I.J. Wireless and Microwave Technologies, **2026, 2, 26-35**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.02.03

A Comprehensive Review of Steganography Based Data Security System

R. Anusha Padmavathi
Department of Electronics and Communication Engineering, Government College of Engineering, Thirunelveli, Tamil Nadu, India.
E-mail: anushapadmavathiphd14@gmail.com

K. S. Dhanalakshmi
Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Virudhunagar District, Tamil Nadu, India.

K. Kalai Selvi
Government College of Engineering, Tirunelveli, Tamil Nadu, India.

Received: 21 July, 2025; Revised: 24 August, 2025; Accepted: 29 January, 2026; Published: 08 April, 2026

Abstract: The recent information and technology developments have impacted data utilization and showed the importance of storing different data types for various purposes. The huge amount of data exchanged between systems through the web, networks, and data storage systems are prone to third-party attacks and demands an effective data security system irrespective of the application. Researchers and developers have secured data using different steganography and cryptography techniques. Steganography uses different mediums to hide sensitive data such as images, videos, text, and audio. This review study discussed the importance of recent trends in steganography and cryptography systems in data security. Various methods and techniques of steganography and their hybrid systems, along with cryptography, have produced efficient results for data security. These methods and techniques are thoroughly reviewed to understand the development of a secure system based on steganography. The image-based steganography systems are widely used in several studies rather than video and audio-based steganographic systems. This paper aims to review different techniques practiced in steganography secure systems and specifically focused on Advanced Encryption Systems, Elliptic Curve Cryptography, and other hybrid systems since they are primarily used among developers and researchers in data security. Overall, developing an efficient security system based on steganography should be resilient to different types of third-party attacks and consider data integrity and data confidentiality to prevent loss of information.

Index Terms: Steganography, Data Security, Advanced Encryption System, Third Party Attack Elliptic Curve Cryptography

1. Introduction

Data security is the term that makes everyone question in our everyday life. In the era of Data science, data is the most preserved item for any field. The things that can be achieved with information could easily turnover major decisions. Governments and private institutions are now heavily reliant on data security. The data transferred between two mediums are prone to third-party attacks, and daily news on data breaches is evidence that any sort of data could be hacked connected to a network system or web.

This Data security is achieved by cryptography and steganography. Initially, research studies and developers used these techniques individually, later on, for an efficient data security system. However, the illicit people try to bring down these secured systems for several motives. And it often demands improvements in data security. The techniques used for data protection depend on the type of data, field of application, and type of hardware employed. The necessity of discussing the various aspects that influence the data security system for the sophisticated deployment of a secured model.

Cryptography and steganography serve different but complementary roles in data protection. Cryptography secures the content of information by transforming it into an unreadable form, while steganography conceals the existence of

This work is open access and licensed under the Creative Commons CC BY License.

the information within a carrier medium. Modern secure systems often combine both approaches to provide layered protection against detection and decryption attacks.

Need of the study

Data and information are the two assets that any institution in today's scenario has prioritized. The ability to transfer data with ease also makes the same exploit. This exploitation is dangerous when the data are sensitive and has precious information. For example, If biometric data of citizens [1] could be exploited. This data exploitation might result in further crimes like creating fraudulent bank accounts and other illicit activities, which cause further damage. It is really necessary to have an efficient data securing system that also should have the ability to survive third-party attacks.

In modern-day medical care, communication networks have better reach, and their usage is highly appreciated for people's comfort. But, things are connected to a network, and the data transferred through them are highly subjected to attacks for many reasons [2]. But some cases are often seen where the patient's data from an institution are potentially dangerous to the patients and their support.

The motivation for the study

Data security systems are highly required for any sophisticated developed system. In the industry 4.0 era, data protection is a widely discussed and researched arena. Data securing resulted in the prevention of many third-party interventions, which could cause damage to the system and develops further chaos. It the essential to develop a robust, secure system that should be prone to multiple interventions.

The importance of sensitive data like patient's medical data, individual personal data, Government policy data, and an institution's data records has their responsibility in securing future reference. These data are a potential target for illicit people who prey on damaging these systems. The data preservations should be taken well care for the sake of people's benefit.

The objective of the study

This proposed study aimed to review various techniques and methods of steganography that are employed to protect data using a steganography system. Specifically, it focused on how the advanced encryption system Elliptic Curve cryptography and other steganography-cryptography combination-based data securing models are effectively deployed for data security.

2. Systematic Review Methodology

This review follows a structured methodology to ensure comprehensive and unbiased coverage of existing research. Relevant studies were collected from major scholarly databases including IEEE Xplore, ScienceDirect, Springer and Google Scholar using keywords such as *steganography, cryptography, data hiding,* and *secure communication*. Papers were selected based on relevance, publication quality, and contribution to steganography-based security from 2018 to 2021.

Inclusion Criteria

Studies published in peer-reviewed journals and reputable conferences between 2018 and 2021 were included. Papers focusing on steganography, cryptography, or hybrid data security techniques with clear methodological descriptions and experimental evaluation were considered. Research addressing performance metrics, security analysis, or practical applications of data hiding was prioritized.

Exclusion Criteria

Studies lacking technical details, experimental validation, or relevance to data security through steganography or cryptography were excluded. Duplicate publications, non-English papers, and works focusing solely on theoretical cryptographic mathematics without application to data hiding were also omitted.

3. Recent Trends In Secured Steganography

Image-based steganography dominates current research due to the high availability of digital images, larger payload capacity, and well-established evaluation metrics such as PSNR and SSIM. Compared to audio and video, images allow simpler embedding models and lower computational requirements. This practicality explains why most experimental studies prioritize image carriers over other multimedia formats.

The steganography applications are wide, and often, the techniques are adjusted or changed to produce better results. In the recent study [3] on modified LSB images, a steganographic technique uses a filter algorithm [3] and a stream of passwords to hide the sensitive data in a non-sensitive file to ignore detection by human eyes. And hence these modified techniques provide better security. The recent developments in securing data are also subject to intrusion

attacks by strangers. And so, research studies started to focus on prone to attack subjects in securing data. The study used two points FFT steganographic technique [4] to encode messages and tested based on the "stirmark" benchmark [4]. This modified technique provides reliability for the secure system by preventing different kinds of attacks.

The technology and methods in the steganography system are often subjected to rapid developments. The most recent technique would have better efficiency than an older system. The time of the development makes the system easier to attack. So, a study made for securing patients' medical data [5] showed a new way of partitioning an image by Henon map would make the system security better. And as a result, the portioning method [5] shows better results when histogram analyses are made with other commercially available techniques. The third-party attack on data security has become a common challenge to overcome day by day, and therefore to improve the effectiveness of the data security, several methods are followed like this study [6] on improving data security in video-based steganography, using an algorithm to select the appropriate frames and then encrypt them. The frames are used to hide the data, giving an additional safety setup for data securing [6]. The study on three-layered security based on Blowfish-AES-RSA [7] has proven that it could provide better security, and it becomes harder to penetrate by brute force attack as the time takes to complete the attack is significantly high.

The advancements in image processing created the opportunity to develop three-dimensional images in steganography. Some researchers are not very aware of the recent developments in 3D steganography. The study on 3D steganography [8] showed various techniques and the development of 3D steganography over 15 years for data security. Also, IoT applications require security nowadays, as the protocols are open and are highly subjected to third-party attacks. Specifically, the medical care-based IoT applications require data security, and the study showed the usage of RFID and Blynk [9] in health care and concerns over data security. The two-level steganographic system has provided data security for the collected data [9].

The neural network-based steganographic systems have much attention among researchers; the study applied a deep neural network [10] and used particle swarm optimization, naïve bias classifier to detect and separate text and then apply the stego technique to retrieve the data. This embedded encoding and decoding is complex to penetrate by third-party attackers. For securing face portraits, a novel face image [11] based steganographic technique is used to protect the data transmitted while using identity documents and machine-readable travel documents. The secret message that needs to be transmitted is reshaped into an image encoded by the different neural network layers producing an encoded image. And another decoder network is used to decode the encoded image.

The results showed that the efficiency of the encryption is much better [11]. Apart from these, different neural networks methods are applied in steganography for several reasons. To generate the stego-text recurrent neural networks used [12], convolutional neural networks extract features, multi-layer perceptron, feed-forward networks, and long short term memory networks [12]. Evasion attacks on neural network-based secure systems are vulnerable and considered one of the few limitations in the neural network-based steganography security system. The study [13] proposed a new technique, Evasion attack steganography (EAST), which combines steganography with the water-marking technique to overcome the attacks on neural networks by encoding data as a label of the image. While many reviewed methods report improvements in embedding capacity and visual imperceptibility, their effectiveness varies significantly depending on application context. Spatial-domain techniques offer low computational complexity but are more vulnerable to statistical steganalysis, whereas transform-domain and chaos-based approaches provide stronger robustness at the cost of higher processing overhead. Similarly, neural-network-based steganography introduces new challenges including high training complexity, dependence on large datasets, and poor generalization across different media types.

Performance differences among steganographic algorithms mainly arise from the embedding domain and transformation strategy used. Transform-domain and chaos-based methods distribute hidden data across frequency components, improving robustness against statistical and compression attacks, whereas simple spatial-domain techniques remain more vulnerable despite lower computational cost.

4. Aes Based Cryptographic System

There are many research studies based on the AES cryptosystem. However, there is a discussion stating that AES's ability to encrypt images is considered as low [14] on speed and time because of generating heavy data with high redundancy properties. So, the study aimed to evaluate different chaos-based AES cryptosystems using a standard FFT algorithm [14] to measure the time spent on computing the encryption. The results have shown that the chaotic-based AES cryptosystem performed faster than AES-D systems [14].

A unique hybrid encryption system based on S-AES and chaos system [15] for images to reduce CPU and RAM usage for encryption and decryption. The encrypted and decrypted images are evaluated by histogram and correlation analyses to examine the changes in images. The proposed chaotic-based S-AES system for encrypting images worked efficiently in CPU and RAM usage while performing the encryption and decryption in MATLAB. Moreover, the proposed system has shown quicker encryption for image security.

The cryptosystem is based on a pseudo chaotic number generator [16] to provide robust security for practical applications. The encryption is supported by the diffusion layer based on horizontal addition diffusion and vertical addition diffusion followed by block cipher and decryption done in the inverse of encryption steps. The evaluation of encryption by the histogram and variable correlations. The confusion, diffusion property analysis, and time usage analysis show that the presented system successfully [16] and robust encryption for images.

The conventional AES-based cryptosystem required to transfer of a static key which would be exchanged during the synchronization of systems, and it often uses open channels for the initial transfer of a static key. This security flaw of transferring static keys could be avoided by the proposed chaotic-based AES cryptosystem [17] as it uses the dynamic key for security synchronization. This method was applied for image encryption and the histogram, correlation analyses were performed and concluded based on the statistical analyses and information entropy, the proposed system has shown the improvement and ability to be applied for practical encryptions [17].

The modified AES algorithm using a novel 5D chaotic cryptosystem [18] showed hyper-chaotic and randomization behavior. This behavior adds more unpredictability to the system and hence proposed system provides high key sensitivity and less computation for encryption. This system is suitable for multimedia applications where speed and security are desirable. The modified AES algorithm [19] by adding key adding transport operation in the initial Sub Bytes operation showed good performance on security based on the simulation. And it is highly suitable for file-sharing through insecure networks [19]. AES-based approaches offer better encryption and fast processing, but their real-world security depends heavily on key management and implementation design. Chaos-enhanced variants improve statistical randomness, yet they often increase computational complexity without always guaranteeing resistance to advanced cryptanalysis.

5. Hybrid Steganography-Cryptography Systems

The steganography system [20] is often considered a replacement for the cryptography system. But, it's a supplement for the cryptography system to provide further assistance in encryption work to enhance security. To reinforce the mobile device security, a different level of security based on hash function combinations and the AES algorithm is created.

Another hybrid system based on AES-128 and discrete cosine transform modulus three, a technique [21], encrypt and embeds in the form of the stegno-image, which provides robust security for the user's information. The secret message-matching with braille method along with disinformation strategy [22] in sending user information assists in securing data by allowing the attacker to read disinformation when they could breach the stegno layer, and creates deception of reading real information.

Also, the attacker might not know the disinformation has other information in it. This fake secret message method [22] could enhance security for the user's information, and it can be applied to text and image-based information.

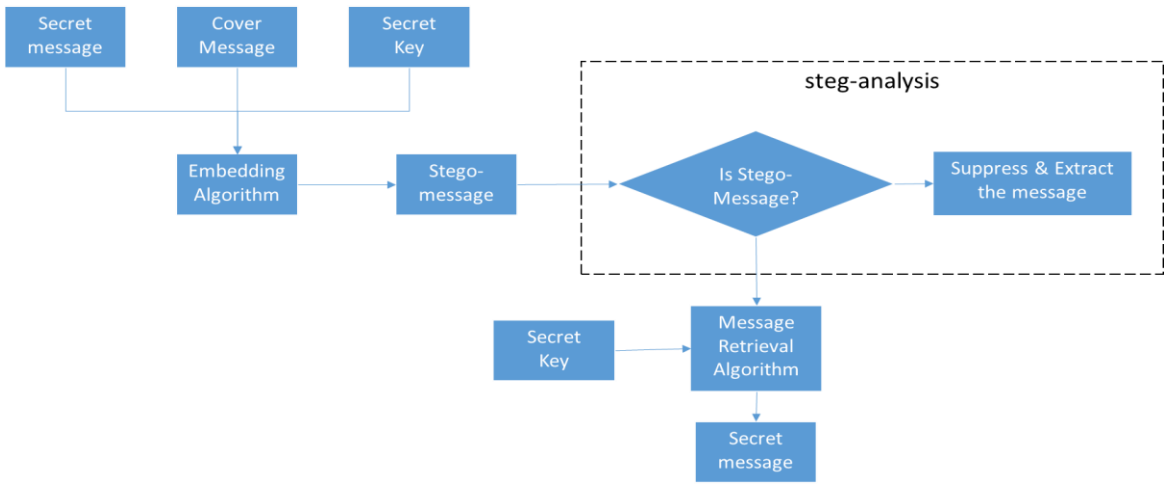


Fig. 1. steg-analysis in stegnography system

Some hybrid systems [23] use standard cryptographic-AES techniques and unique steganography systems. Here, the steganography system divides into two segments. Where the first segment is intended to generate the secret key which initiates the secure transfer of information. The Generation of Dyck words based on the secret key would be the second segment in a hidden channel. The stego-analysis of this system shows it has an advantage in security [23]. A typical stego-analysis has shown in fig. 1.

The mutual security algorithm combines symmetric filter bank block cipher and DWT techniques [24] to encrypt and embed the data in a cover image. To ensure the data integrity of the study includes an MD5 hash function and the

histogram analysis shows the hidden information successfully hidden behind cover images. The results conclude the data protection ability of the security algorithm [24].

The protection and claim for intellectual property [25] are in grave danger to piracy attacks. The need for protecting the ownership of the IP cores demands a secured design to establish the ownership claim stick to the original owner. To perform such assurance, by identifying the robust stego-mark embedded in the design, the legal ownership can be assigned to the original IP creator. Here, the stego-keys are used in larger, and embedding them in two phases gives better security and reliability [25].

6. S-Box Based Steganography System

The non-linearity of the S-box defines the quality of the encryption in a cryptosystem. The higher the non-linearity, the stronger encryption [26]. To achieve a higher non-linearity in S-box, the linear fractional transform parameters are controlled by a proposed scheme. This scheme is then tested for different criteria and applied to mobile app recommendations. The histogram analyses show that it has better security [26]. In another study, for implementing an encryption scheme [27] on the image, three stages incorporating Lucas sequence as the first stage, followed by using S-box and then using a sine logistic map. The histogram and correlation analyses of the proposed system are compared with other schemes, and it shows better security and takes low computing time, which makes it suitable for applications [27].

The algorithm based on a twofold confusion component in S-box [28]and anticipated non-linear component in digital steganography has experimented for different standard digital images. This proposed system has provided data confidentiality and is efficient in data hiding [28].

The authors [29] have applied three-dimensional chaotic maps like three-dimensional Chebyshev and three-dimensional logistic maps on the least significant bit and secret map technique to gain more security. Then the proposed system has been evaluated based on various parameters like PSNR, MSE, histogram, quality index, and information entropy. The concluded results showed the proposed system performed better than previously used methods based on the above-mentioned parameters. Also, the proposed system has shown some resilience towards third-party attacks, such as differential and statistical attacks. The proposed system also produces good quality stegno-images [29].

7. Secured Image Steganography Using Ecc Algorithm

The following discusses the studies on the Error Correction Code technique implementation in the steganography system. The study shows ECC algorithms [30] are embedded with cryptography and steganography system to improvise the data hiding techniques which prevents data intrusion. The authors [31] proposed an ECC-based security system to protect the data from statistical and dynamic attacks. The proposed system is robust to information loss and high speed of retrieving data. ECC provides efficient key exchange with smaller key sizes, making it suitable for lightweight security applications. However, ECC strengthens only the cryptographic layer, while overall system security still depends on the robustness of the steganographic embedding technique.

8. Hybrid Aes-Ecc Model For Data Security

A hybrid secure system based on AES and ECC is an efficient model for data security. The study [32] for securing the data in cloud storage devices uses a hybrid approach of using Advanced Encryption System and Elliptical Curve Cryptography to provide an optimized scheme for data sharing. This scheme was established with data integrity and security for the cloud storage application [32]. The study on using ECC as the first layer and 1-LSB 2-LSB as the second layer for data securing in the medical field discussed the positive and negative aspects of the proposed system. And it has been stated by the authors that any user institution can implement this technique to protect their data. Hybrid AES–ECC models combine fast data encryption with secure key distribution, improving layered protection. Nevertheless, increased system complexity may introduce processing overhead and unaddressed vulnerabilities in practical deployments.

9. Research Gap

Any Data security system has a concern for the safety and integrity of the data. Specifically, the recent developments make it necessary to develop a highly secured updated system. And therefore, developing a steganography system with an updated data secure model and techniques should be considered. Images mostly apply steganographic techniques, and the complexity of transferring contents and other information from images is rarely discussed [33].

The data security systems are subjected to third-party attacks, but studies rarely discuss the ability of their proposed techniques to sustain third-party attacks. Few studies only discuss the type of attacks [7] that happen on a secure system and differentiate the security system's performance on different attacking techniques [29]. Some studies

focus on attacks on the system and methods to overcome the attack. The rapid cloud storage and computing technology developments made them a potential target to be penetrated by third-party attacks [34, 35].

The payload capacity [31] of secure systems is rarely discussed. While performing tests and experiments or simulations, researcher's useless data to evaluate their models. But in a real-time application, data are huge and often organized in very large-scale structures. Some security systems could not handle the huge amount of data. The usage of non-commutative and non-associative structures for developing public key-based cryptography systems [28] should be considered for future studies. Additionally, despite its strong theoretical security, AES and ECC-based systems face practical limitations such as key management complexity, computational overhead in resource-constrained devices, and vulnerability to side-channel attacks during implementation. These challenges can affect real-time applications and IoT environments. Hence, optimization and secure key exchange mechanisms remain active research areas.

The analyzing techniques used in studies are inconsistent with other systems, where the type of evaluating the successful data transfer is widely varied in many studies. Some studies made a comparative analysis with attacking systems[29], and others performed histogram analyses where the data transfer through an image. Future research should focus on evaluating steganographic systems under real-time large-scale data conditions rather than small simulated datasets. There is also a need for standardized adversarial testing frameworks and cross-media embedding techniques that extend beyond images. Developing lightweight, attack-resilient models suitable for IoT and mobile platforms remains an important challenge.

10. Overall Challenges

When data bits replace the least significant bits [30], it becomes easier for statistical attacks by an intruder. And it often requires the optimal search algorithm to give a better position for hiding in the cover pixel. The techniques that are currently followed for the development of a steganography system have challenges [5] like low capacity, robustness, and high penetrating ability. These are essential for a secure system but, due to rapid developments in the field, it often requires new techniques and methodologies to overcome this issue.Although PSNR, MSE, histogram analysis, and entropy are widely used to evaluate steganographic performance, they mainly measure visual distortion and statistical similarity rather than true security strength. A system with high PSNR may still be vulnerable to advanced steganalysis or cryptographic attacks. Therefore, security evaluation must also consider attack resistance and key robustness.

The steganography system uses a dynamic technique [33] which has a challenge in processing latency while embedding incapacity [30]. The data security system is highly susceptible to third-party attacks [7], where the encryption and fail-safe systems are easily turned down by strangers and often require more attention with updated techniques. Steganographic systems face multiple categories of attacks, including statistical attacks that detect hidden patterns, differential attacks that analyse pixel variations, brute-force attacks targeting key spaces, and ML (Machine-Learning)-based steganalysis that learns embedding artifacts. Each attack exploits different system weaknesses, requiring adaptive and multi-layered defense strategies. Understanding these attack models is essential for designing robust security frameworks.

11. Applications

The stenographic-based security system is widely applied to protect data. Depending on the application, the type of technique used differs. Steganographic-based systems are used to protect sensitive data such as Iris bio-metric data [36] of individuals collected for identifications. This sensitivity should be protected; if not, the biometric data could be used for other miscellaneous activities.

Nowadays, mobile authentication is inevitable, and people often use it [20]. The system that supports the security of these authentications gives the user confidentiality and assurance. An individual's computer data and files [37] also can be protected by secure steganographic systems. Table 1 summarizes the reviewed studies along with its key contributions and limitations to facilitate a clearer comparative analysis.

Table 1.Survey table on using steganography and cryptography

References	Algorithm / Technique	Application	Comments	Limitations
[36]	Two fish and Triple data decryption algorithms and Least Significant Bits	Securing Iris templates as a part of protecting biometrics	The proposed system based on securing and retrieving produces an embedded image that human eyes cannot easily identify.	Limited attack analysis
[38]	Blowfish, Edge detection algorithms, and the Least significant bit	For transferring data through image	The study uses blowfish for encryption and edge detection at various stages to secure the image.	Higher complexity
References	**Algorithm / Technique**	**Application**	**Comments**	**Limitations**

[39]	RSA and two sequential layer steganography(video)	Data security using video files	15 different size video files were used to test the proposed methodology in a MATLAB simulation and studied the methods and effects of 1-LSB, 2-LSB, and 3-LSB.	Large storage requirement
[37]	RSA and two sequential layer steganography(audio)	Securing text data on a computer	15 different size audio files were used for evaluation. The proposed study showed that 3-LSB had better accuracy than 1-LSB and 2-LSB.	Sensitive to noise
[20]	LSB, AES, and hash	Mobile device security authentication	This study experimented with three different combinations for security applications from the hash, AES, and LSB, and the results were discussed based on confidentiality, Integrity, and Authentication.	Limited payload
[40]	Chaos function, Canny edge detector, and LSBMR	For transferring data through image	The cover image influences the quality of steganography.	Dependent on image type
[41]	Discrete cosine transform, Elliptic curve cryptography	For transferring data through image	The proposed study can produce an image that has a higher Peak signal-to-noise ratio, Structural similarity index values.	High computation
[42]	Elliptic curve cryptography and image steganography	For securing medical data	This method can be used to protect any sensitive data that needs protection.	Key management complexity
[32]	Advanced-Data encryption and elliptic curve cryptography	For securing data in cloud storage	The results showed better results for ensuring authentication and data integrity.	System complexity
[43]	Blowfish, AES	File security in network servers.	This method reduces the computational cost and is stronger than the triple-DES technique.	No steganography used
[2]	RSA, Blowfish	Data security in Medical care	This study used a Health care dataset from the New York state department to compare with the existing technique, and the results showed that the proposed model has better data security and data retrieval ability.	Computational overhead
[35]	Elliptic curve cryptography	Securing medical data	This proposed system used two layers of security, the first layer of security would be based on the ECC, and the second layer of steganography uses 1-LSb and 2-LSB. This study tested medical data like X-Ray, CT, and MRI scan data.	Limited robustness testing
[7]	Blowfish-RSA-AES	For transferring data through image	The proposed system effectively secures data, as the brute force attack takes a significantly higher time to break in.	High processing time
[31]	Elliptic curve cryptography	For transferring data through image	The proposed system was based on providing better data security and integrity for the high payload capacity systems.	No ML attack testing

Critical Analysis

Figure 2 displayed the critical analysis of the studies that have been used in this survey based on the year.

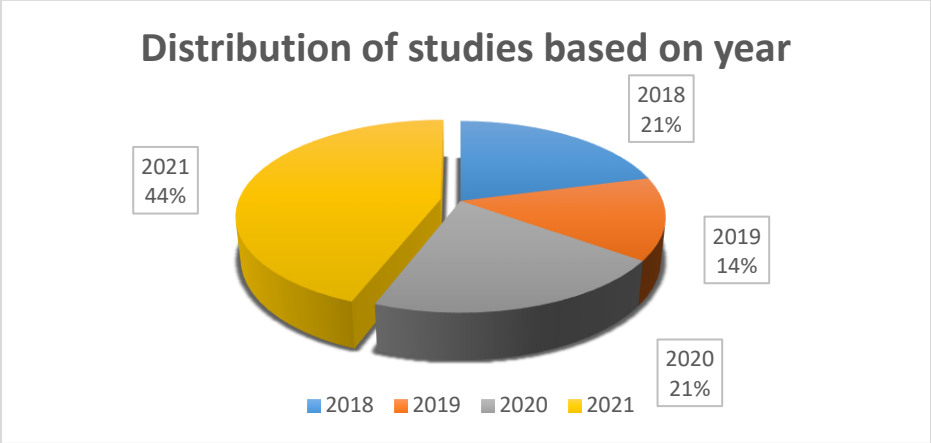


Fig. 2. Distribution of studies based on year

Summary

In this survey study, we have discussed the importance of data security and different techniques employed in securing data using steganography and cryptography systems. The data security systems are a potential target for third-party attacks regularly discussed. However, the studies that are based on data security should evaluate different types of attacks with huge amounts of data in a real-time scenario.Future steganography-based security systems must integrate adaptive embedding strategies, strong cryptographic key management, and resistance to AI-driven steganalysis. Evaluation standards should move beyond visual quality metrics toward attack resilience and real-world scalability. Hybrid intelligent systems combining cryptography, steganography, and machine learning are expected to define the next generation of secure communication models.

References

[1] T. Sridevi, P. M. Rao, and P. Ramaraju, "Wireless sensor data mining for e-commerce applications," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 14, pp. 462-470, 2018.

[2] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-19, 2021.

[3] M. Islam, T. Tanni, S. Parvin, M. Sultana, and A. Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password," *Information Security Journal: A Global Perspective,* vol. 30, pp. 359-370, 2021.

[4] N. Mukherjee, G. Paul, and S. K. Saha, "Two-point FFT-based high capacity image steganography using calendar-based message encoding," *Information Sciences,* vol. 552, pp. 278-290, 2021.

[5] M. M. Hashim, A. A. Mahmood, and M. Q. Mohammed, "A pixel contrast based medical image steganography to ensure and secure patient data," *International Journal of Nonlinear Analysis and Applications,* vol. 12, pp. 1885-1904, 2021.

[6] H. Milad, O. Haydar, and A. Diab, "Enhancement the Security and Efficiency of Video Steganography Using Frame Selection, Data Compression, and Encryption."

[7] T. S. Gupta and R. Srivastava, "Advanced-Data Encryption using Three-Layered Hybrid Cryptosystem and Secured Key Storing using Steganography," 2021.

[8] R. Tanwar, U. Pilania, M. Zamani, and A. A. Manaf, "An Analysis of 3D Steganography Techniques," *Electronics,* vol. 10, p. 2357, 2021.

[9] H. A. Khan, R. Abdulla, S. K. Selvaperumal, and A. Bathich, "IoT based on secure personal healthcare using RFID technology and steganography," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 11, 2021.

[10] D. Pandey, S. Wairya, R. S. Al Mahdawi, S. A.-d. M. Najim, H. A. Khalaf, S. M. Al Barzinji, *et al.*, "Secret data transmission using advanced steganography and image compression," *International Journal of Nonlinear Analysis and Applications,* vol. 12, pp. 1243-1257, 2021.

[11] F. Shadmand, I. Medvedev, and N. Gonçalves, "CodeFace: A Deep Learning Printer-Proof Steganography for Face Portraits," *IEEE Access,* vol. 9, pp. 167282-167291, 2021.

[12] R. Gurunath and D. Samanta, "Insights into Artificial Neural Network techniques, and its Application in Steganography," in *Journal of Physics: Conference Series*, 2021, p. 012043.

[13] S. Ghamizi, M. Cordy, M. Papadakis, and Y. Le Traon, "Evasion Attack STeganography: Turning Vulnerability Of Machine Learning To Adversarial Attacks Into A Real-world Application," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 31-40.

[14] Y. Zhang, "Test and verification of AES used for image encryption," *3D Research,* vol. 9, pp. 1-27, 2018.
[15] Ü. Çavuşoğlu, S. Kaçar, A. Zengin, and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dynamics,* vol. 92, pp. 1745-1759, 2018.
[16] Z. Qiao, S. El Assad, and I. Taralova, "Design of secure cryptosystem based on chaotic components and AES S-Box," *AEU-International Journal of Electronics and Communications,* vol. 121, p. 153205, 2020.
[17] C.-H. Lin, G.-H. Hu, C.-Y. Chan, and J.-J. Yan, "Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm," *Applied Sciences,* vol. 11, p. 1329, 2021.
[18] S. A. Mehdi, K. K. Jabbar, and F. H. Abbood, "Image encryption based on the novel 5D hyper-chaotic system via improved AES algorithm," *International Journal of Civil Engineering and Technology,* vol. 9, pp. 1841-1855, 2018.
[19] A. A. Thinn and M. M. S. Thwin, "Modification of AES algorithm by using second key and modified subbytes operation for text encryption," in *Computational science and technology*, ed: Springer, 2019, pp. 435-444.
[20] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, and A. Gutub, "Secure mobile computing authentication utilizing hash, cryptography and steganography combination," *Journal of Information Security and Cybercrimes Research,* vol. 2, pp. 73-82, 2019.
[21] M. M. Abur, S. B. Junaidu, S. E. Abdullahi, and A. A. Obiniyi, "Securing User's Attributes on Transit to the Cloud using AES-128 bits Cryptography and DCTM3 Steganography Techniques," *Scientific and practical cyber security journal,* 2019.
[22] M. E. Shaheen and A. H. S. Saad, "Using Disinformation to Promote the Security of SMMWB Image Steganography Method," *International Journal of Computer Applications,* vol. 975, p. 8887.
[23] M. Saračević, S. Adamović, V. Miškovic, N. Maček, and M. Šarac, "A novel approach to steganography based on the properties of Catalan numbers and Dyck words," *Future Generation Computer Systems,* vol. 100, pp. 186-197, 2019.
[24] S. Saraireh, J. Al-Saraireh, and M. Saraireh, "Integration of Hash-Crypto-Steganography for Efficient Security Technique," *International Journal of Circuits, Systems, and Signals Processing,* vol. 12, pp. 274-278, 2018.
[25] A. Sengupta and M. Rathor, "Crypto-based dual-phase hardware steganography for securing IP cores," *IEEE Letters of the Computer Society,* vol. 2, pp. 32-35, 2019.
[26] S. Beg, N. Ahmad, A. Anjum, M. Ahmad, A. Khan, F. Baig*, et al.*, "S-box design based on optimize LFT parameter selection: a practical approach in recommendation system domain," *Multimedia Tools and Applications,* vol. 79, pp. 11667-11684, 2020.
[27] S. Wassim Alexan, M. ElBeltagy, and A. Aboshousha, "Image Encryption Through Lucas Sequence, S-Box and Chaos Theory."
[28] S. I. Batool, I. Younas, M. Khan, and N. Yaqoob, "A new technique for the construction of confusion component based on inverse LA-semigroups and its application in steganography," *Multimedia Tools and Applications,* pp. 1-21, 2021.
[29] A. ALabaichi, M. a. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International journal of electrical & computer engineering (2088-8708),* vol. 10, 2020.
[30] S. Kamil, M. Ayob, S. N. H. SHEIKHABDULLAH, and Z. Ahmad, "Challenges in multi-layer data security for video steganography revisited," *Asia-Pacific J. Inf. Technol. Multimed,* vol. 7, pp. 53-62, 2018.
[31] S. D. Tatavarthi and V. Enireddy, "HYBRID TECHNIQUE FOR HIGH PAYLOAD CAPACITY USING ECC AND STEGANOGRAPHY," *Turkish Journal of Physiotherapy and Rehabilitation,* vol. 32, p. 3.
[32] S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage," *Electronics,* vol. 10, p. 2673, 2021.
[33] J. Liu and Y. Zhang, "A Dynamic Steganography Method for Web Images with Average RunLength-Coding," *Journal of Computer Science Research,* vol. 3, 2021.
[34] R. Denis and P. Madhubala, "Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment," *International Journal of Computer Networks and Applications (IJCNA),* vol. 7, pp. 208-230, 2020.
[35] E. S. B. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography," *IJCSNS,* vol. 20, p. 232, 2020.
[36] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools and Applications,* vol. 79, pp. 23483-23506, 2020.
[37] N. Al-Juaid and A. Gutub, "Combining RSA and audio steganography on personal computers for enhancing security," *SN Applied Sciences,* vol. 1, pp. 1-11, 2019.
[38] N. H. Hassoon, R. A. Ali, H. N. Abed, and A. A.-J. Alkhazraji, "Multilevel hiding text security using hybrid technique steganography and cryptography," *International Journal of Engineering & Technology,* vol. 7, pp. 3674-3677, 2018.
[39] N. A. Al-Juaid, A. A. Gutub, and E. A. Khan, "Enhancing PC data security via combining RSA cryptography and video based steganography," *Journal of Information Security and Cybercrimes Research,* vol. 1, pp. 5-13, 2018.
[40] A. Delmi, S. Suryadi, and Y. Satria, "Digital image steganography by using edge adaptive based chaos cryptography," in *Journal of Physics: Conference Series*, 2020, p. 012041.
[41] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access,* vol. 8, pp. 25777-25788, 2020.
[42] E. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography," *Int. J. Comput. Sci. Netw. Secur.(IJCSNS),* vol. 20, pp. 1-8, 2020.
[43] B. L. S. Prasanna, P. Meghana, and M. I. B. Venkateswarlu, "Double encryption using Private Key and Content Based Public Key," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 7, 2018.

Authors' Profiles



R.Anusha Padmavathi working as Assistant Professor in the department of Electronics and Communication Engineering, in GOVERNMENT COLLEGE OF ENGINEERING, THIRUNELVELI, TamilNadu, India. I had graduated with BE degree in Electronics and Communication Engineering from Anna University, Chennai in 2012 and M.E in VLSI DESIGN from PSN ENGINEERING COLLEGE in THIRUNELVELI 2017. My area of interest is Wireless Network Security, image processing and vlsi design.



K. S. Dhanalakshmi working as Assistant Professor in the department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, VirudhunagarDistrict, TamilNadu, India. I am graduated with BE degree in Electronics and Communication Engineering from Anna University, Chennai in 2007 and M.Tech in Digital Communication and Network Engineering from Kalasalingam University, Krishnankoil in 2011. I have received the PhD degree in Intrusion Detection System for Wireless Networks from Kalasalingam Academy of Research and Education, Krishnankoil in 2018. My area of interest is Wireless Network Security, Satellite Communication and Signal Processing.



K.Kalai Selvi completed B.E (Electronics & Communication Engineering) in 2003 at Government College of Engineering, Tirunelveli, Tamil Nadu, India & M.E (Optical Communication) in 2010 at Alagappa Chettiar Government College of Engineering & Technology, Karaikudi, Tamil Nadu, India. Working as Assistant Professor in Government College of Engineering, Tirunelveli, Tamil Nadu. Has 15 years of teaching experience.

How to cite this paper: R. Anusha Padmavathi, K. S. Dhanalakshmi, K. Kalai Selvi, "A Comprehensive Review of Steganography Based Data Security System", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.2, pp. 26-35, 2026. DOI:10.5815/ijwmt.2026.02.03