StegoShield: Securing Secrets with GIF-Based Steganography and Cryptography

Akhina PV
Department of Computer Science
Cyber Security
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: akhinababu3540@gmail.com

Deepnitha Ramachandran
Department of Computer Science
Cyber Security
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: deepnitharamachandran@gmail.com

Saniya Sudhan
Department of Computer Science
Cyber Security
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: saniyasudhan123@gmail.com

Sreelakshmi suresh
Department of Computer Science
Cyber Security
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: sreelakshmistv@gmail.com

Ms. Mafnitha KK
Assistant Professor
Department of Computer Science
Cyber Security
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: mafnitha@vjec.ac.in

***Abstract*—Steganography and visual cryptography are essential techniques in secure digital communication, allowing for covert information exchange and secure data transmission. This paper explores various steganographic methods, with a focus on image steganography, including Least Significant Bit (LSB) substitution, transform domain approaches, and advanced methods such as Spread Spectrum and Patchwork steganography. Additionally, the study examines visual cryptography (VC), which enables image encryption through secret sharing techniques. The effectiveness of different steganographic approaches is analyzed based on criteria such as invisibility, payload capacity, robustness, and resistance to detection. Comparative studies on steganographic techniques in different image formats (BMP, GIF, JPEG) highlight their strengths and limitations. Furthermore, emerging research integrating steganography with deep learning and real-time encryption standards is discussed. The paper also reviews steganalysis techniques used for detecting hidden information, emphasizing the ongoing challenge of developing robust and generalizable detection methods. The findings contribute to the advancement of secure data hiding techniques, addressing the evolving demands of cybersecurity and covert communication in the digital era.**

I. Introduction

In an era of increasing digital surveillance and data interception, the need for secure communication has become more critical than ever. Traditional encryption techniques, such as cryptography, aim to protect data by transforming it into unreadable formats. However, cryptographic methods can raise suspicion and be restricted by governments. Steganography, on the other hand, provides an alternative approach by embedding secret messages within digital media, ensuring that communication remains undetectable. Among various forms of steganography, image-based methods have gained prominence due to the widespread use of digital images and their inherent redundancy, which allows for seamless information hiding.

This paper explores the different methodologies used in image steganography, using methods like Least Significant Bit (LSB) substitution and frequency domain methods that modify image compression components. The strengths and weaknesses of these methods are evaluated in terms of capacity, security, and resistance to steganalysis. Furthermore, the study discusses visual cryptography, a powerful technique that enables secret image sharing without computational decryption, making it useful for authentication and secure data transmission. The integration of steganography with real-time communication and deep learning techniques is also examined, highlighting its potential in modern cybersecurity applications. By analyzing existing research and recent advancements, this research offers a thorough summery of the current landscape of digital steganography and visual cryptography, offering insights into their practical applications and future developments.

II. Literature Survey

[1] T. Morkel J. H. P. Eloff and M. S. Olivier of the University of Pretoria examined solidly the practice of hiding information within digital images, which is termed image steganography. While it is true that steganography moves much deeper than cryptography, which is a method of hiding information within other pieces of information, in the latter a technique referred to as overwriting is used. This is done so that no one attempts to access the ‘crypted‘ document without authorization. Indeed, this technique as many others has its roots in ancient methodologies, but today as the world transitions to a more reliance on digital communication,

TABLE I
COMPARISON TABLE

Reference	Description	Advantages	Disadvantages
[1]	Image steganography hides information within digital images by analyzing embedding techniques, robustness, and detection resistance. It balances invisibility, payload capacity, and security to enhance covert communication.	- Enhanced Security:Conceals message existence, making detection and interception harder. - Adapts to needs with methods like LSB and spread spectrum for security or capacity.	- Some techniques of steganography leave patterns, making detection easier. - Higher capacity reduces secretiv, while secure methods limit data embedding.
[2]	A novel steganography technique for animated GIFs using a variable block partition scheme, enhancing data security and imperceptibility.	- Higher security due to randomized frame selection and variable partitions. - Better image quality with high PSNR (52-59 dB) compared to existing methods.	- Limited to GIF format, restricting applicability to other media types. - Computational complexity due to multi-step preprocessing and partitioning.
[3]	Visual cryptography is a technique for encrypting images so that decryption requires overlaying multiple transparent shares.	- High security as the encrypted shares reveal nothing individually. - No computational decryption is required—simply overlaying shares reveals the image.	- Precise alignment of shares is necessary for correct decryption. - Limited to binary or low-color images, reducing image quality.
[4]	Hybrid Steganography* combines Visual Cryptography and SLSB encryption to securely hide data in images while preserving quality.	- No key requirement. - Robustness.	- limited capacity. - complex decryption.
[5]	Sequential Multiple LSB (SMLSB) method for real-time data concealing multimedia, enhancing robustness and capacity with minimal distortion. While it offers improved security and versatility, it may increase computational complexity and require customization for specific applications. .	- Enhanced robustness and versatility for real-time data hiding in multimedia. - Increased computational complexity and need for customization in specific applications.	- Limited no: of images. - Image hashing must be done properly.
[6]	a novel method for embedding secret data in animated GIFs using a variable block partitioning approach. It enhances data security by applying a randomized frame selection and embedding scheme, ensuring imperceptibility while maintaining high image quality.	- Higher security due to random frame selection and variable partitioning. - Better visual quality with high PSNR (52-59 dB) compared to existing GIF steganography methods.	- Gesture recognition could be used to track and compromise passwords. - Onlookers might be able to observe multiple finger movements.
[7]	LSB steganography in GIF and BMP images, highlighting BMP's higher data capacity with minimal distortion but increased detection risk, while GIF offers lossless compression but limited embedding capacity.	- BMP supports higher data capacity with minimal distortion. - GIF preserves image quality using lossless compression.	- It's still vulnerable to attackers observing the password. - Some users might find the hybrid image and story method confusing.
[8]	Improved LSB data hiding method using OPAP, which enhances stego-image quality with minimal computational overhead but remains vulnerable to detection and image processing attacks.	- Enhances image quality by reducing visual distortion. - Maintains low computational complexity for efficient processing.	- Susceptible to image processing attacks like compression. - Can Still be detected through statistical analysis techniques.
[9]	Through the use of LSB based steganography,a message can be conceal inside a image by substituting the bits of the secret message for each pixel's least significant bit(LSB)	- Widely applicable. - LSB allows data to be embedded without sacrificing visual quality.	- Low steganographic capacity. - Susceptibility to statistical analysis.
[10]	V-CRYPT secures images by splitting them into four encrypted shares, requiring a secret key for decryption.	- No Need for Computation. - Resistance to Phishing Attacks.	- High storage requirements. - The system heavily relieson the correct key for decryption.
[11]	A triple-layer security method using steganography and visual cryptography to hide and encrypt image data.	- Difficult to Detect. - Resistant to Unauthorized Access.	- Quality Degradation. - Risk of Losing Shares.
[12]	enhances visual cryptography using XOR-based VC and AES pencryption for secure image sharing with encapsulated shares.	- No Pixel Expansion. - Resistance to Fake Shares.	- Dependency on All Shares. - Computational Complexity.

information security has become a more pressing issue. The authors note that while there are cryptographic systems in place which governments can stifle or completely obliterate, through steganography, one can freely disguise communication that is fitted within tip of the spear information. The focus of this study is the image based forms of steganography. The study opens with a short explanation of steganography and describes how it differs from other forms like watermarking and fingerprinting, which are used for concealment rather than as an asset for protection of intellectual property. Because digital images require a lot of space and have redundant data bits, which can be altered without severely affecting the quality of the image, a digital image is perfect for hiding information.

[2] Maram Abdullah M. Alyahya, Arshiya S. Ansari, and Mohammad Sajid Mohammadi propose a novel hidden encoding technique in their paper An Animated GIF Steganography Using changeable Block Partition Scheme. The study focuses on enhancing data security by embedding secret information within animated GIF files using a variable block partitioning method. Unlike conventional approaches that primarily use formats like JPEG and PNG, this method utilizes the unique frame-based structure of GIFs to conceal data effectively. The proposed algorithm first extracts frames from an animated GIF, applies preprocessing steps such as resizing, grayscale conversion, and filtering, and then divides the selected frame into variable-sized partitions using a Quad-tree decomposition technique. The randomized selection of frames and partition blocks, along with the use of a shared key, ensures that the hidden data remains undetectable, making the method more secure than traditional GIF-based steganography techniques.

Researchers used the Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) to quantify performance evaluation and assess the strategy's efficacy on a variety of animated GIFs. Even at large embedding capacity, the results showed high imperceptibility, with PSNR values ranging from 52 to 59 dB. The other suggested option retains greater image quality while offering improved data security, according to a comparison with existing approaches like Least Significant Bit (LSB) and Pixel Value Differencing (PVD) techniques. Additionally, the encoded data remained undetectable according to robustness tests conducted utilizing Steganalysis tools such as Try It Out and Ben4D. The study challenges preconceived notions about animated GIFs' limitations in steganography by concluding that they might be a useful tool for securely hiding data. Future research attempts to expand

[3] Dyala R. Ibrahim, Je Sen Teh, and Rosni Abdullah, in their paper An Overview of Visual Cryptography Techniques, provide a comprehensive review of various visual cryptography (VC) schemes. Visual cryptography technique is an encryption technique this divides a hidden image into multiple segments, which can be stacked together to reveal the original image without requiring complex computations or decoding tools. The paper addresses gaps in previous surveys by analyzing over 40 VC schemes based on key performance metrics such as contrast, pixel expansion, computational complexity, and security. The authors discuss different VC categories, including classical VC, extended VC, and more advanced models such as progressive and hierarchical VC, highlighting their respective strengths, limitations, and applications in digital watermarking, authentication, and secure communication.

The paper identifies key challenges in VC, including pixel expansion, poor image quality, and high computational complexity. Although some schemes attempt to minimize pixel expansion to improve clarity and storage efficiency, they often introduce trade-offs in security and computational cost. The study also highlights recent advancements in multi-secret encryption, meaningful shares, and flexible decryption techniques, making VC more applicable in real-world security systems. The authors conclude that while VC has promising applications, further research is needed to optimize trade-offs between security, image quality, and computational efficiency. Future research directions include improving pixel expansion techniques, enhancing multi-secret encryption, and designing VC schemes that better balance usability and efficiency for practical use.

[4] Gokul M, Umeshbabu R, Shriram K Vasudevan, and Deepak Karthik propose a integrated steganography technique combining Visual encryption techniques and Selected Least Significant Bit (SLSB) Encryption to enhance data security in digital communication.In order to reduce the risk of interception and unauthorized access, their method uses visual encryption techniques to split a hidden image into two encrypted image shares, which are then embedded into a cover image using SLSB encryption. The encryption process is generating two shares from the secret message, embedding them into a cover image, and preserving the original image quality with minimal distortion; decryption extracts and recombines the shares to reveal the hidden message. The study shows that the system retains up to 90 percentage of the original image quality while providing strong resistance against hacking attempts. To further improve security and efficiency, the authors propose DCT-based compression and more sophisticated encryption techniques.

[5] The paper titled "Sequential Multiple LSB Methods and real-time data Hiding: variations for Visual Cryptography Ciphers" by Papadopoulos and Psannis presents a novel approach to information concealment and watermarking techniques within visual, vedio, and audio communications. In order to increase security resilience, data capacity, and real-time efficiency, the study suggests the Sequential Multiple Least Significant Bit (SMLSB) method, a sophisticated steganographic methodology. SMLSB boosts robustness against detection and illegal access by including sequential and scrambled embedding patterns, as contrast to typical LSB-based steganography, which merely conceals data in the least significant bits of digital media. The technique ensures little distortion to the original media and is especially useful for real-time and near real-time (NRT) communications. The research also looks at how Visual Cryptography (VC) and steganography can be combined to safely share encrypted black-and-white picture ciphers across a range of media types. SMLSB's flexibility, security, and robustness benefits are carefully contrasted with those of

other steganographic methods, such as Multiple LSB, Matrix Embedding, and Parity Coding. Several variants of the SMLSB approach are described, including its application in visual cryptography ciphers that embed secret images in cover media and divide them into multiple shares. The paper discusses real-time constraints, computational difficulty, and potential applications in real-time multimedia communications, while also highlighting its compatibility with modern encryption standards like RSA, DES, and AES. Potential applications in high-efficiency video coding (HEVC) and secure streaming protocols, comparison with other real-time steganographic algorithms, and experimental validation are among the future research areas recommended in the study's conclusion.

[6] Kombrink, M. H., Geradts, Z. J. M. H., and Worring, M. (2024) in their paper "Image Steganography Approaches and Their Detection Strategies: A Survey" provide a comprehensive review of image steganography techniques and their corresponding detection methods. The authors examine various approaches to steganography, including spatial domain methods (e.g., LSB, PVD, BPCS), transform domain methods (e.g., DCT, DWT, IWT, DFT), and deep learning-based techniques (CNN, GAN). The study highlights the assets and liablities of these methods, particularly in the context of embedding capacity, security, robustness, and imperceptibility. Additionally, the paper addresses steganalysis techniques, categorizing them into visual detection, signature-based analysis, targeted steganalysis, and universal steganalysis. A key challenge identified is the lack of generalizability in steganalysis methods, which often detect only specific steganographic schemes rather than providing a universal solution. The authors also discuss the evolving research landscape, noting that while newer methods hold promise, they require further refinement for practical application. The survey provides a comparative performance analysis of existing detection techniques and calls for future research to focus on developing more generalizable and robust steganalysis methods.

[7] Dr. Eltyeb E. Abed Elgabar and Haysam A. Ali Alamin, in their study "Comparison of LSB Steganography in GIF and BMP Images", explore the effectiveness on Least Significant Bit (LSB) steganography for concealing information within digital images. Their research highlights how steganography is not just about encryption but also about hiding the existence of a message entirely. By infusing secret information within the lowest-order bits of image pixels, LSB steganography ensures imperceptibility to the human eye. However, the success of this technique largely depends on the type of cover image used. The authors analyze GIF and BMP image formats to determine their suitability for secure steganographic communication. The study explains that BMP images offer a higher capacity for data embedding due to their lossless nature and uncompressed format. BMP files support various color depths (1-bit to 32-bit), allowing for greater flexibility in data hiding. Since BMP images retain all pixel information, they can conceal large amounts of data without introducing noticeable distortions. However, the large file size of BMP images makes them less commonly used on the internet, which raises suspicion when transmitted. Additionally, while BMP images are more resistant to compression-based attacks, they remain vulnerable to simple modifications such as cropping, rotation, or format conversion.

On the other hand, GIF images use indexed color palettes with a maximum of 256 colors, which limits the amount of data that can be hidden. The authors note that modifying the lowest-order bit of a pixel in a GIF image can result in noticeable color changes if the index values shift significantly. However, GIF images are widely used on the web and have smaller file sizes, making them less likely to attract suspicion compared to BMP images. The lossless LZW compression used in GIFs preserves hidden data, but the presence of palette-based color mapping makes them vulnerable to statistical and visual attacks that can reveal the presence of hidden messages.

The paper concludes that BMP images are better suited for high-capacity, low-risk environments, where file size is not a concern, and GIF images are preferable for scenarios where inconspicuous communication is essential. However, both formats have weaknesses in terms of robustness against image manipulation and susceptibility to detection. The research by Eltyeb E. Abed Elgabar and Haysam A. Ali Alamin provides a comparative framework for choosing appropriate steganographic techniques based on the security, capacity, and visibility requirements of different applications. Their work contributes to the ongoing development of more secure and undetectable data-hiding techniques in digital media.

[8] Chi-Kwong Chan and L.M. Cheng (2004) introduce an enhanced data-concealing method that combines simple LSB substitution with an Optimal Pixel Adjustment Process (OPAP). This enhancement not only raises the standards of stego-images moreover keeps computational complexity low. Compared to conventional LSB techniques,theirtechniques dramatically lowers the worst-case mean- square error(WMSE) between the cover photos and the stego The study evaluates existing LSB methods, including the optimal LSB substitution approached by Wang et al., and highlights their limitations. By adjusting pixel values after data embedding, OPAP minimizes distortions while preserving the integrity of the hidden data. Experimental results on grayscale images show that OPAP achieves superior image quality and computational efficiency, making it a practical and effective solution for secure data hiding.

[9] The study examines steganography based on least significant bits,a method that pixel values hidden in digital images. While this method allows for high data embedding with minimal visual distortion, it is vulnerable to steganalysis techniques that can detect hidden messages.The study examines basic, adaptive, and random LSB embedding methods, highlighting their trade-offs in security, imperceptibility, and robustness. While adaptive and randomized approaches reduce detection risks, traditional LSB substitution is more prone to statistical analysis. The findings suggest that although LSB-based techniques are effective, they require enhancements to improve security. Future research should focus on integrating cryptographic techniques and machine learning to make LSB-

based steganography more resilient to detection.

[10]Muhamad Ridhwan Bin Nashrudin and colleagues explore the concept of Visual Cryptography (VC), a cryptographic technique that enables secure image sharing by dividing an image into multiple shares.Introduced by Naor and Shamir in 1994, VC makes sure the original image stays safe, because no single share shows any details and putting together a certain number of shares is needed to rebuild it. VC usually focuses on binary images, but some key improvements have extended its use to color images and also made the shares better. VC security depends on human vision. Human vision, therefore, enables it. Using human vision provides security. Due to this, computer attacks are hard to do.

The authors' work details the V-CRYPT system, a version of the conventional VC approach that has been improved to greatly increase the number of shares from two to four. This enhancement importantly increases the system's overall security, but it also makes the encryption and decryption processes even more complicated. Every user encrypts each image through key entry; the key divides every image into four shares that have subpixels for hiding. You have to use the right key to correctly get the original image back. In the decryption, you have to use all four shares. An unintelligible image will show up if the key is wrong, or if the shares are not the same. The V-CRYPT system incorporates these features, thereby solving secure image sharing, which fulfills every need for increased data confidentiality in a linked world.

[11] In their paper, "An Steganography-based Triple Layered Image Data Hiding Using Visual Cryptography," Kukreja and Malik explore the integration of steganography and visual cryptography to enhance the security on digital images. They highlight the increasing prevalence of cyber-attacks that compromise sensitive data, leading to information and identity theft. The authors argue that traditional security measures are insufficient against sophisticated threats, necessitating a multi-layered strategy for safeguarding tthe data. through the combination of steganography, which conceals information within innocuous media, with visual cryptography, which generates shares of the original image without requiring keys, the proposed method aims to create a robust framework for secure data transmission.

The writerrs present a novel technique that embeds secret messages within the lsb of an image, making detection challenging. This secret image is then processed through visual cryptography to create noise-like shares, which are subsequently hidden in different images using steganography. This three-tiered security model significantly improves the reliability and efficiency of secret message transmission. The paper emphasizes the practical applications of this method across various sectors, including healthcare and finance, where safeguarding sensitive information is paramount. Overall, Kukreja and Malik's work contributes to the ongoing research in information security by proposing a comprehensive solution that leverages the strengths of both steganography and visual cryptography.

[12] Sharing a secret pictures with Shares that are incased in Visual Cryptography This research paper examines in depth into enhancing the security of visual cryptography, a method for sharing secret images. The authors offer a safe share generation strategy that aims to fix flaws in conventional visual cryptography, where it is simple to add or alter phony shares, threatening the confidentiality of the data being shared.

The suggested method generates shares using a (2, 2) XOR-based visual cryptography system, which are subsequently individually encrypted using the Advanced Encryption Standard (AES) algorithm. The purpose of these encrypted shares, is to make it impossible to visually get the secret image data from a single share. This method greatly enhances system security by guaranteeing that the secret image may only be restored after both encrypted shares have been properly combined and decoded.

III. Conclusion

It presents a detailed study on the contemporary modes of network security and secure data hiding. The study highlights the capabilities of visual cryptography and a variety of steganography techniques in enhancing data security and secret data communication in the digital network. Although the BMP does possess a bigger capacity in data transfer, it has become evident that out of GIF images, pixel quality retains better and thus imperceptibility. However, advanced techniques such as randomized frame selection and hybrid encryption provide robustness and higher security degree in data transmission over untrusted networks. The integration of real-time crypto applications and emerging approaches to machine learning highlights the promising pathway for enhancing secure communication and intrusion detection systems. However, the continuing challenges in steganalysis, including the demand for an invulnerable yet generalizable manner of detection, remain critical. Further studies should develop optimal trade-offs between security, payload, and computational complexity by addressing detection vulnerabilities and enhancing the robustness of network defenses. This study adds to the growing scientific body aimed at developing secure communication technologies in an age of rising cybersecurity threats.

References

[1] Morkel, Tayana and Eloff, Jan HP and Olivier, Martin S,An overview of image steganography,ISSA, vol.1,2nd.ed,pp.1–11,2005

[2] Alyahya, M.A.M., Ansari, A.S. and Mohammadi, M.S., 2022. An Animated GIF Steganography Using Variable Block Partition Scheme. Comput. Syst. Sci. Eng., 43(3), pp.897-914.

[3] Ibrahim, D.R., Teh, J.S. and Abdullah, R., 2021. An overview of visual cryptography techniques. Multimedia Tools and Applications, 80, pp.31927-31952.

[4] Gokul, M and Umeshbabu, R and Vasudevan, Shriram K and Karthik, Deepak Hybrid steganography using visual cryptography and LSB encryption method
International Journal of Computer Applications,vol.59,pp.14,2012

[5] Papadopoulos, Nikolaos A and Psannis, Kostas E, Sequential multiple LSB methods and real-time data hiding: variations for visual cryptography ciphers, Journal of Real-Time Image Processing,vol.14,pp.75–86,2018

[6] Kombrink, Meike Helena and Geradts, Zeno Jean Marius Hubert and Worring, Marcel Image steganography approaches and their detection strategies: A survey Kombrink, Meike Helena and Geradts, ACM Computing Surveys,vol.57,no.2,pp.1–40,2024

[7] Elgabar, Eltyeb E Abed and Alamin, Haysam A Ali Comparison of LSB Steganography in GIF and BMP Images International Journal of Soft Computing and Engineering,pp.2231–2307,2013

[8] Chan, Chi-Kwong and Cheng, Lee-Ming, Hiding data in images by simple LSB substitution,Pattern recognition,vol.37,no.3,pp.469–474,2004

[9] Chandramouli, Rajarathnam and Memon, Nasir, Analysis of LSB based image steganography techniques Proceedings 2001 international conference on image processing (Cat. No. 01CH37205),vol.3,pp.1019–1022,2001

[10] Nashrudin, Muhamad Ridhwan Bin and Nasser, Abdullah B and Abdul-Qawy, Antar Shaddad H,V-CRYPT: a secure visual cryptography system,2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM),pp.568–573,2021

[11] Kukreja, Bhawna and Malik, Sanjay Triple Layered Security for Data Hiding Using Steganography and Visual Cryptography,Authorea Preprints,2024

[12] Shankar, K and Eswaran, P Sharing a secret image with encapsulated shares in visual cryptography, Procedia Computer Science,vol.70,pp.462–468,2015