Literature Review on Steganography and Cryptography Integrated file sharing system

Sandra KV, **Adith PV, Harshith TV, Aswin P, Anu Treesa George** (Assistant Professor)

Department of Computer Science and Engineering
(Cyber Security) Vimal Jyothi Engineering
College Chemperi, Kannur
Sandra.k.v1234@gmail.com

***Abstract*—The increasing rise of digital communica- tion necessitates innovative techniques to safeguarding sensitive data from sophisticated cyberthreats. This study offers a solid basis for secure data transport by fusing the most recent advancements in steganographic and crypto- graphic approaches. Significant improvements in dura- bility, data capacity, and imperceptibility are provided by techniques including wavelet transformations, DNA- based mechanisms, modulus-based embedding, and edge detection. While advanced steganographic techniques like Pixel Value Differencing (PVD), histogram shifting, and discrete wavelet transformations facilitate data con- cealing, cryptographic techniques like AES and DNA cryptography are examples of approaches that improve encryption. Integrating these strategies ensures end-to- end security and scalability in sectors like government communication, healthcare, finance, and the Internet of Things. Steganography and cryptography together hold considerable promise for improving data security, even in the face of challenges like steganalysis vulnerability and computational complexity. Future research should focus on computing efficiency, adaptive algorithms, and quantum-resilient cryptographic systems in order to address emerging risks and expand application in in- creasingly interconnected digital ecosystems.**

index terms - Image Steganography , Cryptography , Secure File Sharing , ECDH.PVD,Digital Security Secure Communication

I. INTRODUCTION

The rapid growth of digital communication and the proliferation of cyber threats necessitate robust mechanisms for safeguarding sensitive information. As networks and systems become more interconnected, traditional data security techniques frequently fail to withstand sophisticated attacks. To overcome these obstacles, sophisticated cryptographic and stegano- graphic methods must be combined to guarantee sen- sitive data's security and imperceptibility.This study presents a new secure file transfer system that com- bines Pixel Value Differencing (PVD) for stegano- graphic data embedding and Elliptic Curve Diffie- Hellman (ECDH) for cryptographic key exchange. Utilizing ECDH, the system guarantees secure and effective key exchanges, offering a portable yet reliable solution appropriate for resource-constrained settings like mobile platforms and Internet of Things devices. By encoding confidential information into pixel inten- sity variations, the PVD approach improves data hiding while preserving high imperceptibility and resistance to detection. By combining these methods, a dual-layer security system that addresses steganographic and cryptographic flaws is provided. The system can accomplish end-to-end security while maintaining the integrity and quality of the multimedia cover files because to the computational efficiency of ECDH and the flexibility of PVD. Applications in delicate fields where secure and discreet data delivery is crucial, such government communication, healthcare, and finance, benefit greatly from this strategy.

This study pushes the boundaries of secure file transfer systems by fusing the advantages of steganog- raphy with encryption. It emphasizes how ECDH and PVD integration is both feasible and scalable, offering a strong basis for handling today's data security issues in a variety of operational situations.

II. LITERATURE SURVEY

M. Indrasena Reddy et al.[1] suggest a technique that combines wavelet transforms with encryption and steganography to improve safe data transfer. The text is encrypted using the Data Encryption Standard (DES) algorithm and then embedded using the Least Sig- nificant Bit (LSB) technique into the LL subband of a wavelet-transformed image. The original image is split into four subbands (LL, LH, HL, and HH) using wavelet decomposition, and the encrypted text is hidden in the LL subband to provide reduced visual distortion and improved security. Modifying the least important portions of pixel values renders the changes undetectable to the human sight, making the procedure resilient. Once the encrypted text has been embedded, the watermarked image is reconstructed using an inverse wavelet transform and sent. Forward wavelet transformation is used to extract the hidden data at the receiver's end, and the same DES key is used to decrypt it. By fusing the advantages of encryption with secret communication, the combi- nation of cryptography and steganography improves security. Nevertheless, the strategy is limited by the DES algorithm's drawbacks, as its 56-bit key length makes it vulnerable to brute-force attacks. Further- more, the method's scalability for high-capacity data transmission may be limited by its dependency on the LL subband for data embedding. Notwithstanding these limitations, the method shows promise as a workable and efficient way to transmit data securely over public or unprotected networks. Furthermore, the method's scalability may be limited due to its reliance on the LL subband for data embedding, especially for high-capacity data transmission. Dividing the data among several subbands or using adaptive embedding techniques to maximize embedding efficiency while maintaining imperceptibility could help accommodate larger payloads without significantly affecting the im- age quality.

Abbas Cheddad et al.[2] offer a thorough analysis of digital image steganography, dividing approaches into three categories: adaptive, frequency domain, and spatial domain. The principal objective is to im- prove imperceptible safe data embedding in photos. Though they are known for being straightforward, spatial domain techniques like least significant bit (LSB) replacement are quite vulnerable to visual and statistical detection. The use of transforms such as the discrete cosine transform (DCT) and the discrete wavelet transform (DWT) in frequency domain ap- proaches provides enhanced resilience to attacks by en- coding information in changed coefficients. Neverthe- less, these techniques require more processing power. Adaptive steganography is a noteworthy development that uses image statistics to more securely embed data. Although these techniques have advantages, they are limited by the requirement for images with a lot of noise. The requirement for noise-rich pictures and their vulnerability to advanced steganalysis tools limit these approaches, despite their advantages. The au- thors emphasize how urgently techniques that strike a balance between capacity, security, and computational efficiency are needed. The authors also go through the trade-offs that come with designing steganographic systems, especially in practical situations where com- puting limitations are essential. For low-power devices or real-time communication, methods like DWT-based embedding that need a lot of processing power might not be the best option. On the other hand, security may be jeopardized by lightweight techniques that put speed and efficiency first.

Wavelet-based image compression methods are thor- oughly examined by V. V. Sunil Kumar and M. Indra Sena Reddy [3], who highlight the importance of these methods in contemporary image processing. In con- trast to conventional discrete cosine transform (DCT)- based techniques, the authors describe how wavelets localize information in both the spatial and frequency domains, allowing for more efficient compression. High compression ratios without sacrificing image quality are achieved by methods like discrete wavelet transform (DWT) and embedded zerotree wavelet (EZW) coding. When it comes to lowering the storage and transmission requirements for big datasets, these techniques are especially beneficial. Nevertheless, the paper points up difficulties such the computing com- plexity of sophisticated wavelet schemes and blocking artifacts in traditional methods. In order to increase the wavelet-based compression techniques' real-time usability, the authors recommend additional modifica- tions. In order to increase wavelet-based compression techniques' real-time usability and strengthen their integration with steganographic and other multimedia applications, the authors recommend additional opti- mizations. The authors also highlight wavelet compres- sion's potential for safe data concealing in their discus- sion of its integration with steganographic applications. Researchers can increase efficiency and security by embedding data in compressed wavelet coefficients, which lowers the chance of discovery while requiring less bandwidth. Applications like cloud storage and encrypted communication benefit greatly from this synergy between steganography and compression.

Ki-Hyun Jung and Kee-Young Yoo [4] describe a technique for data concealing that embeds hidden data into digital photographs while preserving ex- cellent visual quality by combining edge detection techniques with image interpolation. The suggested methodology uses edge detection to make sure that secret data are embedded into edge regions, which are less susceptible to visual artifacts, and enlarges the cover picture using interpolation techniques to boost embedding capacity. The technique has a peak

signal-to-noise ratio (PSNR) of 44.71 dB, an average embedding capacity of 391,115 bits, and a quality index of 0.9568 for grayscale images. This method's main benefit is its capacity to integrate a lot of data without sacrificing the stego-images' visual quality. The approach guarantees minimum distortion and re- silience to attacks by focusing on edge regions for data embedding. According to experimental findings, the suggested approach performs better in terms of both capacity and quality than alternative reversible data hiding strategies. Nevertheless, there is a trade-off between capacity and image quality because a stronger embedding may result in a lower-quality image. Fur- thermore, the method's reliance on precise edge iden- tification may provide difficulties when working with noisy or complicated images. The suggested approach is appropriate for usage in digital watermarking and secure data transmission since it offers a practical solution for applications needing high-capacity data concealing and high-quality image recovery. The study emphasizes how incorporating adaptive edge detection techniques could improve the embedding procedure even more. Advanced methods like Canny or Sobel edge detection can be used to increase edge local- ization accuracy, decrease embedding artifacts, and improve imperceptibility. Additionally, the approach becomes more robust for complicated or noisy images by integrating machine learning-based edge detection, which may dynamically modify embedding positions based on image properties.

Thien et al.[5] provide a modulus-based data hiding method that is superior to the conventional Least Significant Bit (LSB) substitution. The major objective is to preserve decent visual quality while achieving a high hiding capacity. This technique's mainstay is the modulus operation, which guarantees less distortion than straightforward LSB substitution. By adding fake edges to smooth regions, traditional LSB approaches lower image quality and increase the visibility of concealed data. The suggested approach reduces these distortions by choosing appropriate integer values dur- ing the embedding process, which improves the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). Furthermore, it can handle numbers one by one in real time without the need for base trans- formation, which makes it appropriate for streaming applications. With encoding and decoding durations far less than those of LSB techniques enhanced by genetic algorithms, the method is also computationally effi- cient. However, the primary disadvantages are a trade- off between embedding capability and imperceptibility, as well as possible security flaws against sophisticated steganalysis tools. The modulus-based data concealing technique presents a number of avenues for future development. One such improvement is the incor- poration of adaptive modulus functions, which, like adaptive steganography techniques, modify according to the content of the image. This could enhance the harmony between image quality and hiding capacity, particularly in intricate or textured photos.

AES algorithm-based wavelet-based cryptography and secure data transmission were proposed by M. Indra Sena Reddy et al.[6] Many researchers have looked into combining steganography and cryptogra- phy to improve data security in digital communication. In one prominent method, the Least Significant Bit (LSB) technique for image steganography is used with the Advanced Encryption Standard (AES). Especially for image-based communication, the main objective of this integration is to offer a strong method for safe data transmission. The plaintext is converted into ciphertext and rendered unreadable to unauthorized users by the use of AES, a symmetric key cryptographic method. This approach is preferred due to its effectiveness and robust security features, which enable quick process- ing while preserving high data protection standards. Steganography, on the other hand, is a supplementary method that hides the presence of a message inside a cover medium, such an image. Because it modifies the least significant pixel values without substantially compromising the image's visual quality, the LSB technique is frequently used to encode hidden data into pictures. By using this method, the concealed information can continue to be invisible to the naked eye. Adaptive algorithms that can dynamically modify embedding tactics based on the content of the cover image are one of the issues that still exist in the industry despite the developments. It is anticipated that future studies will tackle these issues, improv- ing the efficacy of steganographic and cryptographic techniques in protecting private data in a digital envi- ronment that is becoming more interconnected by the day

To improve data security in cloud-based IoT in- frastructures, Suyel Namasudra et al. suggested a cryptosystem that combines DNA cryptography and DNA steganography [7].By using a lengthy, randomly generated key to encrypt sensitive information and then embedding it in a cover image, the primary objective is to offer a twofold layer of protection. The main parts of this system are the steganographic technique, which conceals the encrypted data in an image, and the DNA-based cryptography mechanism, which uses the four DNA bases (A, T, C, and G) to encode information. By using this method, the system hopes to increase resis- tance to several types of attacks, including DDoS and statistical attacks, while also lowering computing cost and improving data security. IoT devices, a gateway, a data owner, a cloud service provider, and data users are among the several entities involved in the architecture. Data is gathered by IoT devices and transmitted to the data owner via the gateway, where it is encrypted, concealed in a steganographic image, and then saved

on the cloud server. Because of the fine-grained access control made possible by this design, only authorized users will be able to access the encrypted data. The effectiveness of the suggested cryptosystem's key gen- eration, data encryption, and decryption procedures is a major benefit. These processes are essential for real-time applications in industries like banking and healthcare.

Regarding cryptography with steganography, Osuo- lale et al. proposed the paper "Secure Data Trans- fer Over the Internet Using Image CryptoSteganogra- phy" [8]. The notion of "crypto-steganography," which combines the two methods for improved security, is presented by the author. In addition to discussing a variety of steganography techniques, such as how to conceal messages in text, photos, audio, and video, they also examine the distinctions between secret key and public key steganography. A thorough examination of cryptography's foundations is also included in the article, which highlights its security goals and de- scribes its many primitives, including hash functions, digital signatures, encryption, and message authentica- tion codes. Next, underlining the main characteristics and advantages of the Advanced Encryption Stan- dard (AES) algorithm, the author provides a thorough examination of the algorithm. The study examines the benefits and drawbacks of the Least Significant Bit (LSB) methodology, a well-liked steganography method for concealing data in pictures. Lastly, the study examines the advantages and disadvantages of several picture formats, including BMP, PNG, and GIF, and how they affect LSB steganography. The author uses metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and histograms to assess the effectiveness of different approaches. The implementation of the suggested system and the resulting user interface are described in the paper's conclusion.

A new reversible data hiding approach based on the pixel difference histogram shifting technique is presented by Xian-ting Zeng et al. [9]. It addresses the shortcomings of current techniques and expands on earlier studies on reversible data masking. The idea of reversibility was first presented in earlier publications by Honsinger et al. [9], although Vleeschouwer et al. [10] suggested an alternative strategy based on bijective transformations. Compressing LSB planes for embedding was investigated by Fridrich et al. [11], and Celik et al. [12] improved this technique using the generalized-LSB (G-LSB) approach. The difference expansion (DE) method for reversible data conceal- ment was first presented by Tian [13] and was later enhanced by Alattar [14]. Although these methods improved embedding capacity, Ni et al. [20] presented the histogram shifting technique, which had a smaller payload. In an attempt to enhance the payload, later studies such as Lin et al. [21] and Tsai et al. [22] en- countered problems with noise introduction, restricted recoverability, and the requirement for additional in- formation transfer. The idea of a reference pixel was first presented by Lee et al. [23], but they ran into problems with irreversibility and possible extraction errors. By using multi-layer embedding and the refer- ence pixel notion, the suggested approach overcomes these drawbacks and provides low distortion and a high embedding capacity. It employs histogram shifting, embeds data in the redundant space produced, and makes use of pixel disparities between a reference pixel and its neighbors.Only the length of the buried data and the stego-image are needed for extraction and recovery in this completely reversible procedure. The effects of block size, threshold, and multi-layer embedding on distortion and embedding capacity are also examined in the paper. With a high average pure payload of 1.08 bits per pixel and a PSNR of more than 30 dB, the testing findings show how effective the suggested approach is across a variety of pictures. The benefits of the suggested approach in terms of em- bedding capacity and image quality are demonstrated through comparisons with other reversible data hiding strategies currently in use. In order to further increase the scheme's capacity and flexibility, the article also looks into the possibility of expanding it with more embedding layers.

Ignatius De Rosal Moses Setiadi et al. give a thor- ough analysis of digital image steganography, empha- sizing its objectives, evaluation procedures, methods, advancements, and datasets [10]. The authors begin by outlining the historical background of steganog- raphy and how it differs from watermarking and cryptography. The four primary components of image steganography—imperceptibility, payload capacity, se- curity, and robustness—are then covered in detail. Mean Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), Struc- tural Similarity Index (SSIM), and Kullback-Leibler (KL) divergence are just a few of the assessment techniques that are methodically examined in this work. It additionally categorizes steganographic tech- niques according to their objectives, domains, and methodologies and investigates a range of steganal- ysis methods, both universal and specialized, that are employed to uncover concealed communications. The challenges and opportunities in steganography research are covered in the paper's conclusion. These include the necessity for robust methodologies, the creation of complex approaches, and the significance of trustwor- thy datasets for testing. The authors stress the necessity for more research in this quickly developing sector and stress the significance of comprehending the trade- offs between imperceptibility, payload, security, and robustness.

TABLE I
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[1]	In this paper, a secure data transfer technique utilizing the Data Encryption Standard (DES) and wavelet-based steganography is presented. By embedding the encrypted plaintext within a wavelet-transformed image's low-frequency subband, data security is improved while visual distortion is reduced.	• Steganography and cryptography operate together to create a strong security framework that makes it impossible for unauthorized individuals to obtain the data that is buried. • By using the low-frequency sub-band for data embedding, the hidden message is less noticeable because the original image's visual quality is maintained to a considerable extent.	• Some users may find this method less accessible due to its intricacy, which may necessitate significant knowledge of wavelet transformations, steganography, and cryptography. • The security of the sent data may still be jeopardized by the method's vulnerability to steganalysis tools, which can uncover secret messages.
[2]	With the focus on the spatial, frequency, and adaptive domains, this paper examines and evaluates several digital image steganography methods. It draws attention to strategies, uses, and difficulties in guaranteeing steganographic systems' robustness, undetectability, and data capacity.	• Broad Range of Methods: Provides flexibility and adaptability for many use cases by covering sophisticated techniques like DCT and DWT. • Security Applications: Steganography has useful applications such as smart identity systems and copyright protection, and it improves secure communication.	• Vulnerability to Steganalysis: Robustness is limited by the fact that many techniques are still observable under contemporary steganalysis. • Limited Payload and Quality Trade-offs: Methods such as LSB embedding may result in a compromise between the quantity of concealed data or the quality of the image.
[3]	This study examines wavelet transform-based image compression strategies, focusing on both lossy and lossless approaches. It talks about how wavelets can overcome the drawbacks of more traditional techniques like DCT-based JPEG compression while increasing compression fidelity and efficiency.	• Better Compression Quality: By avoiding blocking artifacts and offering progressive transmission, wavelet-based techniques, such as EZW coding, improve image quality at lower bit rates. • Adaptability: Wavelets effectively compress both low-frequency and high-frequency components by analyzing signals at various resolutions.	• High Demand for Computation: Transform-based techniques, particularly wavelet-based algorithms, can need a large amount of memory and computing power. • Complexity for Real-Time Applications: Because wavelet transformations are hierarchical, implementing wavelet-based compression in real-time systems can be difficult.
[4]	The study presents a data-hiding method that embeds a lot of secret info into photographs while preserving good visual quality by using edge detection and image interpolation. For uses such as copyright protection and authentication, this technique guarantees increased capacity and imperceptibility.	• High Data Embedding Capacity: With little distortion, the suggested approach accomplishes a noteworthy embedding capacity of up to 391,115 bits. • Better Image Quality: The method maintains a PSNR over 44 dB by utilizing edge detection to protect the visual quality of stego-images.	• Complicated Preprocessing: Using interpolation and edge detection calls for a large amount of preprocessing time and computer power. • Dependency on Image Content: The method's efficacy varies depending on the type of cover image, which impacts embedding capability and consistency of quality.
[5]	The study introduces a modulus function-based high-capacity data hiding technique for embedding digit-by-digit data in pictures. For real-time applications, this method provides faster computation and preserves image quality better than the straightforward LSB replacement method.	• High Image Quality: In comparison to conventional LSB replacement techniques, the method maintains a higher PSNR while minimizing visual distortion. • Efficiency and Simplicity: It is appropriate for real-time applications since it uses fewer computer resources and encrypts and decodes data more quickly.	• Limited Adaptability for Non-standard Bases: The approach may not be as flexible for complicated data structures if the modulus does not match standard numeric systems. • Dependency on Host picture Range: The method's applicability to some picture datasets may be limited by the host image's pixel value range.

TABLE II
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[6]	Using the wavelet transform and the AES algorithm, this study proposes a technique for integrating cryp- tography and steganography to secure data transfer.	- By inserting encrypted text in the wavelet-transformed image's LL sub-band, it offers exceptional se- curity for data transfer.	- Because the algorithm uses LSB substitution, it may cause visual distortions in the image, particularly when more data is included.The robustness of the algorithm against attacks is not thoroughly examined in the publication.
[7]	The paper suggests a secure cryptosystem for cloud- based IoT infrastructure using DNA cryptography and DNA steganography	- By combining DNA cryptography and DNA steganography, se- curity is improved. - A novel key generation method based on DNA operations is used.	- The complexity of DNA operations causes the scheme's performance to be comparatively slower. - There is no mathematical security proof.
[8]	This study suggests a way to use steganography and encryption together to send data securely over the internet.	- Steganography and cryptography work together to increase secu- rity. - Robustness: The suggested system can withstand a variety of attacks.	- Complexity: Using two approaches together may make the system difficult to implement. - The possibility of degradation: When LSB insertion is used for steganography, the quality of the cover image may suffer, particularly if a large quantity of data is inserted.
[9]	Based on multi-layer embedding and histogram shift- ing, this work suggests a reversible data concealment strategy.	- Low distortion - High embedding capacity	- Preprocessing images is necessary to avoid overflow/underflow problems. - The number of layers utilised de- termines the embedding capacity.
[10]	An extensive review of digital image steganography is given in this publication. It examines the many objectives, evaluation instruments, techniques, and datasets associated with image steganography.	- Offers a thorough summary of the field. - categorises studies according to steganography objectives, which are frequently disregarded in ear- lier evaluations.	- Mostly concentrates on image steganography, ignoring other steganography kinds like text or audio steganography. - does not specifically discuss steganography's potential for malevolent use or ethical ramifications.

III. CONCLUSION

A strong and dependable basis for protecting private information while it is being transmitted is provided by the combination of encryption and image steganogra- phy techniques for safe file sharing. This dual-layered strategy combines two different but complimentary security measures to solve important issues including data integrity and unauthorised access. Steganogra- phy completely hides the existence of the data by embedding it in a harmless medium, such an image, whereas encryption guarantees that sensitive informa- tion is converted into an unintelligible format that can only be decoded by authorised parties with the proper decryption keys. When combined, these strategies offer a reliable way to maintain anonymity even in dangerous or hostile situations.By embedding secret data in a way that preserves visual quality, steganographic techniques like Pixel Value Differencing (PVD) increase its imperceptibility and make it practically hard for uninvited viewers to notice the existence of con- cealed information. Using the effectiveness and power of elliptic curve cryptography, encryption techniques like Elliptic Curve Diffie-Hellman (ECDH) simulta- neously guarantee secure key exchange and protect data against interception and unwanted decoding. The whole security framework is greatly strengthened by this mix of cutting-edge steganographic techniques and sophisticated cryptographic approaches, which offer a smooth balance between data protection and effective transmission.In the end, this two-pronged approach has enormous potential to improve secure communication methods in a variety of industries, such as government, healthcare, finance, and defence, while guaranteeing that private data is protected from contemporary cy- berthreats. The techniques used to safeguard sensitive data must change along with the digital environment.

Future studies should concentrate on strengthening the system's defences against complex attacks, fixing any flaws, and incorporating state-of-the-art cryptographic techniques that offer more robust defence against new dangers like quantum computing. To guarantee its use across a variety of platforms and industries, the system's scalability and adaptability might also be investigated further.The integration of PVD and ECDH can be a fundamental component of secure file-sharing systems with appropriate implementation, frequent upgrades, and ongoing innovation, opening the door for more resilient and dependable communi- cation techniques in the digital age. Even in the face of changing cybersecurity problems, the system can guarantee the availability, confidentiality, and integrity of critical data by expanding upon this basis.

REFERENCES

[1] M. IndraSena Reddy, "A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryp- tography", International Journal of Computer Applications (2013)
[2] A. Cheddad et al. / Signal Processing; Digital image steganog- raphy: Survey and analysis of current methods (2009)
[3] VVS Kumar M. IndraSenaReddy , "Image Compression Tech- niques by using wavelet transform", Journal of information engineering and applications (2012)
[4] Jung KH and Yoo KY Data hiding using edge detector for scalable images. (2013)
[5] Thien CC, Lin JC A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. (2003)
[6] M. Indra Sena Reddy and A.P. Siva Kumar; Secured Data Transmission Using Wavelet Based Steganography and Cryp- tography by Using AES Algorithm. (2016)
[7] S. Namasudra Computers and Electrical Engineering; A secure cryptosystem using DNA cryptography and DNA steganogra- phy for the cloud-based IoT infrastructure. (2022)
[8] Osuolale, A. Festus ; Secure Data Transfer Over the Internet Using Image CryptoSteganography International Journal of Scientific and Engineering Research. (2017)
[9] X.-t. Zeng, Int. J. Electron. Commun. Reversible data hiding scheme using reference pixel and multi-layer embedding. (2011)
[10] D.R.I.M. Setiadi, S. Rustad, P.N. Andono et al Signal Process- ing ; Digital image steganography survey and investigation. (2022)