Steganography and Cryptography: A Systematic Review

Laxmi Shankar Awasthi[1], Santosh Kumar[2], and Karuna Shankar Awasthi[3]

[1,2,3]Deptt. of Computer Science, Lucknow Public College of Professional Studies, Lucknow.

Abstract

The information world of today is a digital one. Nowadays, data transfer across an insecure channel is a major source of concern. Simultaneously, intruders are expanding across the internet and becoming increasingly active. As a result, some security precautions must be performed to protect the sensitive data from theft. Various ways have been used to encrypt and decrypt the secret data in order to keep it secret. The two most well-known techniques are cryptography and steganography. These two strategies, however, cannot perform as well on their own as they may when used jointly. Steganography is a Greek term that combines the words 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 converts a secret communication into a format that is not human readable, this technology has the drawback of making the encrypted message apparent to everyone. Intruders may try to get the secret message by using heat and trial methods over the internet in this way. By concealing the fact that some transmission is going place, steganography overcomes cryptography's constraint. The secret message is hidden in steganography in medium other than the original, such as text, image, video, and audio. These two strategies are distinct and have distinct meanings. As a result, we will cover several cryptography and steganographic approaches used to keep the communication secret in this paper.

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 World War II, the Germans develop a new technique 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 way, invisible ink was created using a novel technology.

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 utilised by the British to gain control of India. They were supposed to use a vaccination drum to hide themselves from Indians, and then gather their army in India and begin ruling over the Indians. 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 used various cover media to convey their message [1] [2].

A. Application of Steganography:

- To conceal data transmission through an insecure link.
- To protect data from being tampered with.
- It can be utilised in television broadcasting, as well as audio and video synchronisation.
- To examine any user's network traffic.
- To grant access to digital information [8].

B. Different techniques of image Steganography:

1) Text steganography:

The secret data can be buried behind any text file that can be transferred over an insecure channel using this technique.

- Example:
  Message to send - Because Evan is able to run, encoding text in a natural setting is advantageous.
  Original Message- Encoding Text in Natural Surrounding Is Deliberately Effective Since Evan Can Run.
  Secret Message- SECRET INSIDE

2) Audio Steganography:

Secret data can be buried behind any audio media using the audio steganography approach, as seen in Fig 1. This approach often employs two forms of audio. One audio track serves as a cover for the secret message, while another serves as a cover for the cover media.

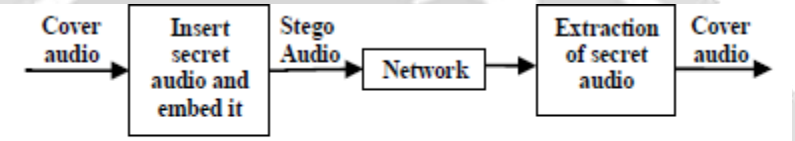

Fig. 1. Example of audio Steganography

3). Video Steganography:

As demonstrated in Fig. 2, the secret data can be buried behind a video file, allowing for a huge amount of data to be hidden.

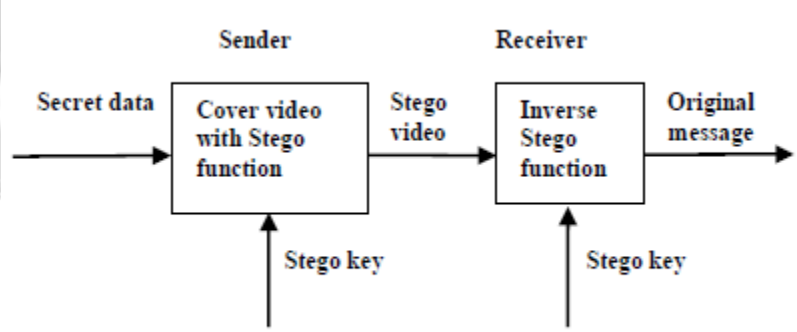

Fig. 2. Example of video Steganography

4). Image Steganography:

The secret data can be buried behind any cover image using this technique. Hidden data can be found in the form of text or images. The stego picture can then be sent through an insecure channel after embedding. The Image Steganography technique is depicted in Figure 3.

Fig. 3. Example of image Steganography

2. PREVIOUS WORK:

The creator of "edge detection" proposed a method for embedding a significant amount of text data across the edge of a colour image. Because of its large storage capacity and undetectability, the edge is chosen as a hiding spot. In this technique, the 3*3 window method is used to detect edges, and the first component alteration method is used to store text. The proposed technique produces a large embedding capacity as well as a high quality embedded image [3].

Author presented KVL technique in "KVL Algorithm: Improved Security & PSNR For Hiding Image In Image Using Steganography," in which author took a cover image and applied transform domain over it to convert it into RGB colour components. The colour components were then transformed to binary code and reduced by up to 35% using the Run Length Encoding technique. Then, using the Triple DES technique and hash function, the compressed data is encrypted and masked behind any cover image that could be used as a stego image. Now, this stego image was transferred across an insecure channel, and the secret message was obtained by reversing the processes at the receiving end [4]. The author developed an Edge based LSB in which edge pixels are utilised to hide the secret message in "A Novel Approach for Data Hiding utilising LSB on Edges of a Gray Scale Cover Images." Two factors, Mean and Standard deviation, were utilised to find the edges of an image. The edge pixels are then obtained using a canny edge detector. This stego image is conveyed to the receiver by integrating the secret message.

The two parameters are obtained again at the receiving end, together with the concealed message [5]. Authors presented a method in "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection." The author of "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" developed an image steganographic technique that combines the RSA and Hash-LSB algorithms to provide greater protection to secret data and the proposed algorithm.

The hash function is utilised to create a pattern in which secret data can be put over the LSB bit of the cover picture in this technique. Data encryption is accomplished using the RSA technique, which provides security against data theft and leaking. Secret data is saved at the LSB of each RGB pixel value of the cover image, resulting in no discernible alterations. This method is significantly more secure than any other method now in use [6].

The author offered a new technique to solve the disadvantages of the LSB technique in "A New Method in Image Steganography with Improved Image Quality." The author used two bmp photos with sizes of (24 x 502 x 333) and (24 x 646 x165), respectively, in this proposed work. The first image is dark while the second image is light. The secret message and the pixel value of the image are then found to have identical bits, and the secret message is placed there. This method is 83 percent more efficient than the LSB method. In VB6 programming, the recommended concealment algorithms have been implemented. In 2012, language was developed on a twin core 2.0 GHz processor [7].

The author presented a new technique for picture steganography augmentation in "Enhancing Steganography in Digital Images," in which hidden data can be put at the frames of video files. The

region of interest is chosen to locate the pixel where data must be saved. In this approach, the movie is first broken into frames, then data is saved in a specific location, and a stego video is created. Human face or skin tones are employed for selecting an area of interest, and the RGB image is converted into YCbCr to do this. Cr protects data by hiding it and maintaining its confidentiality, while Cb has a centre point of skin tone. The secret data parameters were carefully computed before embedding so that they would create relatively few distortions in the cover video [9]. The author of "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain" proposed a method for embedding secret data over the three components of a colour image, namely Red, Green, and Blue. To do this, the three components (RGB) of a colour image are first isolated from the picture pixels, and then three independent m*n matrices are created for each colour component.

After that, each matrix is subjected to the pixel value differencing algorithm. 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 proposed method will proceed in this manner, and the secret message will be integrated in the overall image. This approach improves image quality while also providing good security for the cover image [10]. The author proposed a new way of information concealing in "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," in which a hash LSB technique is used to hide the existence of a secret message. The secret message is also converted into a form that is not human readable using a cryptography process known as the RSA algorithm.

In this method, a combination of steganography and cryptography is employed to hide the existence of the secret message; also, if someone detects the existence of the secret message, obtaining the hidden data without knowing the secret key will be impossible [11]. The author of "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity" proposes that the cover picture be treated as a big capacity medium. 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 advantage of transmitting the secret message over the channel each time a new key can be used. The DES algorithm is used to achieve asymmetric key cryptography, and in this proposed work, the author combined the best features of both methodologies to achieve the best outcomes [12].

The author presented a technique to offer safety and isolation during medical data storage and communication in "A Synthetic Stegano-Crypto Scheme for Securing Multimedia Medical Records and Their Associations." This technique was established because human errors in medical facilities and hospitals are strongly tied to one another. As a lossless synthetic process, the suggested technology combines Steganography with Cryptography. Information security is managed using encryption, and secret data association is done using data concealing in this technique. SCAN Encryption Compression-Concealing, LSB Hiding, and Regional Hiding with Segmentation are combined into a single information hiding and encryption process in the proposed synthetic methodology. The SCAN methods are based on a 2D spatial domain methodology, which can result in a huge number of transformation scanning routes. The LSB Hiding algorithm is an information concealment technique in which the secret data is put on the nth least significant bits of a host picture. In Regional Hiding with Segmentation Information Hiding, pixels from one message image are hidden in the most corresponding segments of the host image. The choice of such a complicated safe technique was made in order to provide a very high level of security to private data and in response to the increasing rise of numerous undesired attacks via an insecure channel [13].

3. CONCLUSION:

The primary goal of this work was to provide an overview of various steganography and cryptography techniques. As we've seen, cryptography and steganography both have different features for protecting data across the network. However, if they are not combined, they do not produce an exact outcome. However, the difficulty with these methods is that they require a lot of room to hide the secret data. As a result, data compression measures should be used in conjunction with both techniques. Before embedding,

compression can be applied to either the secret message or the cover image. The LSB technique, on the other hand, is the most generally utilised technique, although it has a number of downsides, including a reduction in image quality and the creation of suspicions. As a result, embedding in the edge area is a superior choice for data concealment. Because changes near the edge are difficult to detect, large amounts of data can be stored without being noticed.

4. REFERENCES

1. Khalil challita, Hikmat Farhat, "combining steganography and cryptography new directions," IJNCAA, Vol 1, 2011, pp 199-208.
2. Pritam Kumari, Chetna Kumar, Preeyanshi and Jaya Bhushan, "Data Security Using Image Steganography And Weighing Its Techniques," International Journal Of Scientific & Technology Research Volume 2, Issue 11, November 2013, pp. 238-241
3. Sneha Arora, Sanyam Anand, "A Proposed Method for Image Steganography Using Edge Detection," International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 2, February 2013, pp 296-297.
4. Kamlesh Lakhwani1, Kiran Kumari, "KVL Algorithm: Improved Security & PSNR for Hiding Image In Image Using Steganography," International Journal of Computational Engineering Research, 2015, Vol 03, Issue 10, pp.1-6.
5. Krishna Nand Chaturvedi, Amit Doeger, "A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images", International Journal of Computer Applications (0975 – 8887) Volume 86 – No 7, January 2014, pp 36-40.
6. Vijay Kumar Sharma, Vishal Shrivastava,"A Steganography Algorithm for Hiding Image in Image by Improved LSb Substitution by Minimize Detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1 pp 1-8.
7. Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality," Applied Mathematical Sciences, Vol. 6, 2012, no. 79, pp. 3907 – 3915.
8. Jasleen Kour, Deepankar Verma, "Steganography Techniques –A Review Paper," International Journal of Emerging Research in Management &Technology ISSN: 2278-9359, Volume-3, Issue-5, May 2014 pp.132 -135.
9. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Enhancing Steganography In Digital Images," Canadian Conference on Computer and Robot Vision, IEEE 2008, pp: 326-322.
10. J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain," International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp 83-93.
11. Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013. pp. 363-372.
12. Smita P. Bansod Vanita M. Mane Leena R. Ragha, "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity," International Conference Multimedia Medical Records and Their Associations", IEEE 978-1-4244-3298, 1 sept 2009.
13. N. Bourbakis, A. Rwabutaza, M. Yang, A.N. Skodras and R. Ewing, "A Synthetic Stegano-Crypto Scheme for Securing Multimedia Medical Records and Their Associations", IEEE 978-1-4244-3298, 1 sept 2009.