Steganograph Embedded with Cryptography and Digital Watermarking

Abhishek Pandey[1], Ninad Solunke[2], Smit Shah[3] and Prof. Amit Kukreja[4]
[1]*UG Scholar, Department of Electronics and Telecommunication, K. J. Somaiya Institute of Technology, Sion*
[2,3]*UG Scholar, Department of Computer Engineering, K. J. Somaiya Institute of Technology, Sion*
[4]*Professor, Department of Electronics and Telecommunication, K. J. Somaiya Institute of Technology, Sion*

***Abstract*—Information security is becoming increasingly important with the increasing popularity of digital technologies and internet communications. Networks are used to transmit confidential documents, financial information, and personal data daily. The use of cryptography has been a traditional method for protecting data by transforming it into an intractable code. Even so, intruders can still detect the encrypted information. Why? The problem can be resolved by using steganography, which not only transforms data into another format but also conceals it from detection in digital media like images, audio, or videos. Despite the need for secrecy and invisibility, it's crucial to demonstrate that the online content belongs to a specific individual and is not compromised. Through digital watermarking, identification data is integrated into the media. A thorough discussion of the mixed approach has been developed using three technologies: cryptography, steganography, and digital watermarking. The proposed method involves encryption, concealment through stenography (through embedding of an external watermarked layer), and authentication through Embedding of a water mark. The utilization of multi-layered techniques greatly enhances data security by ensuring that information is protected from damage on one layer while the other layers continue to safeguard it. The authors suggest that a combination of the three methods can be deemed dependable and effective means of protecting data transmission in various sectors such as defence, intelligence, and cyber security. They follows analysis.**

***Index Terms*— Cryptography, Digital Watermarking, Encryption, Security, Steganography.**

I. INTRODUCTION

With the internet, sharing of information has become much more widespread in recent years, making it necessary for people and organizations to protect their data. Why? For the majority of this time, open networks are susceptible to the transmission of confidential messages and partially disclosed financial transactions. This makes them a prime target for attackers. Modern communication systems must ensure the confidentiality, integrity, and authenticity of data.

Cryptography is a widely used data protection technique? By means of cryptography, a plain text can be converted into an inconspicuous and unimportant cipher text using encryption techniques like RSA and AES [11], [12]. Even with cryptographic protection, communication cannot be hidden. Why? Encrypted information can be thought of as a neon sign that flashes "there's something interesting." This leads an attacker to explore different methods of breaking the code, such as using cryptanalysis or force. To safeguard sensitive data, additional security measures must be put in place. Unlike traditional methods, artificial imaging has the ability to hide confidential information in digital formats like audio files, videos, or images. The use of steganography permits the hiding of data from outside entities, unlike cryptography. The use of low-pass filtering (LSB) is one of the oldest and most basic techniques in image steganography, which results in the utilization of minimal bit of information in pixel values. The advantage of this approach is that it preserves hidden information while maintaining a visual image that is almost identical. Containing compression, noise addition, and image processing may require additional defence strategies beyond steganographic techniques. Hidden information in digital content that comes from another source can be extracted after the fact, even if it's damaged, modified or simply used as the original copy, to provide proof of ownership or identity. The use of watermarking is also applied by digital rights management, media authentication systems, and other functions to operate.

II. LITERATURE REVIEW

A. Cryptography for communication

Cryptography is a big part of keeping digital information safe by changing it into a format that unauthorized people cannot read. It helps make sure that information stays secret does not get changed and that the person sending it can be verified when they communicate. Cryptography is used for this purpose. The main kinds of encryption methods used in cryptography today are symmetric and asymmetric. Symmetric ciphers, like AES are fast and good at encrypting things while asymmetric schemes, like RSA provide a way to exchange keys.

Many researchers have said that cryptography alone cannot guarantee safety because even encrypted information can still be attacked and sensitive data can be revealed. Cryptography has its limitations. Additionally brute-force attacks and cryptanalysis are still threats especially if weak keys or old algorithms are used. Cryptography is not enough on its own. That is why experts recommend using cryptography with methods to get better security. Cryptography should be used with methods.

B. Steganography Techniques for Data Hiding

Steganography is a way to hide messages inside things like images, audio or video files so that other people cannot see the communication. Steganography is used for this purpose. The significant bit method is the most common one, where secret information is put into the parts of the pixel values that are not very important without changing the image quality too much.

Steganography has been shown to be a tool for keeping communication safe by hiding data not just encrypting it which can still reveal the data. Steganography is useful for this. However steganographic methods can be easily attacked by adding noise compressing or analyzing statistics and so on. To overcome these problems it is crucial to rely on both the encryption of the message and the steganographic technique being used so that one helps the other. Steganography and encryption should work together.

C. Digital Watermarking for Authentication

Digital watermarking is a process that puts identification information into media to protect copyrights and verify the content. Digital watermarking is used for this purpose. Watermarks can be either visible or invisible, depending on what they're used for. Most of the time invisible watermarking is used, in security systems because it does not affect the image quality of the media it is embedded in.

TABLE I: Summary of Related Works on cryptography and steganography

Sr. No.	Research Paper	Key Contribution	Limitation
1	Cryptography and Network Security [1]	Encryption protects data confidentiality using robust symmetric and asymmetric techniques	Does not conceal the existence of communication
2	Exploring Steganography: Seeing the Unseen [2]	Data can be invisibly embedded within digital media files without perceptible distortion	Hidden data remains detectable by steganalysis tools
3	Digital Watermarking and Steganography [3]	Watermarking ensures ownership proof and content authentication in digital media	Designed for ownership verification, not for data secrecy
4	Handbook of Applied Cryptography [4]	Comprehensive handbook covering secure encryption and key management techniques	Complex implementation with high computational overhead
5	Linguistic Steganography: Survey, Analysis and Robustness Concerns [5]	Linguistic and text-based steganographic hiding methods introduced for covert messaging	Very low data hiding capacity compared to image-based methods
6	Analysis of LSB Based Image	LSB substitution provides	Highly vulnerable to JPEG

	Steganography Techniques [6]	simple and efficient image-based data hiding with minimal distortion	compression and image manipulation
7	Information Hiding — A Survey [7]	Combining multiple information hiding techniques significantly improves overall system security	Integration of methods leads to increased system complexity
8	Steganography in Digital Media: Principles, Algorithms and Applications [8]	Advanced adaptive image steganography techniques with improved statistical undetectability	Computationally expensive; impractical for real-time systems
9	A Fair 56 Benchmark for Image Watermarking Systems [9]	Robust watermarking benchmark methodology developed for fair system evaluation	Embedded watermarks may degrade perceived media quality
10	A Method for Obtaining Digital Signatures and Public-Key Cryptosystems [10]	The asymmetric RSA algorithm enables secure public-key encryption and digital signatures	Relatively slow performance compared to symmetric-key methods
11	AES Proposal: Rijndael [11]	AES provides fast and highly secure symmetric block encryption adopted as global standard	Key distribution and management remain challenging in open networks
12	Information Hiding Techniques for Steganography and Digital Watermarking [12]	Multi-layer security is achievable by integrating steganography and cryptography approaches	Integration of multiple layers introduces significant system complexity
13	An Information-Theoretic Model for Steganography [13]	Information-theoretic model defines conditions to minimize steganographic detection probability	Model is largely theoretical with limited direct practical applicability
14	Watermarking Systems Engineering [14]	Engineering study presents robust and reliable authentication watermarking techniques	Watermarks remain vulnerable to targeted geometric removal attacks
15	An Overview of Image Steganography [15]	Comprehensive survey of image steganography demonstrates effective data concealment strategies	Methods are not robust against noise addition and signal distortion
16	Digital Image Steganography: Survey and Analysis of Current Methods [16]	Survey provides a broad overview of spatial and transform domain steganographic techniques	Existing methods require further improvement in security and capacity
17	Hybrid Security Using Cryptography and Steganography [17]	Combining cryptography and steganography offers improved dual-layer data protection	Hybrid approach incurs high processing time and computational overhead
18	Enhanced Data Security Using Digital	Enhanced digital watermarking scheme	Provides limited confidentiality; not suitable

	Watermarking [18]	effectively protects ownership of digital content	for covert communication
19	Disappearing Cryptography: Information Hiding: Steganography and Watermarking [19]	Encryption techniques effectively secure data content against unauthorized access	Does not conceal the fact that encrypted communication is occurring
20	Applied Cryptography: ProtocolsAlgorithms and Source Code in C [20]	Foundational security principles and best practices for robust cryptographic system design	Requires integration with other techniques to achieve full communication security

Several researchers have already shown that watermarking is very helpful when used with techniques for extra protection. Watermarking and steganography can work together to provide protection. Digital watermarking is a part of this process. Cryptography, steganography and digital watermarking are all important for communication.

Recent research focuses on hybrid security systems that integrate cryptography, steganography, and digital watermarking to achieve multi-layered protection [7], [17]. In such approaches, the secret data is first encrypted, then hidden within a cover medium using Performing confidentiality, concealment, and authenticity at the very same time, this combined approach is a great security enhancer. If a security system's one layer is broken, and the other layers are still functioning to protect the data, it is almost impossible for an intruder to reach the data without the authorization. A good explanation and the annotation of this concept can be seen in source [13]. The research paper indicates that hybrid security systems are more robust against all sorts of attacks like data interception, data alteration, and illegal replication.

III. METHODOLOGY

This research employs a dual strategy of a detailed literature survey and a conceptual system design aimed at creating a hybrid framework by combining cryptography, steganography, and digital watermarking for secure data communication. Since the goal is not to fabricate a physical model, the focus will be on analyzing, structuring, and elaborating these existing techniques so as to demonstrate the security enhancement potential of the hybrid method. Hence, the approach is mainly about grasping the fundamentals of each method, assessing their advantages as well as disadvantages, and coming up with a layered hybrid model that integrates their features in an efficient way.

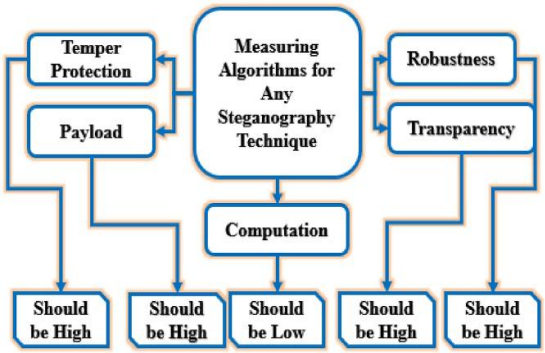

Fig. 1. Block Diagram Representing Performance Evaluation Criteria for Steganography Techniques

This research paper was first-time exposure to cryptography, steganography and digital watermarking through a broad literature searching and reading. The texts encompass IEEE publications, journals and standard reference books meant for encryptions, data hiding and watermarking techniques, etc. [1], [3], [7]. The obtained information was divided among the three main topic areas: data encryption, data concealment and data authentication. This division made it easier to understand what role each method plays in the overall security and the points at which their integration(s) is/are most beneficial.

On the basic conceptual level, the integrated scheme consists of three layers where the data protection is implemented at each layer through various techniques and only at the end of all these steps is the actual data finally secured. The first layer involves the use of cryptography for the purpose of data encryption. The original data (plain text or digital data) is transformed into a cipher text using an appropriate encryption algorithm such as AES or RSA. Thus encryption provides confidentiality such that even if the data is intercepted, it cannot be understood without a proper decryption key [10], [11]. Selection in the encryption method relies on. simply security requirements, computational aspects, and key management, etc.

The study kick-starts with an in-depth examination of academic literature, reference books, and various

research instruments related to the topics of cryptography, steganography, and digital watermarking. The source materials consist of IEEE papers, periodicals, and classical reference works that discuss various encryption algorithms, methods of hiding information, and watermarking techniques [1], [3], [7]. The gathered data is divided into three big sectors: data encryption, data concealment, and data authentication. The first phase is a literature review that mostly includes academic papers, textbooks on data protection and security models, and digital watermarking. In fact, noting the changes.

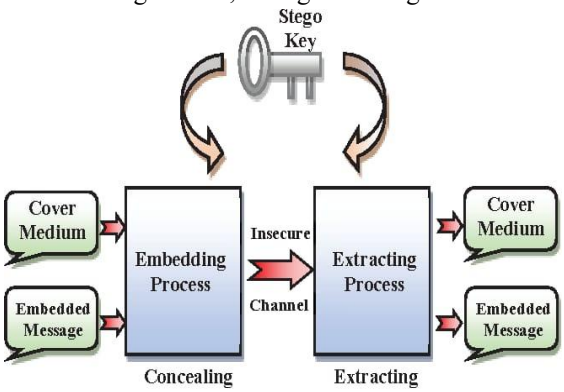

Fig. 2. Block Diagram of a Steganography System

The next step after encryption is the use of steganography for data embedding. The encrypted data is concealed in a cover media, usually a digital image, through steganographic methods like the Least Significant Bit (LSB). The LSB technique is based on altering the minimal bits in the pixels to contain the encrypted data without a significant change in image quality [6], [16]. It is a very important phase as it makes sure that the data remains invisible to the eyes of the unauthorized users. The selection of the cover medium and the embedding method significantly influence the ability to remain imperceptible and resistant to discovery.

The last stage is oriented towards digital watermarking, which is the method of inserting authentication or ownership information into the stego-object. A watermark, which can be a logo, a signature, or a unique identifier, is incorporated into the media in order to substantiate its authenticity and disallow any potential instances of piracy [3], [14]. The watermark can be both visible or invisible depending on the end-use needs. In a majority of secure communication systems, invisible watermarking is the method of choice because it does not disrupt the visual appeal of the media while, at the same time, providing secure layers.

IV. RESULTS

The results of this research are derived from an in-depth analysis of existing literature and studies on the integration of cryptography, steganography, and digital watermarking. Since this work is based on a conceptual and review-based methodology, the results focus on the expected performance, advantages, and effectiveness of the proposed hybrid security model rather than experimental implementation.

TABLE II: Formalization of Security and Performance Criteria

Parameter	Form
Confidentiality	f
Imperceptibility	$\Lambda = fc$
Robustness	$L \approx \lambda$
Data Integrity	$P \approx \lambda$
Authentication	$H \approx 0.30\lambda$
Parameter	Form
Confidentiality	f

The analysis indicates that combining these three techniques significantly enhances the overall security of data communication systems. Every method adds something different to the system: cryptography keeps the data secret, steganography hides the data itself, and digital watermarking allows you to check authenticity and ownership. Combined, these methods form a multi-layered security system that is significantly stronger than any single one of them.

V. CONCLUSION

This research is a complete and detailed examination on how cryptography, steganography, and digital watermarking can be combined for the purpose of secure and reliable data communication. The use of digital platforms for the transmission of sensitive information is becoming very popular. As a result, advanced security mechanisms are being sought continuously and the need for such mechanisms is greater than ever. Purely relying on the traditional methods that use only one security technique at a time may no longer be enough to counter the modern threats from cyber criminals who require stronger and multi-layered protection decreasing attacks.

Based on literature review and analysis, it seems that each method plays a distinct role in data security. Cryptography ensures that data is kept confidential by

converting the clear text into a coded version, which is not understandable to unauthorized users. On the other hand, the existence of the data is still visible after the cryptographic process. By hiding the encrypted data within digital media, steganography not only solves the problem but also makes it less likely for the data to be detected during transmission. Besides, digital watermarking can be used to link the authenticating and verifying of the data to the media through embedding in such a way that the authenticity and integrity of the data are guaranteed.

These three methods, when combined, form a hybrid security model that has several layers of protection. If the security of one layer is breached, the other layers can still protect the data, thereby making it very difficult for unauthorized persons to get access. This approach, in which layers are stacked, greatly increases the level of resistance against various attacks like eavesdropping, data tampering and unauthorized duplication.

While the joint system may increase operational complexity and media quality preservation might be challenging, the benefits of greatly improved security justify these few drawbacks. This hybrid strategy demonstrated effectiveness in scenarios with stringent data protection requirements, including military communications, bank systems, healthcare data exchanges and digital content distribution.

In short, combining steganography, cryptography, and digital watermarking results in a potent, efficient and reliable way to secure data communication in today's digital world. The next research may concentrate on the optimization of these methods by implementing advanced technologies like artificial intelligence, machine learning, and blockchain to enhance performance, scalability and security.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.

[2] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," IEEE Computer, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[3] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed., Morgan Kaufmann, 2008.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[5] K. Bennett, "Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text," Purdue University, Technical Report, 2004.

[6] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in Proc. IEEE Int. Conf. Image Processing (ICIP), 2001, pp. 1019–1022.

[7] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, July 1999.

[8] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2009.

[9] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," in Proc. SPIE Security and Watermarking of Multimedia Contents, 1999.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[11] J. Daemen and V. Rijmen, "AES proposal: Rijndael," National Institute of Standards and Technology (NIST), 2001.

[12] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.

[13] C. Cachin, "An information-theoretic model for steganography," in Proc. 2nd Int. Workshop Information Hiding, 1998, pp. 306–318.

[14] M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, Marcel Dekker, 2004.

[15] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in Proc. ISSA Conference, 2005.

[16] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[17] K. Raja, K. Venugopal, and L. M. Patnaik, "A secure image steganography using LSB, DCT and compression techniques," International Journal of Computer Science, 2012.

[18] S. Gupta and R. Gupta, "Enhanced data security using watermarking and cryptography," International Journal of Computer Applications, 2013.

[19] P. Wayner, Disappearing Cryptography: Information Hiding—Steganography and Watermarking, 3rd ed., Morgan Kaufmann, 2009.
[20] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., Wiley, 1996.