Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

Implementation Of Novel Framework For Improving Cybersecurity Using Steganography

Pinky Shinde[1*] , Dr. Dhanraj Verma[1] , Dr. Santosh Pawar[2] and Dr. Ritesh Yadav[3]

[1]Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore-452016

[2]Department of Electronics & Communication Engineering, Dr. A. P. J. Abdul Kalam University, Indore-452016

[3]Department of Physics, Dr. A. P. J. Abdul Kalam University, Indore-452016

*Corresponding Author Email: pink.shinde@gmail.com

ABSTRACT:

As steganography has been researched in the sense of informatics and computer science, a variety of algorithms have been developed to insert messages in seemingly harmless data, all with the intention of creating secret and secure steganographic protocols in mind. Imperceptibility and robustness are therefore predicted properties of a stego-medium. Robustness is an important property for stopping unintended recipients from discovering secret messages. Even then, the stego agency should be unable to withstand attacker attacks. With all of this in view, the three most important aspects of a steganographic scheme are as follows: Imperceptibility, embedding strength, and robustness are all essential characteristics. Imperceptibility refers to an individual's failure to distinguish between the cover and the stego object, and hence the inability to detect the existence of hidden materials.To implementation of novel framework for improving cybersecurity using steganography Create a novel steganographic algorithm using a multi-level deep learning model.

I. INTRODUCTION

Watermarking and steganography A "noise-tolerant" signal provides a coded signature, such as audio or video. It is typically used to classify the copyright of a digital signal. The material is embedded inside an object to provide copyright security, since this means ownership of the information. Regardless of who or how many copies of the job are produced, no two fingerprints are supposed to leave the same impression. This condition gets more difficult for the property owner as they discover customers who fail to follow the terms of their licence agreement. Gastric helicobacter is a type of bacterium that only develops in the presence of H. pylori and is related to the development of peptic ulcer disease. It doesn't matter whether you succeed or not, as long as you have the job done. The art of concealing a hidden message inside a seemingly harmless item.

Steganography is a Greek term that literally means "covered prose." It incorporates different clandestine modes of communication in order to conceal the post.' The phrase "steganography" was first used in this sense. The book was meant to be an introduction to all aspects of cryptography, with a tendency against modern and unconventional approaches and techniques. Steganography was first recorded in fifth-century BC Greece, when wax tablets were covered to conceal letters. The letter was totally covered under the wax wrapping, notwithstanding the fact that it remained unread. Artaeus, who was married to Miltaus' daughter, attempted to assassinate him and meet with his Greek son-in-law Darius, who was under the Persian king Darius. To that end, he sheared the hair of his most trusted slaves and inked a note on their heads. When the individual's hair grew back, he sent another veiled slave back, and by the time that person arrived, the hair had been cut off. Aeneas managed to supply the soldiers with multimedia communications after several years without this. A woman's threaded earrings can conceal written notes like this. Acrostics, an ancient Greek method, is used to discover a hidden message inside each sentence, such as rhyming a word or place in a book or passage with an entity or name. Although they may be easy, acrostics have stood the test of time. In reality, this technique was widely used during this time period as well. Furthermore, paintings have sometimes been used to hide information, such as altering the length of a line, utilising several colours, or making odd patterns. As great artists such as Leonardo Da Vinci, Michelangelo, and Rafael have had their work decoded, secret meanings in their works have been discovered. During the Franco-Prussian war of 1870, the French realised for the first time that microphotography enabled their birds to hold more information than normal text in messages in some situations, and they used the technique of printing secret text in tiny images for new communications. The idea of printed images smaller than postage stamps is now known as the microdot. It is known as the Microdot invention since it was used during World War II. It was once referred to as "shattering," but it is more commonly referred to as "the German process" or "the German way" of dealing with effects. Since Europe's postal service was well-patrolled at the time, it was frequently used by prisoners and soldiers. The cryptographer Gustav Simmons developed the first Steganography problematical Studies project, known as the Prisoner's Dilemma, in 1983 as a prisoner's method to better interact in a modern era. Krazy Kat is credited with inventing the most prevalent method of steganography, which is also described as a prison escape plan involving two convicts cooperating. They can only communicate via unsecured networks. The warden is aware; otherwise, she would be on the lookout for some sort of error on the part of the inmates. As a consequence, inmates can devise a non-obtrusive method of concealing their communications from the warden. This excerpt from Winbladh's Technologies addresses the question that standard steganography would require an eavesdropper wishing to chat covertly with a listener who is a rider on the prisoner's dilemma.

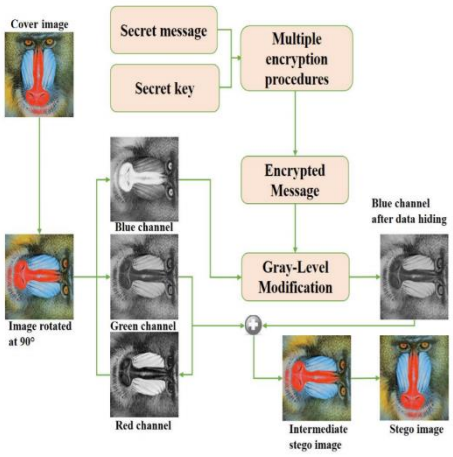

Figure 1: . Recovered hidden image using an encoding/decoding scheme

The steganographer makes minor changes to the media, hoping that the individual seeing it would overlook the internal data, allowing the inside knowledge to be communicated without anybody knowing. Even the convict had to distinguish between cryptography and steganography. Cryptography foresees, but does not obstruct, information protection. However, in countries where cryptography is banned, the rise of open source information activism has expanded the popularity of steganography. Today, the main goal of steganography is to protect classified information. The need for online access has skyrocketed, rendering the internet the most powerful and quick way to communicate with clients and peers. Around the same moment as data on the internet has been turned into a vulnerability for copyright infringement, secrecy has hit new heights.

II. RELATED WORK

Steganography and cryptography are two distinct approaches for maintaining data safe and confidential [9]. Steganography is a means of concealing secret messages in digital media that no one can identify [10]. The primary goal of steganography is to safely transmit secret messages through images [11]. Steganography does not alter the composition of the secret message, but it conceals the shift within the mainstream, rendering it undetectable [11]. Though cryptography conceals the intent of messages in order to keep them concealed from prying eyes [12]. Steganography strategies include the secrecy of the data encoding scheme [13], and once the encoding mechanism is defined, the steganography process may be recognised and tracked. The stenographic approach conceals the fact that messages are being transmitted through digital media; such communication strategies are invisible between the sender and the recipient [14], and encryption obscures the integrity of the information such that only the sender and receiver recognise it [9]. Personal secrecy, individual authenticity, and data authenticity are all aspects of information security addressed by cryptography [15]. More research on these methods, though, is needed to help citizens understand the advantages of combining them. Many traditional steganalysis schemes depend on handcrafted features, and the outcomes are often devoted to the handcrafted technique of strong feature descriptors. Rich graphics, which are high-dimensional vectors designed to capture complex statistics such as dependencies between neighbouring pixels, are the latest cutting-edge features. This level of information is achieved by integrating a number of submodels derived from noise residuals obtained using linear and nonlinear high-pass filters.

Unlike conventional steganalysis techniques, this one relies on utilising deep learning to continuously learn effective functions. Previous research [1] proposed using deep learning to avoid the traditional two-stage steganalysis method. Convolutional Neural Networks are one of the most well-known deep learning architectures, and the current design is based on them. It starts by preprocessing the data with a fixed high-pass filter, then extracts feature illustrations utilising several layers of convolution and pooling operations, and finally transfers the extracted features to completely connected layers for classification. In a nutshell, the feature extraction and classification modules are integrated in a single network architecture. The back-propagation algorithm is used to train the whole network, allowing all parameters in both phases to be fully initialised. Aside from that, we'll discuss how to use transfer learning to help train a CNN model for improved steganalysis results.

III. PROPOSED METHODOLOGY

The suggested approach is a more advanced and dependable method of mapping secret data to one of the RGB image's three channels. The suggested methodology incorporates the principles of transposition, bitxoring, bits shuffling, secret key, and cryptography to construct a complex steganographic scheme. In contrast to other alternatives, the suggested solution has several levels of security. 1) To throw the attacker off balance, all three channels of the input carrier image are transposed so they can be used to map secret data. 2) A set of encryption protocols, one after the other, are used to secure the hidden key and secret details. 3) Utilizing the gray-level adjustment procedure, concealed data is mapped to the carrier image's blue channel (GLM). The proposed solution utilises two distinct modules to protect obscured data from carrier image pixels: encryption and visualisation. Figure 1 represents the proposed system's overall diagrammatic representation. The modules of the proposed algorithm are briefly discussed on the following pages.

Encryption Module

This module is in charge of encrypting the secret key as well as the secret info. This module's final performance is an encrypted private key and secret data pieces. On the hidden key and secret info, this module executes the following operations.

1) Select the secret data and a suitable secret key for encryption

2) Convert the secret key into one-dimensional (1-D) array of bits

3) Apply the bitxor operation on these bits with logical 1.

4) Shuffle these encrypted bits such that the bits with even and odd indices are interchanged.

5) If secret key bit =1

Then perform bitxor operation of secret message bit with logical

1. Else Do not perform bitxor operation.

2. End if 6) Repeat step 4 until all secret data bits are encrypted.

Mapping Module The secret encrypted data is mapped into the carrier image pixels by this module. The carrier image channels are converted first, followed by a 1-1 mapping of hidden data bits and image pixels. This module produces a stego image that contains hidden material.

Embedding Algorithm

Input: Cover colour image, secret key, and secret data

Output: Stego image

1) Select the colour cover image and divide it into red, green, and blue channels

2) Apply image transpose on all the three channels of the input image

3) Encrypt the secret key and secret data according to the encryption module 3.1

4) If the first bit of secret data=1

Then convert all pixel values of blue channel to odd by adding 1

Else

Convert all pixel values of blue channel to even by adding 1

5) Map the secret data of step 4 based on secret key bits (SKB) such that

If SKB=0 && pixel value=even OR SKB=1 && pixel value=odd

` Then leave the pixel unchanged

Else if SKB=0 && pixel value=odd

Then subtract 1 from pixel value

Else if SKB=1 && pixel value=even

Then add 1 to pixel value

6. Repeat step 5 until all secret bits are mapped with the gray-levels of carrier image

7. Take the transpose of all three planes and combine them to make the stego image

Extraction Algorithm

Input: Stego image, secret key

Output: Secret data

1. Divide the red, green, and blue channels in the colour stego image.
2. Apply image transpose to the stego image's three channels.
3. Extract the blue channel's LSB.
4. Repeat steps 3 and 4 before all hidden pieces have been removed successfully.

5. Apply the reverse method of encryption module 3.1 to decode these bits. get the source text

The data presented below represents the experimental results for evaluating picture efficiency. This, as indicated, has been implemented in MATLAB using the Karim et al. [40] technique. The evaluation is carried out using a series of tests on various colour samples of differing dimensions. Similarly, one initiative plans to provide an 8-kilobit text file as part of a series of colourful images, such as a baboon, helicopter, plane, residence, and house in an image file. A second version of the same experiment involves using a variable number of data points in a single standard picture. It occurs in the same image, but at various spatial scales. For comparison reasons, both objective and subjective calculations have been done on the method proposed. It is impossible to see the difference between cartilaginous and noncartilaginous bones with the naked eye. Figure 2 shows standard colour cover images as well as a few stegograms and their brightness distribution histograms. As shown in Figure 2, it is impossible to tell if the cover image or the stego image in the centre of the cover was used. Several techniques, including ones, have been compared using root mean square error (RMS), peak signal-to-noise ratio (PSNR), mean square error (MSE), and normalised cross-relation (NCC) (RMSE). Additional advantages of the proposed method involve histograms, histogram changeability, and comparison diagrams. Eqs. (1)– (2) and (3) are used to obtain the PSNR, MSE, and NCC equations (Equation 4). (4).

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) \quad (1)$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \quad (2)$$

$$RMSE = \sqrt{MSE} \quad (3)$$

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S(x,y)\times C(x,y)\right)}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S(x,y)\right)^2} \quad (4)$$

where x and y are the loop counter dimensions, M is the maximum total of all covered pixels, and N is the cover image, and C is the number of images. Karim et alexperimental .'s findings are presented in shows the aggregate PSNR, MSE, and RMSE ratings for both techniques. Photos with a PSNR of 40 or higher are well-rendered. However, as shown above, the PSNR score (peak signal-to-noise ratio) was observed to be slightly lower than 30dB, resulting in observable deformation in 3D stego picture quality in applications such as CAD, virtual prototyping, and video games. Since data is one of the most important resources to defend as transmitted around the internet, the rising problem of cyber security must be addressed immediately. Data security is mainly associated with safeguarding data from intruders, unauthorised users, and other non-communicating entities. This not only guarantees high security, but it also protects data from being tampered with. Cryptography and steganography are two approaches that have been used to improve the security of data transfers over the internet. Whereas cryptography is characterised as

the technique of concealing information by translating plaintexts to cypher texts and advanced transmitting them to the intended recipient using an undisclosed key, steganography provides or extends security to a greater degree by concealing the cypher text in text, image, video, or other formats. Watermarking and fingerprinting are two additional techniques used in accordance with steganography for data concealment. Watermarking is the process of covering a message in a cover object received by several individuals. It is synonymous with intellectual property protection. In fingerprinting, specific marks are embedded in the cover item that are obtained from various persons.

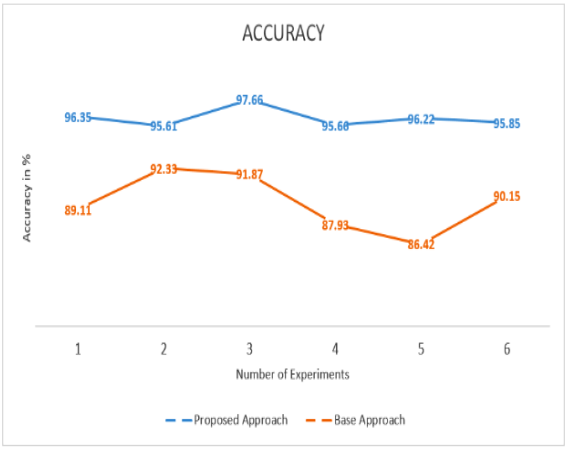

Figure 2: Accuracy proposed approach with existing

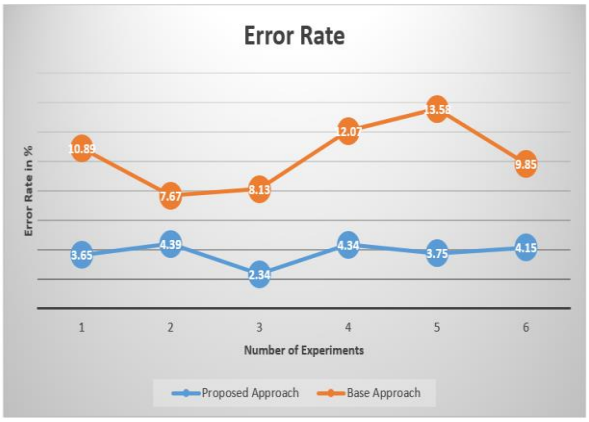

Figure 3: Error rate proposed approach with existing

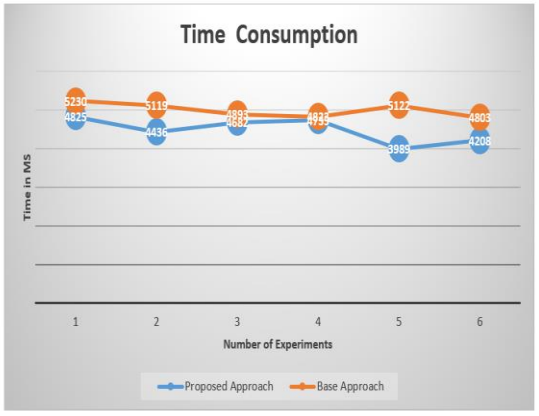

Figure 4: Time proposed approach with existing

The unique field was chosen for its good capacity to mask data that is not easily discoverable by the human visual system in this research to recommend selected views in the development of image steganography utilising the deep learning concept. We suggest a stochastic model for exploitability analysis that considers the relationship between vulnerabilities, their lifecycles, and discovery occurrences such as the period of public distribution, activity availability, and the likelihood of different vulnerabilities becoming discovered.

To perform an exploitability analysis, we employ procedures such as predictable route length, probability path, and node rating. Furthermore, we examine how Exploitability attributes such as access vector (the type of access required to exploit the vulnerability), access complexity (how challenging it is for a hacker to exploit the vulnerability), and authentication (the degree of authentication desired to exploit the vulnerability) change with time. The ability of steganalysis algorithms to adapt to real-world conditions is referred to as practicality. Deep learning in payload with multilevel (HTML, TCP/IP, digital image, audio, and video) steganography implementation

IV. APPLICATIONS OF STEGANOGRAPHY

- Secret Communications = The usage of steganography hides the fact that the email is private, allowing the author, post, and receiver to remain anonymous. Without alerting possible criminals, a trade secret, schematic, or other confidential material may be transmitted.
- Feature Tagging Elements = such as names of people in a picture or positions on a map may be inserted within an image. Only those with the decoding stego-key would be able to retrieve and display the features after copying the stego-image.
- Copyright Protection = Copy retention systems prohibit data from being replicated, typically digital data. The recent increase in interest in digital steganography and data embedding is due to the insertion and study of watermarks to secure copyrighted content.

V. CONCLUSION

As suggested in this report, a steganography approach based on a fixed trend and histogram analysis is proposed. The secret bits are more easily included in the least significant bytes (LSB) of the selected pixels than in random pixels in LSB embedding and retrieval. The children were shown the puzzle bits. The first part is focused on a pattern, while the second is based on colour. It is possible to summarise it as follows: The peak signal-to-noise ratio and lower mean square errors of the techniques suggest that the human visual system is appropriate. Both wellknown images yielded promising outcomes using this technique. These shapes, as shown by Lena, Baboon, and peppers, cannot be identified by the human eye. The stego key is difficult to locate using brute force, rendering it safer by nature. As comparison to the original secret image, the suggested methodology shows that the concealed text is well-distributed throughout the LSB. This technique has more potential than some of the others mentioned previously, and yet the accuracy of the stego image is excellent. Both of these studies, when taken together, are decisive in favour of the proposed data steganography method.

REFERENCE

1. J. Bieniasz and K. Szczypiorski, "Towards Empowering Cyber Attack Resiliency Using Steganography," 2018 4th International Conference on Frontiers of Signal Processing (ICFSP), Poitiers, 2018, pp. 24-28, doi: 10.1109/ICFSP.2018.8552068.

2. A. Kuznetsov, O. Smirnov, A. Onikiychuk, T. Makushenko, O. Anisimova and A. Arischenko, "Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 161-165, doi: 10.1109/DESSERT50317.2020.9125032.

3. D. Han, J. Yang and W. Summers, "Inject Stenography into Cybersecurity Education," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, 2017, pp. 50-55. doi: 10.1109/WAINA.2017.30.

4. M. A. Abbas, "Improving deep learning performance using random forest HTM cortical learning algorithm," 2018 First International Workshop on Deep and Representation Learning (IWDRL), Cairo, 2018, pp. 13-18. doi: 10.1109/IWDRL.2018.8358209.

5. S. Hossain and M. A. N. I. Fahim, "A simple way of image encryption using pixel shuffling and pixel manipulation," 2017 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, 2017, pp. 1-4. doi: 10.1109/ICCITECHN.2017.8281819.

6. H. Kim, N. Bruce, S. Park and H. Lee, "EnCase forensic technology for decrypting stenography algorithm applied in the PowerPoint file," 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, 2016, pp. 1-1. doi: 10.1109/ICACT.2016.7423533.

7. G. R. Kotapalle and S. Kotni, "Security using image processing and deep convolutional neural networks," 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 2018, pp. 1-6. doi: 10.1109/ICIRD.2018.8376292.

8. M. Zheng, S. h. Zhong, S. Wu and J. Jiang, "Steganographer detection via deep residual network," 2017 IEEE International Conference on Multimedia and Expo (ICME), Hong Kong, 2017, pp. 235-240. doi: 10.1109/ICME.2017.8019320

9. S. Wu, S. H. Zhong and Y. Liu, "Steganalysis via Deep Residual Network," 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS), Wuhan, 2016, pp. 1233-1236. doi: 10.1109/ICPADS.2016.0167

10. C. Zheng, M. Shen, X. M. Li and X. Zhang, "Texture adaptive steganography via Convolutional Neural Networks," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2017, pp. 1416-1420. doi: 10.1109/CompComm.2017.8322776.

11. B. Li, M. Wang, J. Huang, and X. Li. A new cost function for spatial image steganography, in ICIP, pp.4206-4210, 2014

12. V. Sedighi and J. Fridrich. Content-adaptive steganography by minimizing statistical detectability, IEEE TIFS, 11(2):221-234, 2016

13. S. Tan and B. Li. Stacked convolutional auto-encoders for steganalysis of digital images, in APSIPA, 2014.

14. Y. Kortsarts, and Y. Kempner, "Enriching Undergraduate Computer Science Curriculum with Steganography Examples," Journal of Computing Sciences in Colleges, Vol. 28 (6), pp. 192-193, June 2013.

15. D. Dhobale, et al. "Steganography by hiding data in TCP/IP headers," International Conference on Advanced Computer Theory & Engineering IEEE, vol 4, pp. 61-65, 2010.

16. K. Kadam, A. Koshti, and P. Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341, May-June 2012.

17. X. M. Li and Lin Dai, "A Novel Approach for Double Image Encryption" in Proceedings of IEEE Region 10 Conference, pp. 697-701, 2010.

18. A. Meghdad; M. B Parmida, and M. H. Hesam,"Chaos-Based Medical Image Encryption Using Symmetric Cryptography," in Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications, 2008.