Design and Development of a Key-Based Image Steganography Web Platform for Confidential Data Protection

Anoshan Yoganathan and Nivitha Rajendran

Abstract The security of confidential information in online communication is one of the critical issues. Whereas encryption protects information, steganography offers a great deal of protection to the very process of communication. The contents of this paper are the design, development, and thorough assessment of a web-based, key-dependent image steganography system with a design tailored towards confidential data protection. Having a solid library of HTML, CSS, JavaScript, and Python (Flask) and the Pillow library to process and manipulate images, our system combines Least Significant Bit (LSB) embedding method with the standard cryptographic features of the industry. In particular, a key obtained through PBKDF2 is used to encrypt messages with AES-GCM, to provide high confidentiality and integrity, to initialize a cryptographically secure pseudorandom number generator (CSPRNG) to use non-sequential pixel embedding. This method goes a long way to increasing the security level against brute-force and steganalysis attacks, unlike the simpler LSB implementations. The site provides an expressive, user-friendly interface to embed and retrieve encrypted messages in PNG and BMP images, which allows sophisticated steganography to be used by non-technical users. Extensive functional, performance, security and usability testing was done. The quantitative tests, such as PSNR, SSIM, and capacity distortion analysis of standard datasets, verify that the system maintains image quality and reliably embeds the data. Security tests such as comparisons with existing known techniques of steganalysis indicate better levels of robustness. Its ease of use is also authenticated by the usability studies. This publication does not merely offer a pragmatic, safe, and inviolable solution regarding covert digital communication, but also offers a polished structure of incorporating the superior cryptographic principles into the reachable web-based steganography utilities.

***Index Terms*— Steganography, Image Security, Least Significant Bit (LSB), Web Application, Chaotic Systems**

I. Introduction

In the more digitalized space, sharing of confidential information over networks is the most important activity that is secured. Although cryptographic techniques such as encryption do protect information by making it inaccessible to unauthorized individuals, they also give away the fact that some kind of secret communication took place. Instead, Steganography is intended to hide the fact that such communication exists at all, by conceiving the hidden message inside such even apparently innocent mediums of cover as a digital image. This early art is based on the Greek terms, steganos (covered) and graphia (writing), which provides another veil of secrecy and, as such, it is an invaluable asset to a situation requiring actual undercover communication.

Anoshan Yoganathan is an Undergraduate Student at the Department of ICT, South Eastern University of Sri Lanka. (Email: anoshan6@gmail.com)

Nivitha Rajendran is a Graduate from the Department of ICT, South Eastern University of Sri Lanka. (Email: nivitharajendran98@gmail.com)

Image steganography has gained further popularity because of the high use of digital pictures and their redundant nature of data that leaves room to make minor changes that the human eye cannot detect. One of the basic techniques of this field is the Least Significant Bit (LSB) technique, which directly interferes with the least significant bit(s) of pixel values to store hidden data. Although straightforward and unproblematic in terms of image quality, the traditional LSB implementations tend to have weak security controls, which exposes them to numerous steganalysis schemes and extraction by unauthorized parties upon its combination with simple scrambling algorithms. More so, a large number of current steganography solutions are either desktop-based, specialized knowledge, or have inconsistent security, which restricts their availability and their wider use.

This study mitigates these limitations by proposing the development and design of a secure, accessible and easy to use web based image steganography system. The main value that we will add is the synergistic combination of the LSB embedding method with the current cryptographic standards and a dynamic web interface, which is a solid solution in the confidential protection of data. In contrast to the previous systems relying on the simplistic key-dependent scrambling, both our platform use cryptographically secure algorithm: user-provided keys are

ISSN: 2961-5992

processed by PBKDF2 to securely derive messages, and AES-GCM is used to encrypt messages and guarantee their confidentiality and integrity. Embedding the encrypted data in pixel LSBs is also randomized with the help of a Cryptographically Secure Pseudorandom Number Generator (CSPRNG) fed with a variant of the secret key, which adds a lot of resistance to statistical steganalysis, brute force attacks.

The system was written in HTML5, CSS3, JavaScript in the front-end and Python (Flask) and Pillow library in back-end image processing and can be accessed by any modern web browser in a platform-independent manner. In this paper, the methodology that involves architectural design, cryptographic execution is described and the process of LSB embedding is also detailed. We offer our stringent analysis including the functional tests, the performance tests, the security assessment against typical steganalysis techniques, and formal usability study. The findings indicate that our site is a functional and trustworthy tool of covert digital communication as it has succeeded in integrating invisibility, high data storage, and security. The objective is to develop the disconnect between the theoretical principles of steganography and practical, secure, and generally deployable implementations that enable individuals and organizations to have greater data privacy.

II. Literature Review

The paper is built on the existing information on the field of data concealment algorithms and introduces the ways of concealing data secretly in text, images, and audio. LSB method is known to be easy and effective and therefore, a guiding process in the area. Studies point out that information must be placed meticulously on the various forms of media, otherwise the cover carriers may get very deteriorated. Another recommendation is to select lossless format like PNG to achieve the optimum steganographic output and prevent the loss of information.

The last trends in image steganography have included the application of chaotic systems, Lorenz and Rossler systems, and Bloom filters to enhance the security as well as the capacity. Such randomization of placement of embeddings is done using chaotic filters to ensure that the placement of embeddings is in a manner that is intractable, but to provide a very efficient storage and retrieval policy, Bloom filters are used. The combinations are made and formed to make them resistant to most forms of attacks especially when used on large scale [3]. Moreover, the chaotic image encryption scheme based on the Lorenz system has been proposed that generates the key matrices which are highly confused and diffused hence enhance the security of the encryption schemes [4]. It has also been shown that dual chaotic encryption scheme using both Lorenz and Rossler systems have higher entropy and can resist brutality attack and are therefore suitable in preprocessing in steganographic system [5].

More so, innovations extend to neural networks to deliver audio messages to image information, where an imperceptible embedding and high-quality images are acquired after adversarial training [6]. They have also applied convolutional neural networks to come up with better image-in-sound steganography methods, which are compression and noise resistant [7]. The technique often incorporates the least significant bits of picture and sound documentaries in order to hide hidden messages more effectively as well as to store multiple files, and a suggestion of enhancing the technique in the frequency field coding [8].

The hybrid model consisting of chaotic stream ciphers as well as steganography has been discussed as a means of improving the privacy of the data hiding. These ciphers are ever evolving the concealing technique to the extent that they have become difficult to detect and even more difficult to Steg analyze and crack by brute force [9]. The lightweight encryption of Lorenz system is effective and applicable in embedded and IoT systems since it is efficient and can be applicable in steganography integration in resource-constrained environments [10]. Invention of hybrid encryption in chaotic Lorenz equations and simulated Kalman filters have been developed that uses dynamic switching of key to obfuscate secure data and offer end-to-end security [11]. The comparative analysis of the steganography methods shows that there is a vacuum in the performance of the traditional methods and recommends the adaptive use of LSB and chaotic encryption as the alternative to improve the performance [12]. New LSB methods with 2D chaos enhance security and reliability to statistical attacks which make use of both space domain as well as frequency domain information to improve the quality of hiding and anti-detection methods [13]. It has also been confirmed that the Bülban chaotic map has achieved efficient and reliable image encryption which is secure compared to the statistical and entropy encryption and can thus be applied to real-time steganography [14].

However, the existing steganography tools, the vast majority of which are usability limited, are not always as easy as they can be made to seem. Neither do they tend to possess a very solidified security regarding key management and cross platform support. The research paper addresses such gaps because it develops a web-based application that protects user credentials and conceals information through encryption and thus it is simple to access the data using a simple interface. The concept is to have a safe system which is convenient to utilize and protects valuable information inbuilt in images with the help of another key. It further has a responsive web interface having a powerful backend on which to revert to the messages by keying in the stego-image, and the corresponding matching key. Decryption can only be done with the original key with which the process of encryption was done. The web is created using HTML, CSS, JavaScript, Python (Flask) and Pillow image processing library. This type of technology stack ensures fast performance, platform neutral and simple scalability and can be employed on an individual and small-scale level.

However, many existing steganography tools are limited by usability, often requiring programming or command-line expertise. They also frequently lack robust, unified security for key management and cross-platform support. This research addresses these gaps by developing a web-based application that protects user credentials and hidden information through encryption, making data retrieval simple via an intuitive interface. The goal is to establish a secure, user-friendly system that protects important data embedded within images with a separate key. This app offers a responsive web interface, combined with powerful backend support. By inputting the stego-image and the matching key, the

ISSN: 2961-5992

retrieval module makes it possible to recover the message. You can only use the original key to decrypt data encrypted by the system. HTML, CSS, JavaScript, Python, and the Flask framework were used to make this web application. The Pillow library is used for processing and editing images. Since this stack offers fast execution, independence from the platform, and can scale effortlessly, it is reliable. Anybody with a modern browser can use this application, making it suitable for home use or small businesses. The direct impact is that this research shows how web applications can now be used for hiding information via steganography. This technique can become especially valuable if encryption alone is not sufficient and sending encrypted files could be spotted. Staff at news organizations, those who report wrongdoing, or human rights campaigners may choose to exploit this technology for sending sensitive information privately [15].

The paper emphasizes that the developed web-based approach effectively combines the principles of steganography and implementation techniques to provide a proven, widely applicable method for confidential communication. Work is ongoing to further enhance this platform by supporting a range of file formats and by developing advanced authentication protocols and machine learning techniques for robust data hiding. Further, it is noted that this study provides a comprehensive and methodologically rigorous review of cryptographic techniques, integrating considerations of security depth, usability, and key management. The comparative evaluation of symmetric encryption algorithms highlights the superiority of AES across key sizes and platforms, while also emphasizing the often-overlooked practical dimensions of key handling [16].

III. METHODOLOGY

The establishment of web-based key-based image steganography platform adhered to the methodology of software development which is safe, efficient and user-friendly. It began by undertaking a rigorous analysis of the requirements in order to state the core objectives of the system. The main aim was to develop an internet product of embedding and retrieving sensitive text data in digital images with a secret key provided by the user. Platform independence, a clean and responsive interface, minimal performance overhead and high integrity and confidentiality were all non-functional requirements. Once the requirements were determined, it became possible to pick appropriate technologies and tools that would help to reach the intended objectives:

- **Frontend:** Frontend is implemented by means of HTML5, CSS3, and JavaScript to introduce a visual, responsive, and interactive user interface. It allows easy uploading of images, typing, and submitting keys in the browser through these technologies.
- **Backend:** Python based, Flask micro web framework since it is lightweight and easy to combine with third-party libraries. Flask allows the building of RESTful endpoints to support encoding and decoding services to ensure secure communication between the server processing and client inputs.
- **Image Processing:** All image processing operations were done by the Python Pillow library that is important in the steganographic functionality. Direct pixel-level access and manipulation is permitted in Pillow, which is required to execute the Least Significant Bit (LSB) steganography technique.

LSB method was selected because it is easy to use, efficient and does not affect much on image quality when used appropriately. The values of pixel colors in the least significant bits are altered to hide the secret message by the system. These LSB modifications can be perceived by the human eye to a great extent, and they do not affect the visual quality of the stego-image.

A. Embedding Process

Collection of the input

The service takes a plaintext message and a user input key.

Key-Dependent Scrambling

The secret key is an anti-embedding parameter, which scrambles or rearrange the binary bit-stream of the message. This forms a pseudo-encryption layer which makes the security much higher.

Payload Framing

Framing of the scraped binary message with certain marks is so as to guarantee its successful extraction:

1. Some magic stream of bytes (e.g., 0xDEADBEEF) which to indicate the existence of a hidden message.
2. An indicator of length giving the size of the hidden message.
3. A version number so as to enable future protocol changes.
4. A cryptographic random number salt/nonce which is a modification of the key by the PBKDF2.
5. A Message Authentication Code (MAC) which was produced by calculating AES-GCM to guarantee integrity and authenticity of messages to prevent tampering.
6. The unicode processing is adopted to support proper encoding and decoding of messages having different character sets.

LSB Embedding

The encoded bitstream is a framed, encrypted one and embedded systematically in the LSBs of pixel values of the chosen image. The process entails the even distribution and reduction of distortion. The secret key is used to seed a cryptographically secure pseudorandom number generator (CSPRNG) which determines the embedding order of pixels and channels. This renders the locations of embedding to be unpredictable in the absence of the key.

Output

The modified image is stored in a lossless format, e.g. PNG, to avoid the destruction of embedded information by the lossy compression (JPEG is avoided because of this risk).

ISSN: 2961-5992

B. Extraction Process

Collection of input

The stego-image along with the exact key at which the stego-image is being embedded is entered by the users.

LSB Retrieval

The application reads LSBs of every pixel in the same CSPRNG-seeded sequence as when embedding, to reconstruct the encrypted bitstream.

Key-Dependent Descrambling

This is a method using the given key where the system tries to rearrange or decrypt the bits.

Payload Unframing and Validation

This is done by first searching the magic bytes in the system. In case it is found, it reads the length, version, and retrieves the MAC. It is then verified by the secret key to ascertain that the integrity and authenticity of the message are intact through the MAC.

Message Recovery

In case the key is correct and in case the validation is successful, the original hidden message is recovered. In the event of wrong key entered or validation of MAC is not done, the system will produce an invalid or unreadable output and no access can be made by an unauthorized party.

C. Security Enhancements and Check-up

Introduction of Key-Based Mechanism

This offers an additional security in addition to basic steganography, and brute force or wrong extraction cannot happen.

Input Checking

Checking of the uploaded images has been done according to the format compatibility (PNG/BMP) and size constraints. The length of text, which is inputted is verified not to be more than the size of the pixels in the image to avoid overflow problems.

Error Handling

The application will accept misguided entries or unacceptable operations gracefully by showing the user easy to understand error messages.

Overall, the methodology is a lightweight, secure, and scalable web-based format of concealing data in images by means of the light steganography of the LSB, supplemented with a new key-dependent scrambling, a robust payload framing, and CSPRNG-seeded embedding, which makes it more secure. This is by using modern web development language and Python-image processing, which is an effective way of providing a genuine platform to hide and extract confidential textual information. The validation of inputs, handling of errors and ensuring that correct keys are used when making a decryption are all important aspects of the implementation.

IV. Results and Discussion

This study has been able to showcase an image steganography web-based tool, which is a sure and safe way of hiding digital data. The system has embedded the stealth mechanisms, the contemporary pictorial solutions as well as an intuitive design in order to simplify the procedures of concealing and retrieving the essential information. The application worked well to dynamically hide messages in pictures during implementation and testing. The key to the success of the system was the Least Significant Bit (LSB) data embedding algorithm which was used because it is easy to use, has high reliability, and reduces the visual effect to the minimum. The pixel values are adjusted, which is not visible to human eye and tests were carried out to ensure that there was no visible degradation of images after the data embedding. These results are consistent with the literature including the 2004 article by Chan and Cheng which suggested that LSB attacks are almost invisible.

This system is not just LSB-embarkation. It uses a key-dependent scrambling algorithm and strong payload framing, which consists of magic byte sequence, message length, version, salt/nonce and AES-GCM Message Authentication Code (MAC). This would help increase the security of the embedded data. The system is not just used to conceal simple messages but rather encrypt or order the messages with the help of an assigned key that is specified by the user. The fact that it has an access code will guarantee the safety of messages and unauthorized extraction using a different key will be virtually impossible. This is to counter an important weakness that was witnessed in the early steganography software where the content may be revealed in case the encryption technique is detected (See Figure 1, Figure 2, Figure 3, Figure 4, Figure 5 and Figure 6).

It is a fully web-based system unlike traditional software that may necessitate a separate program download and platform specific installation, makes it highly accessible and platform compatible with an interaction that is real-time. The tool can also be exploited by users without special technical abilities or skills. An application can be created with HTML5, CSS3, and JavaScript on the front-end and Python Flask with Pillow library to process images giving a fast and responsive application that is easy to maintain. Although the existing implementation mostly works with lossless image formats such as PNG and BMP to maintain data integrity, it is proposed that in the future, it will also be implemented to support DCT-based embedding of JPEG images to be more flexible.

Though key-based scrambling is central to our strategy, we could augment it with more advanced cryptographic functions such as AES-GCM or RSA to offer even greater security protection against more advanced steganalysis attacks. The existing system has a balance between a simple design and useful features that the system has without jeopardizing on the ease of use. The reliable security feature of the product was demonstrated by testing, which always gave correct results with messages appearing when the correct key was entered and without any message appearing as a result of a failed attempt with an incorrect key. The responsive design and the fact that the system provides a clear direction on what to do, in case of an error or uploading a wrong file, is another advantageous design of the system.

ISSN: 2961-5992

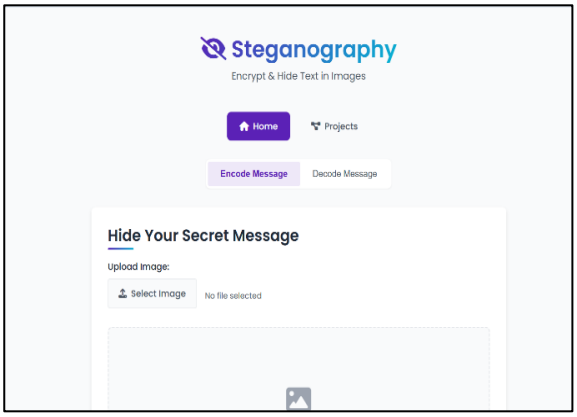

Fig. 1: Web Application Interface 01

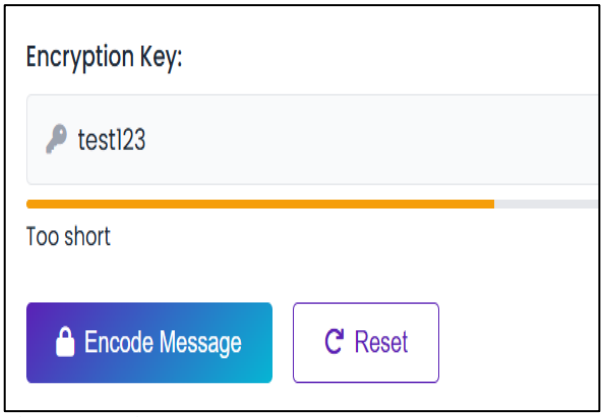

Fig. 4: Encryption Key

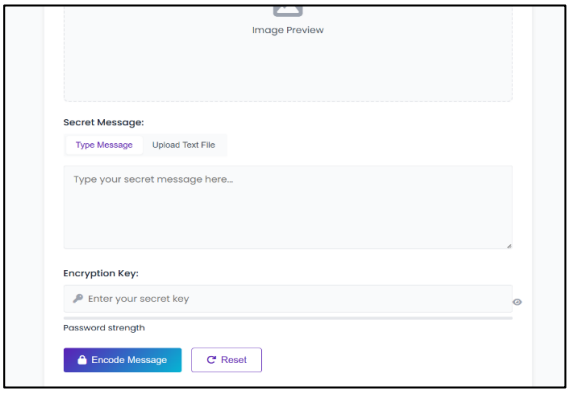

Fig. 2: Web Application Interface 02

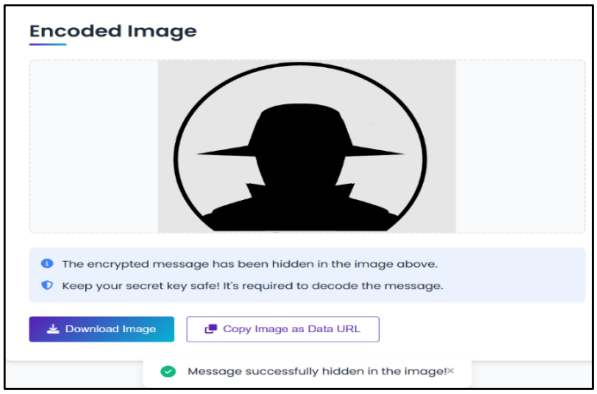

Fig. 5: Encoded Image

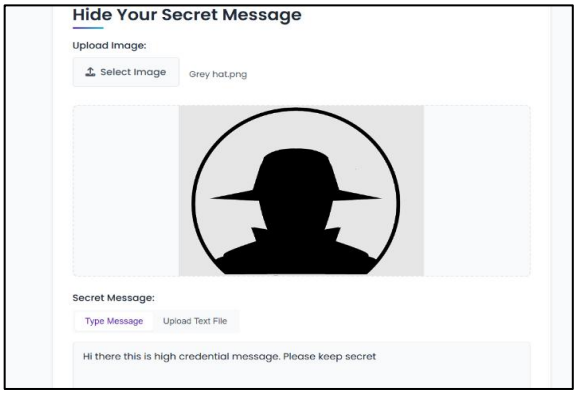

Fig. 3: Image Inserted

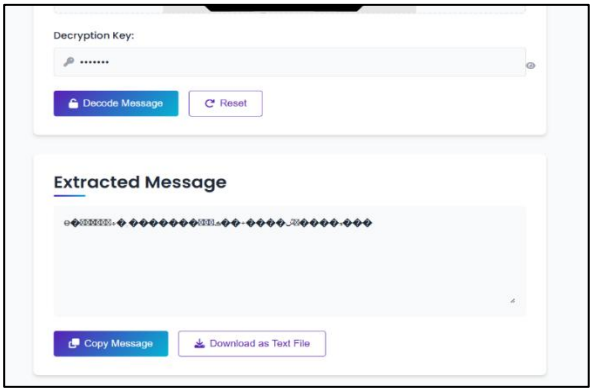

Fig. 6: Extracted Message

On the whole, this platform has proven to be a very appropriate example of showing that steganography, applied to the key-based techniques within a web-based setting, offers a rather viable and easy to use means of ensuring the safety of data. The opportunities to improve it in the future may involve the mobile interface, account management and user message logs, enhanced encryption protocols, and cloud storage integration to share the information safely. Audio processing or video processing capabilities would also make it more convenient. All these features are useful in establishing this steganographic tool as reliable, up-to-date and trustworthy in confidential communication.

V. Conclusion and Recommendations

The researchers were able to design and present an efficient, secure and user-friendly web-based image

ISSN: 2961-5992

steganography system on the basis of Least Significant Bit (LSB) insertion. The implementation of a new key-based mechanism of message bits scrambling as well as an efficient payload framing method prior to embedding was essential to the increase of confidentiality and integrity of the concealed data. The system enables embedding and recovery of text messages in digital images in a secure manner by simple and intuitive means, and thus usable even by non-technological users. Moreover, modern web technologies are used to guarantee platform neutrality, light-weight performance, and independence of software. The findings indicate that a steganography system, which is LSB-based, reinforced by user-provided keys and provided by an interactive web interface can be used as a secure medium of communication. The stego-images generated had an outstanding visual quality and there was no apparent degradation and, when decrypted using the right decryption key, message retrieval was always high. Such findings signify that the suggested system is not merely technologically valid, but it is also of much practical significance in terms of the applications of secure communications, including the protection of personal data and the confidential transactions of an enterprise level. The project will seal the gap between the abstract knowledge of steganography and its practical implementation by solving the shortcomings of any of the current tools, including the inability to secure it or to use it. It shows that safe online communication is attainable when it is carefully designed and appropriate mix of technologies is used.

To develop in the future some improvements are proposed. Support of audio and video files in the media formats will greatly extend the usefulness of the system. The implementation of more sophisticated cryptographic protocols like AES-GCM or RSA would also help the security of messages as it would not be a mere scrambling but a full-fledged encryption. The use of important derivation methods such as PBKDF2 and nonce-based encryption using AES-GCM would increase message confidentiality and authentication. Moreover, it would be better to add user authentication and access control to enhance flexibility as well as security.

The other area that has potential is the application of AI-based tampering detection systems that could be used to detect more advanced steganographic attacks and counter them. The ability to integrate cloud storage and share would make it easy to use collaboratively and at the enterprise level. The development of the next version may consider the addition of client-side encryption and embedding based on WebCrypto and Canvas APIs to reduce the disclosure of sensitive information to vulnerabilities of servers. It would be more flexible to extend the tool to facilitate JPEG embedding based on DCT-domain methods, particularly to users who will be utilizing compressed image formats. Strict performance and reliability evaluations, including PSNR, SSIM and capacity-distortion curves, and performance benchmarking of encode/decode time on standard data, such as BOSSBase or BOWS2, should also be included in future work. Furthermore, it would be appropriate to apply and experiment with different steganalysis techniques: chi-square, RS, SPA, or CNN-based detectors would be useful to compare the level of detectability and error rates to the current tools, including OpenStego or SilentEye. Lastly, a formal usability test, quantification of the SUS scores, time to complete tasks, and rate of errors would be a valuable input to the understanding of user experience and interface design enhancement.

In general, this project shows that in case of integrating steganography into the context of modern web technologies and key-based security measures, the latter can become a useful and efficient tool of safe, secret, and reliable digital communication.

REFERENCES

[1] B. Souvik, R. Bratati, and P. Debrupa, "Network security and cryptography: A review," Int. J. Adv. Eng. Manag., vol. 3, no. 7, pp. 4172–4176, 2021.

[2] S. Chandak, "Text, image and audio steganography," Int. J. Sci. Technol. Res. Innov., vol. 1, Apr. 2023.

[3] A. Salim et al., "Image steganography technique based on Lorenz chaotic system and bloom filter," Int. J. Comput. Digit. Syst., Aug. 2024.

[4] D. A. Q. Shakir, A. Salim, S. Q. A. Al-Rahman, and A. M. Sagheer, "Image encryption using Lorenz chaotic system," J. Tech., vol. 5, no. 1, pp. 122–128, Mar. 2023.

[5] A. Y. Albakri and O. Karan, "A two-layer for image encryption using Lorenz and Rossler chaotic systems," J. Multidiscip. Comput. Eng. Res., vol. 2024, pp. 9–19, Feb. 2024.

[6] Q. P. Huu et al., "Deep neural networks based invisible steganography for audio-into-image algorithm," arXiv:2102.09173, Feb. 2021.

[7] J. Ros et al., "Towards robust image-in-audio deep steganography," arXiv:2303.05007, Mar. 2023.

[8] A. Chadha and N. Satam, "An efficient method for image and audio steganography using least significant bit (LSB) substitution," arXiv:1311.1083, Sep. 2013.

[9] S. Haimour, M. R. Al-Mousa, and R. R. Marie, "Using chaotic stream cipher to enhance data hiding in digital images," arXiv:2101.00897, Jan. 2021.

[10] P. K. Singh, B. Jha, and S. Kumar, "An efficient and lightweight image encryption technique using Lorenz chaotic system," Math. Model. Comput., vol. 11, no. 3, pp. 702–709, 2024.

[11] N. Q. Ann et al., "A new hybrid image encryption technique using Lorenz chaotic system and simulated Kalman filter (SKF) algorithm," in Proc. 6th Int. Conf. Electr., Control Comput. Eng. (InECCE), Springer, Mar. 2022, pp. 441–453.

[12] A. Z. Abd Aziz, M. F. Mohd Sultan, and N. L. Mohamad Zulkufli, "Image steganography: Comparative analysis of their techniques, complexity and enhancements," Int. J. Percept. Cogn. Comput., vol. 10, no. 1, pp. 59–70, Jan. 2024.

[13] I. J. Kadhim et al., "A secure image steganography based on LSB technique and 2D chaotic maps," Comput. Electr. Eng., vol. 109, Art. no. 109566, 2024.

[14] M. Z. Talhaoui, X. Wang, and M. A. Midoun, "Fast image encryption algorithm with high security level using the Bülban chaotic map," J. Real-Time Image Process., vol. 18, pp. 85–98, 2021.

[15] M. J. A. Sabani and U. M. Rishan, "Effectiveness of ATM security mechanisms: A review analysis," in Proc. 9th Int. Symp. (Full Paper), South Eastern University of Sri Lanka, Oluvil, Nov. 27–28, 2019, pp. 234–242.

[16] T. N. Ahamed, M. J. A. Sabani, and M. S. Shafana, "Foundations of cryptographic defense: Navigating algorithmic strengths, key dynamics, and network security challenges," Sri Lankan J. Technol., vol. 6, no. 1, pp. 34–52, 2025.

ISSN: 2961-5992