A REVIEW ON DIFFERENT TYPES OF CRYPTOGRAPHY TECHNIQUES" SHOULD BE REPLACED BY "EXPLORING THE POTENTIAL OF STEGANOGRAPHY IN THE MODERN ERA

Vipin Jain*

*Teerthanker Mahaveer Institute of Management and Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: vipin555@rediffmail.com

DOI: 10.5958/2249-7137.2021.02569.6

ABSTRACT

The information world of today is a digital one. Nowadays, data transfer via an insecure channel is a significant source of worry. Simultaneously, intruders are expanding throughout the internet and becoming more active. As a result, certain security precautions must be implemented to safeguard the confidential data from theft. Various methods have been used to encrypt and decode the secret data in order to keep it hidden. The two most well-known methods are cryptography and steganography. These two methods, however, cannot perform as well on their own as they may when used jointly. Steganography is a Greek term that combines the terms stegano and graphy. Steganography is a combination of the words stegano and graphy, which meaning "hidden writing." Steganography is a technique for concealing the fact that data is being sent. While cryptography transforms a secret communication into a format that is not human readable, this method has the drawback of making the encrypted message accessible to everyone. Intruders may attempt to obtain the secret message by using heat and trial methods via the internet in this manner. By concealing the fact that any communication is going place, steganography overcomes cryptography's restriction. The secret message is concealed in steganography in medium other than the original, such as text, image, video, and audio. These two methods are distinct and have distinct meanings. As a result, we will explore different cryptography and steganographic methods used to keep the communication hidden in this article.

KEYWORDS: *Steganography, Cryptograph, LSB, Cipher Text, Steganalysis, Cryptanalysis.*

1. INTRODUCTION

Steganography has been around for quite some time. In the past, Greek historian Herodotus tattooed the secret message on the slave's scalp, and when the hairs grew back, the slave was dispatched to the destination. During WWII, the Germans develop a new technology known as Microdots. In this technique, Germans are instructed to reduce the size of a secret message or image until it is the same size as the typed period. Later, this method was used to engrave a secret message on a wooden piece, which was then covered in wax. In the same manner, invisible ink was created using a novel method(1)(2)(3)(4). The secret message is written with a special type of ink called invisible ink, and the message can only be retrieved when the paper is heated in this method. This strategy was also employed by the British to gain control of India. They're supposed to use a vaccination drum to hide from Indians, then gather their army in India and begin ruling over Indians(5–8).

The prisoner's problem helps to clarify the concept of steganography. In this problem, two inmates devise a plan to elude capture. A warden was assigned to keep an eye on them. As a result, they should begin communicating in such a way that their communication remains undetectable. They utilized a variety of cover media to deliver their message(9,10)(11).

1.1. Application of Steganography:

1. To conceal data transmission via an insecure route.
2. To protect data from being tampered with.
3. It may be utilized in television broadcasting, as well as audio and visual synchronization.
4. To examine any user's network activity.
5. To regulate who has access to digital information.

1.2. Different picture steganography techniques:

1.2.1. Text steganography:

The secret data may be concealed behind any text file that can be transmitted over an insecure channel using this method. Example:

- Message to transmit - Since Evan can run, encrypting text in a natural setting is advantageous.
- Original Message- Since Evan Can Run, It Is Deliberately Effective To Encode Text In Natural Surrounding.
- Secret Message- SECRET INSIDE

1.2.2. Audio Steganography:

Secret data may be concealed behind any audio file using the audio steganography method illustrated in Figure 1. This method often employs two kinds of audio. One audio track serves as a cover for the hidden message, while another serves as a cover for the cover media(12)(13)(14)(15)(16).

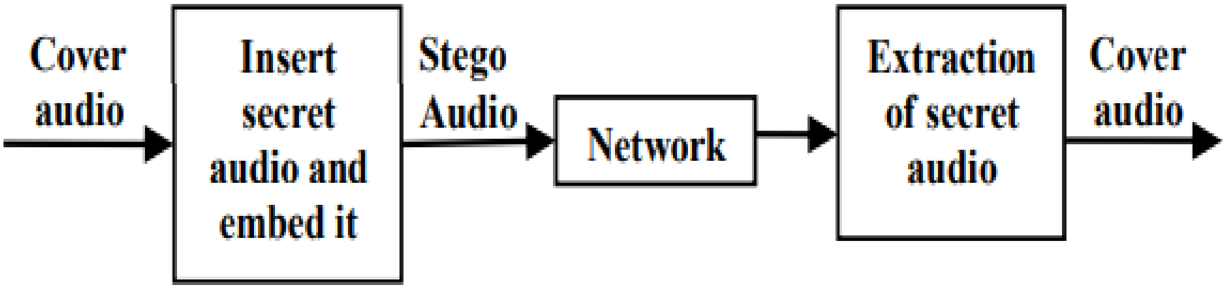


Figure 1: Illustrates the steganography technique of data hidden behind audio.

1.2.3. Video Steganography:

Figure 2 shows how secret data may be concealed behind a video file, allowing a huge quantity of data to be hidden behind it.

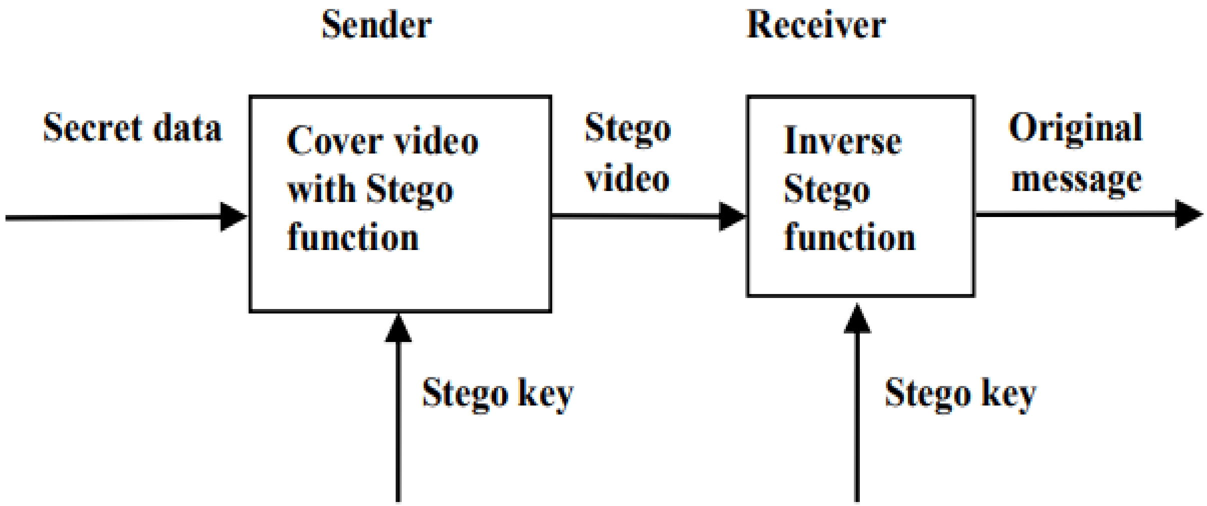


Figure 2: Illustrates the steganography technique of data hidden behind video.

1.2.4. Image Steganography:

The secret data may be concealed behind any cover picture using this method. Hidden data may be found in the form of text or images. The stego picture may then be transmitted via an insecure channel after embedding(17)(18)(19).

2. LITERATURE REVIEW

J. Mandal et al. proposed a method to embed the secret data across the three components of a color picture, namely Red, Green, and Blue, in their paper "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain." To do this, the three RGB components of a color image are first extracted from the picture pixels, and then three distinct m*n matrices are created for each color component. After that, each matrix is subjected to the pixel value differencing technique. The first bit of the secret message is embedded over the first pixel block of the red component, then the second bit is embedded over the first block of the green component, and finally the third bit is embedded over the first pixel block of the blue component. The processing of the suggested technique will proceed in this manner, and the secret message will be incorporated in the overall picture. This technique improves picture quality while while ensuring image security(20).

N. Bourbakis et al. presented a method to guarantee safety and isolation during medical data storage and transmission in their paper "A Synthetic Stegano-Crypto Scheme for Securing Multimedia Medical Records and Their Associations." This method was developed because human errors in medical facilities and hospitals are strongly linked to one another. As a lossless synthetic approach, the suggested technology combines Steganography with Cryptography. Information security is managed using encryption, and secret data association is done using data concealing in this method. SCAN Encryption Compression-Concealing, LSB Hiding, and Regional Hiding with Segmentation are combined into a single information hiding and encryption technique in the proposed synthetic methodology. The SCAN methods are based on a 2D spatial domain approach, which may result in a huge number of transformation scanning pathways. The LSB Hiding algorithm is an information concealment technique in which the secret data is placed on the nth least significant bits of a host picture. In Regional Hiding with Segmentation Information Hiding, pixels from one message picture are hidden in the most matching segments of the host image. The choice of such a complicated safe method was made in order to offer a very high degree of security to private data and in response to the increasing development of different unwanted attacks via an insecure channel (21).

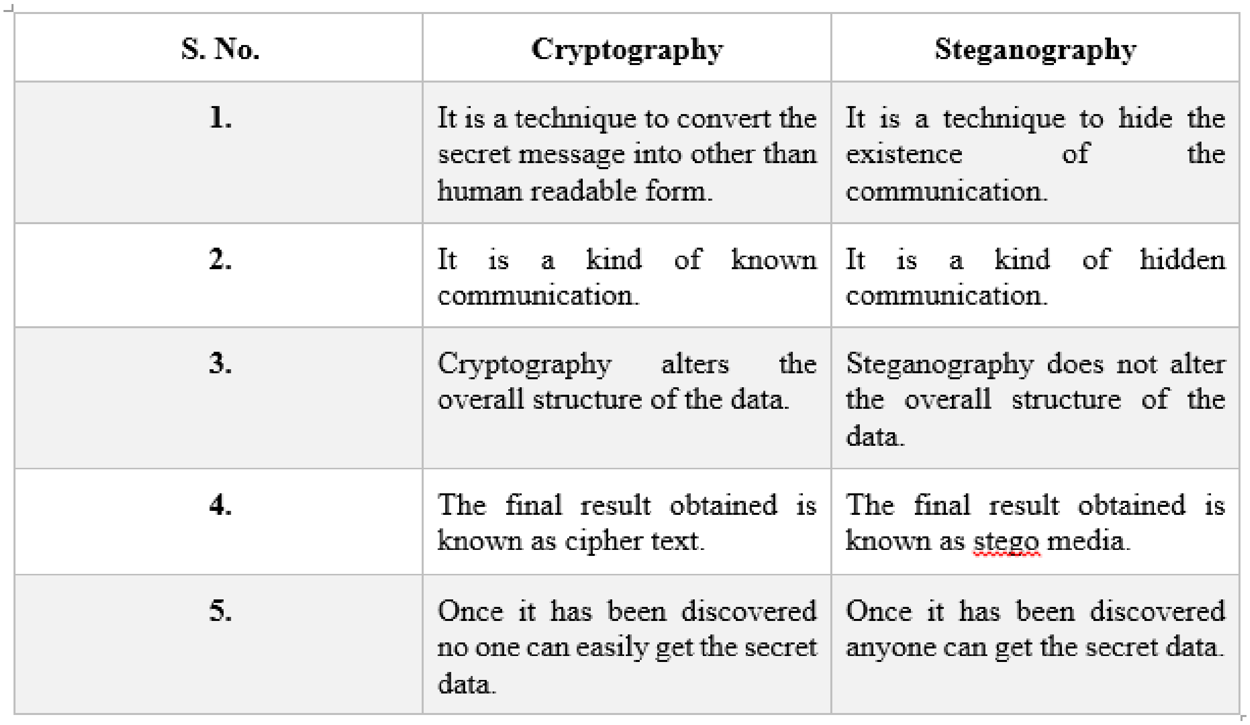
Smita P. Bansod et al. in “Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity,” proposed that cover image is considered as large capacity media. Hybrid cryptography, which combines symmetric and asymmetric key encryption, is used to encrypt the secret message in this method. The RSA Algorithm is used for symmetric key cryptography, which has the benefit of sending the secret message across the channel each time a new key may be used. The DES algorithm is used to create asymmetric key cryptography because it is simple to use and takes much less time to compute than the RSA method. Though both of these methods have disadvantages, the author of this suggested work used the advantages of both techniques to get the greatest outcomes(22).

Atallah M. Al-Shatnawi in “A New Method in Image Steganography with Improved Image Quality” proposed a new technique to overcome the disadvantage of LSB technique . The author used two bmp pictures with sizes of (24 x 502 x 333) and (24 x 646 x165), respectively, in this suggested work. The first image is dark while the second image is bright. The secret message and the pixel value of the picture are then found to have identical bits, and the secret message is inserted there. This method is 83 percent more efficient than the LSB method. On a dual core 2.0 GHz computer, the suggested concealing techniques were implemented in the VB6 programming language. The author suggested a novel method for picture steganography improvement in “Enhancing Steganography in Digital Images,” in which hidden data may be placed at the frames of video files. The area of interest is selected to locate the pixel where data must be saved. In this manner, the movie is first split into frames, then data is saved in a particular area, and a stego video is created. Human face or skin tones are utilized for selecting an area of interest, and the RGB picture is converted into YCbCr to accomplish this. Cr protects data by concealing it and maintaining its secrecy, whereas Cb has a central point of skin tone. The secret data settings were carefully computed before embedding so that they would create very few distortions in the cover video(10).

3. DISCUSSION

Below Table 1 is demonstrating the difference between cryptography and steganography.

TABLE 1: ILLUSTRATES THE DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY.



S. No.	Cryptography	Steganography
1.	It is a technique to convert the secret message into other than human readable form.	It is a technique to hide the existence of the communication.
2.	It is a kind of known communication.	It is a kind of hidden communication.
3.	Cryptography alters the overall structure of the data.	Steganography does not alter the overall structure of the data.
4.	The final result obtained is known as cipher text.	The final result obtained is known as stego media.
5.	Once it has been discovered no one can easily get the secret data.	Once it has been discovered anyone can get the secret data.

2.1. Steganalysis:

Various Steganalysis methods and approaches are available to accomplish this. Here are a few that will be discussed:

2.1.1. Patterns that are unusual:

Suspicions are raised when unusual patterns appear in digital media. TCP/IP packet headers are sometimes used to send secret information across an insecure connection. Because a person does not pay attention to the TCP/IP header because it includes some reserved space, headers are utilized. However, such packets that are unreliable for it may be filtered by the firewall(23).

2.1.2. Visual Detection:

The secrecy of a concealed message is broken by examining repeating patterns. The stego picture is compared to the original cover image to accomplish this, and obvious changes are noted. If the cover picture isn't accessible, known signatures are utilized to determine if the hidden message exists(24)(25)(26). Padding or cropping in a picture is another way to detect the presence of the hidden information. Another consideration is the file size difference between the secret and cover images. A significant color variation or picture quality deterioration may often raise concerns.

Here are some examples of potential Steganographic attacks:

- Steganography-only assault: This attack is only effective if the steganography medium is accessible for analysis.
- Known carrier attack: When both the original cover and the steganography medium are accessible for analysis, this attack is used.

- Known Message assault: This attack is triggered when the Steganalyst is aware of the secret message.
- Chosen Steganography attack: When the message carrier and Steganographic tools are known to analysis, this attack may be successful.
- Chosen Message Attack: When the message and message concealing algorithm are known to the analyst, this attack is used.

2.2. Cryptanalysis:

Cryptanalysis is a method for decrypting the security of cryptographic systems. This method is used to get access to safe encrypted data without knowing the key that was used to encrypt the data. Here are some examples of potential cryptographic attacks:

- Ciphertext-only assault: This attack is used when the ciphertext can be analyzed.
- Known Plain Text Only: When a collection of ciphertext matching to plaintext is known, this attack is used.
- Chosen-plaintext (chosen-ciphertext): This attack is successful when the cryptanalyst can choose the ciphertext at random from a list of plaintext.
- Adaptive selected plaintext: This attack occurs when ciphertext corresponding to any plaintext is recovered using the preceding encryption algorithm's learning.

Though many picture steganography methods have been created, some of the most recent approaches will be covered.

4. CONCLUSION

The primary goal of this article was to provide an overview of different steganography and cryptography methods. As we've seen, encryption and steganography both offer different characteristics for protecting data across the network. However, if they are not combined, they do not provide an accurate outcome. However, the issue with these methods is that they need a lot of room to conceal the secret data. As a result, data compression methods should be used in conjunction with both approaches. Before embedding, compression may be applied to either the secret message or the cover picture. The LSB method, on the other hand, is the most commonly utilized technique, although it has a number of disadvantages, including a reduction in picture quality and the creation of suspicions. As a result, embedding in the edge region is a superior choice for data concealment. Because changes near the edge are difficult to detect, large amounts of data may be stored without being noticed.

REFERENCES

1. Nainwal N, Jawla S, Singh R, Saharan VA. Transdermal applications of ethosomes–a detailed review. Journal of Liposome Research. 2019.

2. Maithani M, Sahu S, Chaudhary AK, Singh R. Development and validation of a novel RP-HPLC method for simultaneous determination of salbutamol sulfate, guaifenesin, and ambroxol hydrochloride in tablet formulation. J Liq Chromatogr Relat Technol. 2012;

3. Sehrawat R, Maithani M, Singh R. Regulatory aspects in development of stability-indicating methods: A review. Chromatographia. 2010.

4. Sandhu M, Sureshkumar V, Prakash C, Dixit R, Solanke AU, Sharma TR, et al. RiceMetaSys for salt and drought stress responsive genes in rice: A web interface for crop improvement. BMC Bioinformatics. 2017;

5. Alemami Y, Mohamed MA, Atiewi S. Research on various cryptography techniques. Int J Recent Technol Eng. 2019;

6. Al Busafi S, Kumar B. Review and analysis of cryptography techniques. In: Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020. 2020.

7. Kumar V, Sharma A, Mitali VK, Sharma A. A survey on various cryptography techniques. Int J Emerg Trends Technol Comput Sci. 2014;

8. Tripathi R, Agrawal S. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. Int J Adv Found Res Comput. 2014;

9. Bharti P, Soni R. A New Approach of Data Hiding in Images using Cryptography and Steganography. Int J Comput Appl. 2012;

10. Al-Shatnawi AM. A new method in image steganography with improved image quality. Appl Math Sci. 2012;

11. Bajaj J, Dwivedi J, Sahu R, Dave V, Verma K, Joshi S, et al. Antidepressant activity of Spathodea campanulata in mice and predictive affinity of spatheosides towards type A monoamine oxidase. Cell Mol Biol. 2021;

12. Manjit K, Abhishek M. Plant growth promoting rhizobacteria (PGPR) for enhancing sustainable agriculture and revolutionized tools for farmers. Res J Biotechnol. 2021;

13. Bilal M, Singh N, Rasool T. A model supported biomedical waste for the enhancement of mechanical properties of concrete. Model Earth Syst Environ. 2021;

14. Sidana A, Kaushal S, Farooq U. Evaluation of antileishmanial potential of Gentiana kurroo royle by in vitro and in silico methods. J Appl Pharm Sci. 2018;

15. Talwar R, Chatterjee AK. Estimation of power dissipation of a 4H-SiC schottky barrier diode with a linearly graded doping profile in the drift region. Maejo Int J Sci Technol. 2009;

16. Sharma R, Chander R. Test OfWeak Form Efficiency In The Indian Stock Market. Indian J Financ. 2010;

17. Yadav CS, Yadav M, Yadav PSS, Kumar R, Yadav S, Yadav KS. Effect of Normalisation for Gender Identification. In: Lecture Notes in Electrical Engineering. 2021.

18. Anand V. Photovoltaic actuated induction motor for driving electric vehicle. Int J Eng Adv Technol. 2019;8(6 Special Issue 3):1612–4.

19. Singh D. Robust controlling of thermal mixing procedure by means of sliding type controlling. Int J Eng Adv Technol. 2019;

20. Mandal J. Colour Image Steganography based on Pixel Value Differencing in Spatial Domain. Int J Inf Sci Tech. 2012;

21. Bourbakis N, Rwabutaza A, Yang M, Skodras AN, Ewing R. A Synthetic stegano-crypto scheme for securing multimedia medical records and their associations. In: DSP 2009: 16th International Conference on Digital Signal Processing, Proceedings. 2009.

22. Bansod SP, Mane VM, Ragha R. Modified BPCS steganography using Hybrid cryptography for improving data embedding capacity. In: Proceedings - 2012 International Conference on Communication, Information and Computing Technology, ICCICT 2012. 2012.

23. Mehta K, Chander R. Examination of january, december and november effects on the indian stock market. Indian J Financ. 2010;

24. Sharma K, Goswami L. RFID based Smart Railway Pantograph Control in a Different Phase of Power Line. In: Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020. 2020.

25. Khatri M, Kumar A. Stability Inspection of Isolated Hydro Power Plant with Cuttlefish Algorithm. In: 2020 International Conference on Decision Aid Sciences and Application, DASA 2020. 2020.

26. Stojkovikj S, Oklevski S, Jasuja OP, Najdoski M. Visualization of latent fingermarks on thermal paper: A new method based on nitrogen dioxide treatment. Forensic Chem. 2020;