ADV MATH
SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.7, 4985–4990
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.63 Spec. Iss. on AMABDA-2020

AN INNOVATIVE INVESTIGATION OF STEGANOGRAPHY TO CONTROL CYBER ATTACKS

HUMA KAUSAR ABDUL KADAR[1] AND TRYAMBAK HIRWARKAR[2]

ABSTRACT. Steganography, a part of information hiding techniques, is another route for secure communication. The primary thought of steganography is to implant the secret information into an irrelevant plain computerized media, for example, a picture, a bit of video or sound, and transmit this somewhat changed advanced media to the expected beneficiary without drawing in unlawful onlookers' consideration so the beneficiary can get the touchy information secretly. The steganographic calculation utilizes one public key and one private key to create a binary sequence of pseudorandom numbers that show where the components of the binary sequence of a secret message will be embedded. Prior to the inclusion of the message, the picture experiences a few changes. After the inclusion, the converse changes are applied backward request to the first changes. The addition itself assumes possibly position if an entropy edge of the comparing square is fulfilled and if the pseudorandom number shows to do as such. In this paper, the significant point is to investigate a few different ways of consolidating with steganographic techniques to accomplish a mixture framework. Also, a portion of the distinctions in basic cryptographic techniques were introduced too.

[1] *corresponding author*

2010 *Mathematics Subject Classification.* 13P25, 34K35.

Key words and phrases. Secure Communication, Image Steganography, Data hiding, Text, security.

1. Introduction

Cryptography is the study of ensuring information by encryption techniques. As cryptography all alone doesn't shroud the way that a message is secret, to give this steganography is utilized. The capacity to shield delicate information from foes, particularly during their transmission through channels that are against having spills, is critical in a universe of rising cyberwar. These days, every electronic communication are by and large constantly and naturally checked by both private and state-possessed smart frameworks that have colossal registering power. Specifically, every transmission of figure content calls the consideration of any of these frameworks and surely is picked to be examined, among others, by contenders and any kind of contradicting powers. The utilization of electronic transmission media requires a strategy that points out less administrative programmed frameworks. Present day Steganography offers a degree of administration that incorporates security, legitimacy, honesty, and classification of the transmitted information.

Secure information transmission over communication channels has been a basic issue since the start of the computerized time. With the constant advancement of cryptographic calculations, information communication is made secure and private. Cryptography is a fundamental instrument to shield information from unapproved access by changing over them into ambiguous messages. Be that as it may, such a message raises doubt during transmission. Further, analysts propose that each cryptographic calculation can be effectively attacked. In this way the communication connect is dependable till the cryptographic calculation is unbreakable. A protected information transmission framework comprises of two phases. The primary stage includes encoding the secret message and sending it from the sender to the beneficiary. The subsequent stage contains getting the encoded message and unscrambling it at the recipient's end.

A fruitful attack requires a block attempt of the encoded messages and decoding it to remove the first message. Since a cryptographic calculation can be effectively attacked the communication framework gets shaky. Along these lines there emerges the need to conceal the presence of the protected communication framework on display. This is the place steganography is required. Steganography is the technique for disguising concealed messages inside other computerized media. It weights on protecting the message mystery as opposed to making the concealed information secure against attacks. Not just it conceals the rationale of secret message yet it additionally typifies it into spread pictures. The mix of cryptography with steganography builds the security of a protected communication channel; as a fruitful attack would require modifying the procedure of information hiding and information extraction. In this manner breaking gets more enthusiastically since it requires ID of transporter that disguises the secret message before its extraction and interpreting.

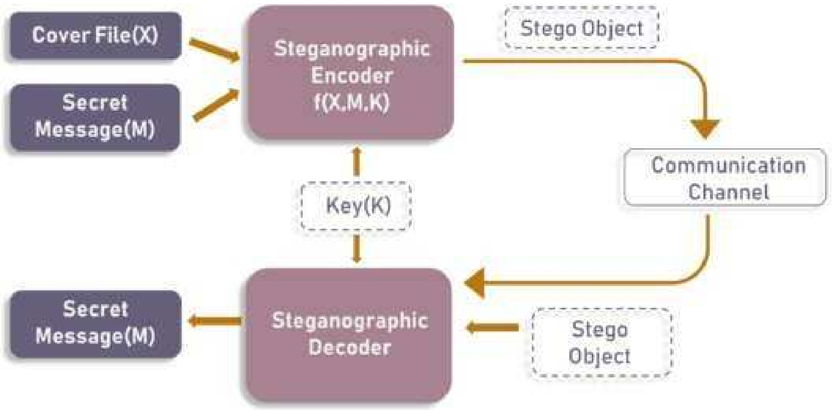

FIGURE 1. Simple architecture of steganography

The performance of stenographic algorithms can be estimated by two principle rules, installing limit and perceptibility. In this manner, novel steganographic algorithms are relied upon to build the picture limit and the encryption quality of the message. The picture limit can be expanded by versatile techniques that choose where to embed best the message. For instance, the Pixel-Value Differencing technique proposes to insert a bigger number of information in edged regions than in smooth territories. In steganography, the implanting limit is characterized as the most extreme number of bits that can be installed in a given spread picture. In any case, the steganographic limit is the greatest number of bits that can be installed in a given spread picture with an immaterial likelihood of location by a foe. Accordingly, the inserting limit is bigger than the steganographic limit.

2. LITERATURE REVIEW

The staggered steganography was initially proposed by Al-Najjar for picture steganography in [1]. The fundamental thought in this paper was to conceal a distraction picture into LSB places of the spread and the first secret information is installed into the LSB places of the bait picture.

Encryption and steganography are two general techniques for hiding secret information [2, 3, 4]. Information is shrouded utilizing an encoding strategy that lone approved people with the best possible key can decipher it in encryption. Then again, steganography shrouds secret information such a way, that concealed information is impalpable to the customary eyewitness. The secret information can be implanted legitimately or some change can be applied to it before the installing procedure. By and large, changes incorporate encryption, pressure, change or a blend of advanced change techniques. In [4], Vitaliev proposed two strategies for information hiding. In the primary strategy, plain content is covered up into a sound sign and in the subsequent technique; a sound document is covered up in a picture object. In [5], Petitcolas et al. introduced a strategy where a book object is covered up into another content article. In [6], Al-Najjar et al. proposed a technique where a sound record is installed in a picture in the wake of performing encryption and pressure. In [7], Marvel proposed a shrouded communication strategy by hiding of a picture into another picture in his Ph.D. Paper. In [8], Solanki introduced a media information hiding method to conceal a picture into a video document in his Ph.D. Paper.

In [9], Lou et al. proposed an information hiding strategy to secure a clinical information. This paper recommends a numerous layer information hiding method in spatial space. The decreased distinction development strategy is used to implant the bit stream at all critical bits (LSBs) of the extended contrasts. A lot of information is implanted in a clinical picture by utilizing this strategy where nature of the picture is likewise be kept up. Additionally, the first picture can be reestablished subsequent to extricating the concealed information from the stego-picture.

Mixed drink party impact is utilized in sound steganography framework where visually impaired key idea is applied to oppose the attack in the framework [10].

Table 1: Comparative investigation of present steganography for cyber attacks

S. No.	**Author (year)**	**Proposed**	**Merits**
1	Krishna Bhowal et al. (2019)	Proposed method has several potential benefits in hidden communication.	To update the level of security while transmitting the confidential information over public channels
2	Radu Nicolae et al. (2018)	Using an Arduino development board (or equivalent)	Increasing the accuracy and the resolution of the forecast and allows early warning in case of extreme weather phenomenon
3	Åđtefan MOCANU et al. (2017)	A combination of image based steganography with encryption	The original information is encrypted and embedded into different graphic sent to the destination through different channels and then restored.
4	Marwan Ali Albahar et al. (2017)	A novel method based on Steganography to fortify the pairing process and thwart MITM attacks	Used for providing a high level of security
5	Marwa et al. (2016)	A merged technique for data security has been proposed using Cryptography and Steganography technques	To improve the security of the information. Two levels of security have been provided using the proposed hybrid technique.

CONCLUSION

Steganography expands the security of information to be transmitted and furthermore guarantees that lone approved work force can approach that message. This paper presents an audit of steganography and techniques that are utilized for steganography. Different papers have been evaluated on steganography. It is examined that there is different kinds of steganography like content, sound, video, picture, system or convention steganography. Techniques of steganography have been checked on and concentrated in the paper.

REFERENCES

[1] J. AL-NAJJAR: *The decoy: Multi-level digital multimedia steganography model*, Proc. of 12th WSEAS International Conference on Communications, Heraklion, Greece, July. 2008, 23-25.

[2] R.J. ANDERSON, F.A.P. PETITCOLAS: *On the limits of the steganography*, IEEE Journal of Selected Areas in Communications, **16**(4) 1998, 474-481.

[3] D. ARTZ: *Digital steganography: Hiding data within data*, IEEE Internet Computing Archive, **5**(3) (2001), 75-80.

[4] D. VITALIEV: *Digital Security and Privacy for Human Rights Defenders*, Dublin: The International Foundation for Human Right Defenders, 2007. 77-81.

[5] F.A.P. PETITCOLAS, R.J. ANDERSON, M.G. KUHN: *Information hidingâĂŞA survey*, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, **87** (1999), 1062-1078.

[6] A.J. AL-NAJJAR, A.K. ALVI, S.U. IDREES, A.M. AL-MANEA: *Hiding Encrypted Speech Using Steganography*, China, Sept. 15âĂŞ17: WSEAS Beijing, 2007, 275-281.

[7] L.M. MARVEL: *Image steganography for hidden communication*, Ph.D. Dissertation. University of Delaware, spring, 1999.

[8] M. SOLANKI: *Multimedia Data Hiding: From Fundamental Issues to Practical Techniques*, Ph.D. Dissertation. Santa Barbara, US: University of California, 2005.

[9] D.C. LOU, M.C. HU, J.L. LIU: *Multiple layer data hiding scheme for medical images*, Computer Standards and Interfaces. **31**(2) (2009), 329-335.

[10] B. GUPTA BANIK, S.K. BANDYOPADHYAY: *Blind key based attack resistant audio steganography using cocktail party effect*, Security and Communication Networks, **2018** (2018), Art. no. 1781384, 1-21.

[1,2]DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, SRI SATYA SAI UNIVERSITY OF TECHNOLOGY & MEDICAL SCIENCES, SEHORE, BHOPAL-INDORE ROAD, MADHYA PRADESH, INDIA.

E-mail address: humak1523@gmail.com