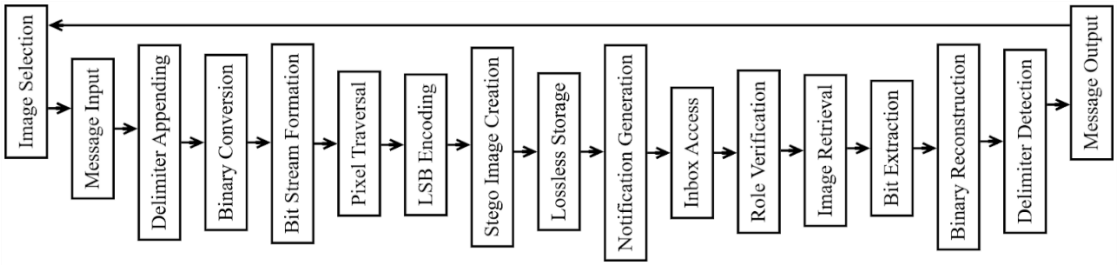

Fig. 3: Operational flow of Steganography

4. Stego Image Generation and Notification: After embedding, a new stego-image is generated and saved in a lossless format such as PNG to avoid compression-related data loss. The system records metadata such as sender, receiver, and timestamp in the database. A notification is automatically triggered to inform the recipient about the new hidden message. This step completes the secure transmission phase.

5. Access Control and Image Retrieval: The recipient accesses the inbox where stego-images are filtered based on role permissions. The system verifies whether the user is authorized to view the specific image before granting access. This ensures that only intended users can proceed with extraction. The image is then retrieved for decoding.

6. Message Extraction and Decoding: The system reads the least significant bits from the image pixels and reconstructs the binary sequence. This binary data is converted back into characters until the delimiter is detected, marking the end of the hidden message. The extracted message is then displayed to the user in readable format. This completes the steganography communication loop.

4. RESULTS AND DISCUSSION

Figure 4 depicts the interface used for creating and issuing new GOs. It allows authorized government users to define order details, assign priority levels, and select intended recipient roles. Issued orders are securely stored and made accessible only to designated users. This screen ensures structured dissemination of official directives. The figure highlights controlled and authenticated order management within the system.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Figure 5 illustrates the secure data sharing interface designed for exchanging confidential government information. It allows authorized users to enter sensitive content and specify the roles permitted to access the shared data. The system ensures that only intended recipients can view the information. This screen supports protected inter-departmental communication. The figure emphasizes confidentiality and controlled data distribution.

Figure 6 depicts the process of creating a new steganography message, where confidential information is embedded within an image before transmission. It shows how the sender selects the recipient role, uploads a cover image, and inputs sensitive content to be concealed. The process ensures that the data is encrypted and securely transmitted using image-based hiding techniques. This figure emphasizes the integration of data security with steganographic encoding to prevent unauthorized access.

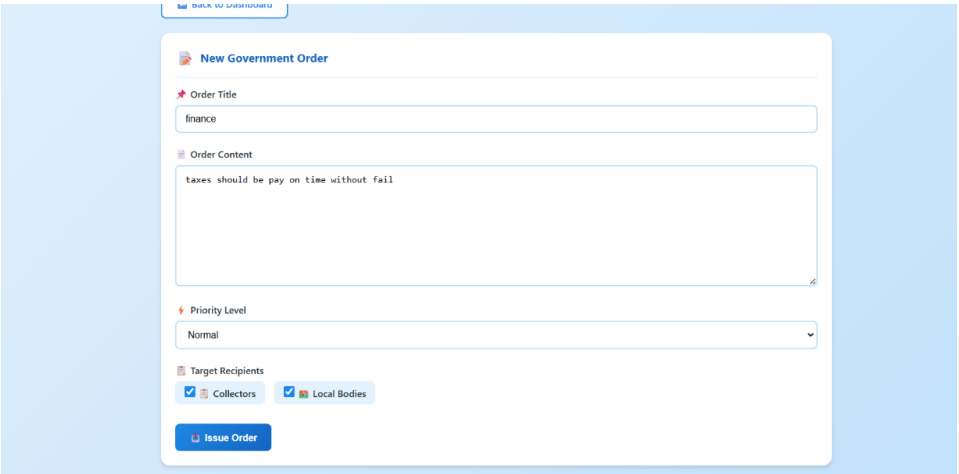

Figure 4: Creating New GO Screen

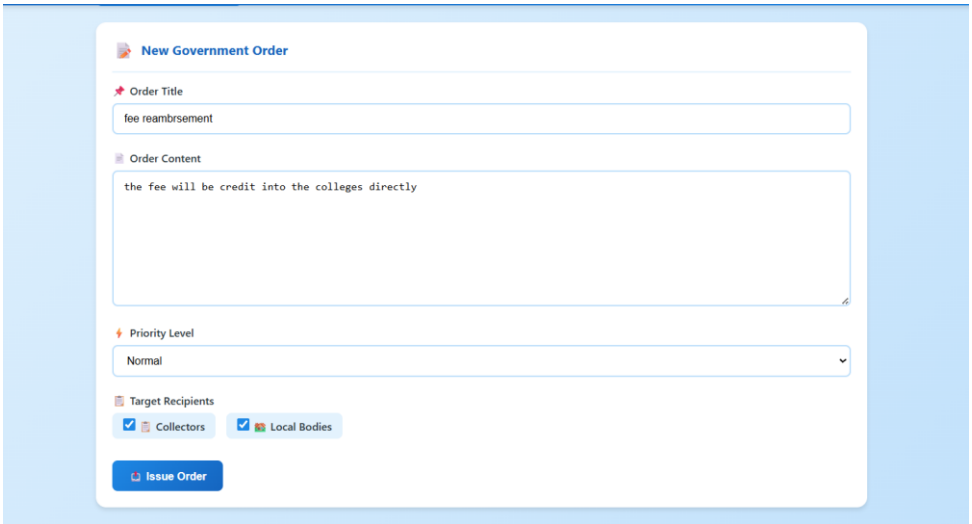

Figure 5: Sharing Confidential Data Screen

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

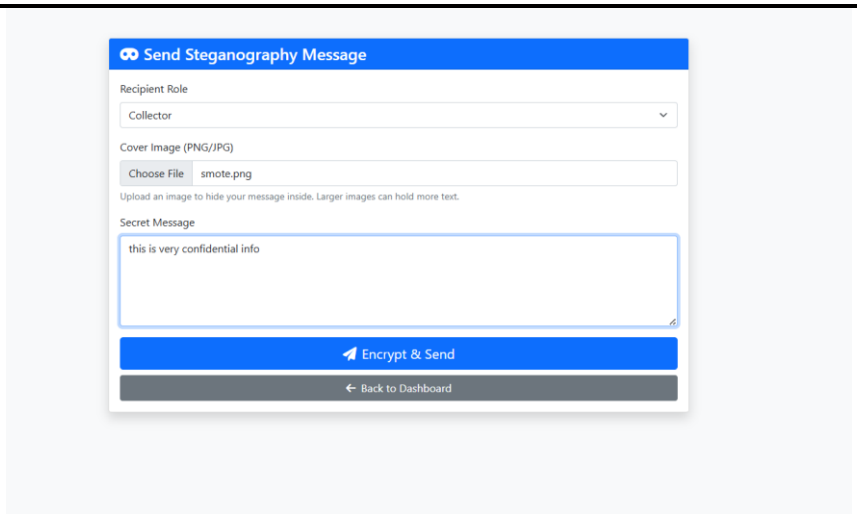

Figure 6: Creating New Steganography Message

Figure 7 illustrates the Steganography Transaction History, which maintains a record of all transmitted stego messages within the system. It demonstrates how each transaction is logged with details such as timestamp, recipient, and associated images. This logging mechanism ensures traceability and accountability for all secure communications. It also supports monitoring and auditing of data exchange activities.

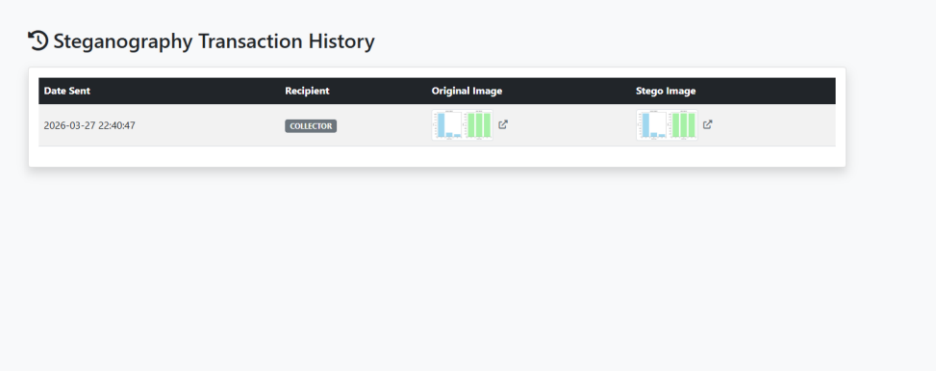

Figure 7: Steganography Transaction History

Figure 8presents the Received GOs screen, which allows collectors to view official directives issued by government authorities. The screen displays active orders along with relevant details such as priority and issuance information. It ensures that collectors receive authenticated and role-specific instructions. This mechanism supports timely dissemination of government decisions. The screen strengthens coordination between government and district-level administration.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Figure 8: Received Governments Orders Screen

Figure 9 illustrates the Steganography Inbox with received stego images, highlighting the availability of incoming hidden messages for extraction. It demonstrates how users can view sender details, roles, and associated image files containing concealed information. The presence of extraction functionality indicates the system's capability to decode embedded messages securely. This figure reflects the complete lifecycle of steganographic communication from reception to access.

Figure 10 depicts the decryption of a stego image and the extraction of the hidden message, representing the final stage of secure communication. It shows how the embedded confidential text is successfully retrieved from the encoded image. The process ensures that the integrity and confidentiality of the message are preserved during extraction. It highlights the effectiveness of combining encryption with steganographic techniques.

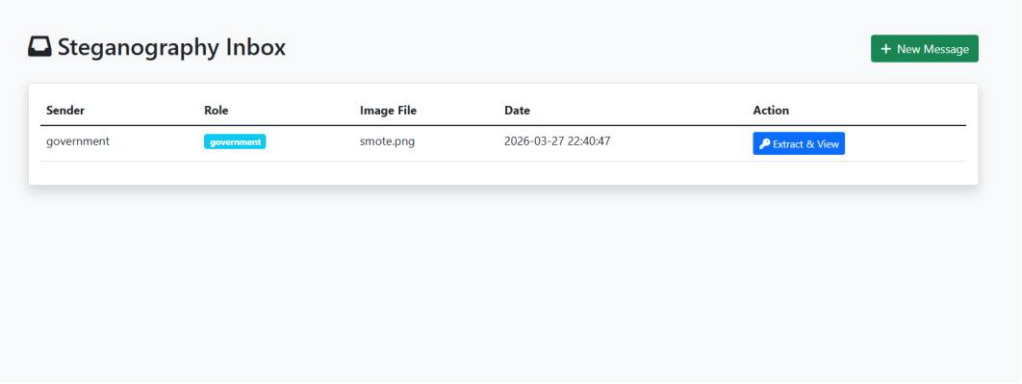

Figure 9: Steganography Inbox and Received Stego Images

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

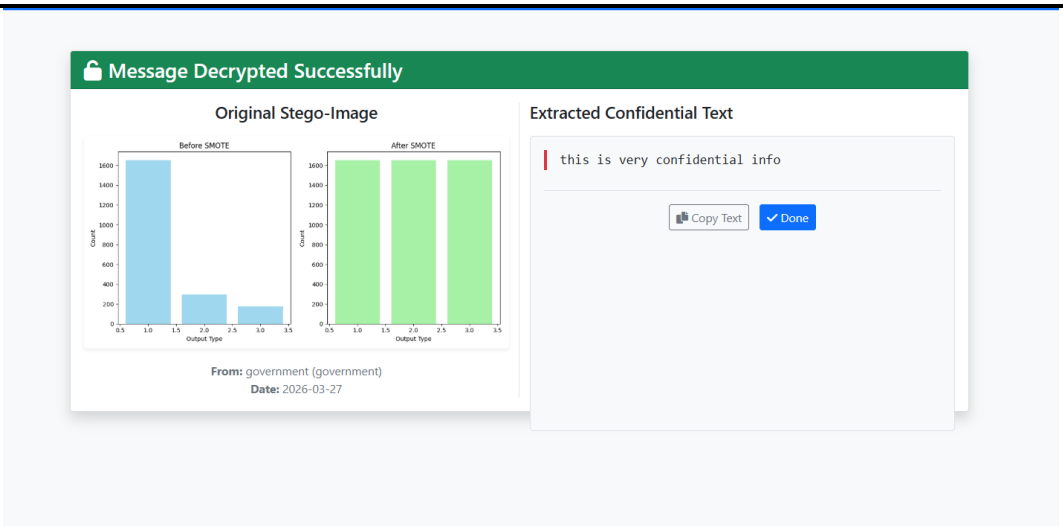

Figure 10: Decrypting Stego Image and Message

5. CONCLUSION

The proposed secure data sharing and communication system demonstrates an effective approach for managing administrative data, encrypted documents, and hidden communication within a unified digital platform. By integrating a Flask-based web application with role-based authentication, multi-factor verification, AES-based encryption, and steganography, the system ensures that sensitive information is accessed and transmitted only by authorized users such as government, collector, and localbody roles. The implementation enhances overall efficiency by centralizing data management, reducing manual intervention, and enabling faster processing of documents and messages. The use of lightweight technologies such as Flask and TinyDB minimizes system complexity and resource consumption, making the solution suitable for scalable and portable deployments. Encryption mechanisms ensure confidentiality of stored files, while steganography adds an additional layer of covert communication for secure message exchange. Role-based dashboards and notification systems further improve usability by delivering relevant information directly to users based on their responsibilities. The system significantly improves reliability and security by enforcing strict access control, secure session handling, and protected data storage. Compared to conventional manual or unsecured digital systems, the proposed solution reduces the risk of data leakage, enhances traceability of operations, and ensures timely and controlled information flow. Overall, the implementation provides a robust, secure, and efficient framework for modern administrative data management and communication.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

REFERENCES

[1] Marakas, G.M.; O'Brien, J.A. Enterprise Information Systems, 13th ed.; McGraw-Hill Higher Education: New York, NY, USA, 2007.

[2] Anttiroiko, A.V. Electronic Government: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2008; Volume 3.

[3] Popa, A.M.; Mocanu, S. Scalable Ecosystem Dedicated To Digitalization Of Citizen-Administration Interaction. UPB Sci. Bull. Ser. C 2021, 83, 59–72

[4] Farida, I.; Setiawan, R.; Maryatmi, A.S.; Juwita, M.N. The implementation of E-government in the industrial revolution era 4.0 in Indonesia. Int. J. Progress. Sci. Technol. 2020, 22, 340–346.

[5] Masiero, S. Digital identity as platform-mediated surveillance. Big Data Soc. 2023, 10, 20539517221135176.

[6] Park, J.-H.; Park, S.-C.; Youm, H.-Y. A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls. Appl. Sci. 2025, 15, 785. https://doi.org/10.3390/app15020785

[7] Marian, C.V.; Mitrea, D.A.; Rusu, D.S.; Vasilateanu, A. Transparent Digital Governance: A Blockchain-Based Workflow Audit Application. Appl. Sci. 2025, 15, 11694. https://doi.org/10.3390/app152111694

[8] Lo, O.; Buchanan, W.J.; Sayeed, S.; Papadopoulos, P.; Pitropakis, N.; Chrysoulas, C. GLASS: A Citizen-Centric Distributed Data-Sharing Model within an e-Governance Architecture. Sensors 2022, 22, 2291. https://doi.org/10.3390/s22062291.

[9] Lykidis, I.; Drosatos, G.; Rantos, K. The Use of Blockchain Technology in e-Government Services. Computers 2021, 10, 168. https://doi.org/10.3390/computers10120168.

[10] Han, Jin & Wang, Cheng & Miao, Jie & Lu, Mingxin & Wang, Yingchun & Jin, Shi. (2020). Research on Electronic Document Management System Based on Cloud Computing. Computers, Materials & Continua. 66. 2645-2654. 10.32604/cmc.2021.014371.

[11] Rehman, S.; Talat Bajwa, N.; Shah, M.A.; Aseeri, A.O.; Anjum, A. Hybrid AES-ECC Model for the Security of Data over Cloud Storage. Electronics 2021, 10, 2673. https://doi.org/10.3390/electronics10212673.

[12] Fatima, S.; Rehman, T.; Fatima, M.; Khan, S.; Ali, M.A. Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing. Eng. Proc. 2022, 20, 14. https://doi.org/10.3390/engproc2022020014.

[13] Anggraini, Dian & Adi, Kusworo & Suseno, Jatmiko. (2024). Electronic document management systems implementation across industries: systematic analysis. Indonesian Journal of Electrical Engineering and Computer Science. 36. 264. 10.11591/ijeecs.v36.i1.pp264-273.

[14] Sternad, Simona & Jordan, Sandra & Bobek, Samo. (2023). Managing Document Management Systems' Life Cycle in Relation to an Organization's Maturity for Digital Transformation. Sustainability. 15. 15212. 10.3390/su152115212.