IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Implementing Steganography in E-commerce Systems

Dr R RAMYADEVI
ASSISTANT PROFESSOR, SRM IST, RAMAPURAM, CHENNAI

Ms R PRIYA
ASSISTANT PROFESSOR, SRM IST, RAMAPURAM, CHENNAI

***Abstract*—Without a documented security policy stating what assets are to be safeguarded and what is required to protect those assets, it is impossible to develop secure commerce systems. Threats will be assessed, and rules will be implemented to protect those assets. Protecting Electronic Commerce Assets is dependent on both defense and commercial security rules, which say that assets must be protected from unauthorized disclosure, modification, and destruction. Outsiders should not be given access to firm private information. Outsiders should not be given access to secret company information. Assets are protected while in transit between client computers and remote servers with Protecting Electronic Commerce Channels. During communication, steganography is the skill of concealing information within files. The strength of this study is to investigate and the cryptographic technique employed determines the effectiveness of steganography used on 'multimedia' files like text, static picture, audio, and video. Either the cover must be made more resistant to steganography or a better steganographic algorithm must be created to achieve confidentiality.**

Keywords — E-commerce, security, Steganography, Cryptography, Segmentation, Steganalysis

I. INTRODUCTION

With the quick development and utilization of E-commerce, privacy has turned into a progressing and increasing concern for the clients, suppliers, technologists just as the approach creators. While it is hard to finish an exchange in a web-based business by a client without giving private data, shielding that data from multiplying is one more troublesome issue for the suppliers, technologists and approach producers. clients of internet businesses are reluctant to give private data or even to peruse on the web on the off chance that they accept their security isn't ensured.

There are advances in policies, just as are being developed stages to assist with ensuring protection at current and in future. BBB Online, TRUSTe and WebTrust are a portion of the organizations offering types of assistance for normalized security insurance innovation and strategy. In any case, there is a need to find out about the scope of security issues to fabricate usable and powerful systems for those organizations and other protection assurance advancements and approaches. there is a need to find out about the scope of security issues to fabricate usable and viable systems for those organizations and other security-protected innovations and arrangements. This paper presents past, existing, and future security issues and their answers regarding internet business.

A. PRIVACY AND SECURITY IN E-COMMERCE

A set of criteria necessary to maintain an individual's dignity and autonomy are all examples of the phrase "privacy" [12]. The word commerce is an act of trade between two parties in which a set of conditions and mutual satisfaction are negotiated, based on the building of trust between the parties. By utilising an online system that is available through computer systems and public networks, like the internet, "e-commerce" does the same objective.

The term "privacy in e-commerce" refers to the protection of both the privacy of entities involved in e-commerce transactions. People are currently living in the e-commerce era. Trading practices are increasingly shifting from "conventional" to e-commerce. [14] People submit personal information while performing e-commerce transactions, and that information is disseminated and reaches the hands of unauthorized parties, raising security and privacy concerns. Every day, there is news concerning

possible security breaches on the Internet and in e-commerce.

Several surveys performed around the world over the last few decades have indicated high levels of awareness about e-commerce privacy. However, several studies, technologies, and regulations have been developed to address the issues of privacy threats and concerns. This paper presents general information regarding e-commerce privacy, methods people are losing their privacy while using e-commerce, privacy threats, existing technology and rules to preserve privacy, and research in this article.

B. E-Commerce Framework and Privacy Issues

The fundamental objective of e-commerce is to trade between business-to-business (B2B), business-to-consumer (B2C), and consumer-to-consumer (C2C) in an online shop accessible over the internet. Private information such as addresses (transmitted as mailing/billing information), credit card numbers (exchanged for payments), and other personal information is exchanged between parties engaging in this type of commerce. to finish a transaction. [19]The catch is that the parties' information is maintained and warehoused for other commercial objectives such as direct marketing, research, and selling to third parties.

TABLE I. MINIMUM REQUIREMENTS FOR SECURE ELECTRONIC COMMERCE

Requirements	Meaning
Integrity	prevention against unauthorized data modification
Nonrepudiation	prevention against any one party from reneging on an agreement after the fact
Authenticity	authentication of data source
Confidentiality	protection against unauthorized data disclosure
Privacy	provision of data control and disclosure
Availability	Availability

E-commerce is seen as a significant technique for gathering personal information from customers. Monitoring techniques may be linked to e-commerce through various means, such as "Applets," which can track and gather users' browsing behaviour, as well as private information such as passwords stored in cookies.

C. STEGANOGRAPHY

Steganography is the practise of concealing secret information within a quasi-file or message in order to evade detection. Although most of the research has focused on approaches such as Cryptography to render secret information unreadable to an unwanted recipient, more emphasis should be given on hiding this confidential info so that the undesired recipient is ignorant.

As an additional factor for concealing or protecting data, steganography can be combined with encryption. The contrast between the two division in steganography is as described in the following: Cryptography attempts to encrypt information, while steganography tries to encapsulate it.

Steganography's purpose is to conceal secret information within a carrier media so that it can be securely conveyed with a low chance of being traced. Steganography could be refers to the art and science of writing concealed messages in such a way that almost no one other than the sender and intended receiver is aware of their existence [1]. Through concealment, this creates a sense of security.

An encrypted message may additionally be very conspicuous. One would possibly now not understand the supposed meaning of the message; however it is obvious that it exists. Steganography makes a try to conceal the truth that the secret alternate even exists, thereby no longer drawing interest to it. The file, like pictures, sound, textual content, audio, or video, replaces bits of unused facts with some distinct bits that have been acquired secretly or unauthorized.

The Steganographic procedure is summarised in the diagram below[10]:

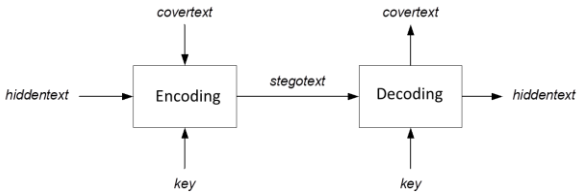

FIG. 1 BLOCK DIAGRAM OF A STEGANOGRAPHY SYSTEM

1) HISTORY OF STEGANOGRAPHY

The word steganography is derived from the Greek words steganos meaning hidden or protected whereas graph (meaning to put in writing). The exercise can be traced again to the Golden Age in Greece, the place where it is believed that the Miletus ruler, Histaeus used steganography to ship a secret message to his buddy Aristagorus to prepare a rebel in opposition to the Persian. Histaeus shaved the head of his most relied on slave, and embed the message on his scalp [2]. Once the hair had grown back, the slave used to be despatched to Aristagoras to supply the hidden message.

In some stories of Steganography in Greek history, a secret message was inscribed on a wooden tablet and covered with wax. The engraved tablet may therefore be readily delivered to the appropriate recipient without raising any suspicions about the existence of the hidden message. In 440 BC, the Spartan ruler Demaratus is supposed to have used this approach to deliver a secret message warning of imminent attacks on Greece.

According to more recent sources, American military personnel used Steganography during World War II to conceal secret communications from the Japanese. They spoke the Navaho language, an Athabaskan language spoken by the Navajo in the southwest United States. This was a more secure and quicker means of communication than radio. It was safer since the Japanese had never heard this language before and so couldn't comprehend it, and it was faster because no encryption was necessary or utilized. Null Ciphers were also widely used as a kind of Steganography in the nineteenth century. This method of transmitting secret information is still widely used today, particularly by prison gangs. Null Ciphers are a traditional method of hiding a message in another without the need for a complex algorithm..

2) BACKGROUND

Recently, the research on hypothetical establishments of data concealment has progressed rapidly. Embedding the process of data concealment into secured correspondences improved data concealing computations and precise models of channel limits and lapse rates.

The fundamental and most important requirement of steganography frameworks is that the hidden message is indistinguishable from the original message by other people. The framework has to be imperceptible in nature. Additionally, stego-media, which uses separated messages, is undefined from spread media, which uses only plain text messages.

Spread media and stego-media should appear indistinguishable under every possible measurable assault, and the implantation method should preserve media constancy. [8] The contrast between stego-media and spread media must clearly be seen.

Traditionally, steganography employs two types of systems: a public key and private key. Both sender and receiver impart a secret key to convey a message. Here, the data message may take any form and can be transmitted as a data stream. Open key cryptography utilizes two keys, - a public and a private key. The private key is used for separating the shrouded message while the public key is used for implanting the secret message. In spite of the intimidating number of steganographic systems used, research on the "detainees' issue" was abandoned by Simmons[5] in 1983. The author of the paper examines in detail steganographic methods Ref. [2].

II. STEGANOGRAPHY TECHNIQUES

Various techniques are used in Steganography. Some of these include:

A. Physical Steganography :

To hide messages, you need some kind of physical medium. Examples from history, such as the use of wax tables and shaven heads, date to the Greco-Roman era highlighted in the History section above.

The use of microdots is a recent example of physical steganography. In the early 20th century, espionage agents used microdots to send information back and forth. The microdot traditionally had a size less than that of a typewriter period. Paper microdots in WWII were embedded in and covered with collodion (an adhesive). By viewing it against a reflective surface, one could observe it glancing light. There are alternative techniques, such as inserting microdots into slits cut along the edge of a post card[1].

B. Printed Steganography

Steganography digital output can take the form of printed documents. An initial encryption of the message, the plaintext, produces a ciphertext. In order to create the stegotext, a cover text is modified so it can contain the ciphertext. Cover texts can be designed to carry secret messages by manipulating parameters such as letter size, typeface, spacing, etc. The recipient can only decode a message once they have figured out the encryption algorithm. Imagine staring at a picture for a long period of time and trying to adjust your vision until you see a different shape emerge from it.

C. Network Steganography

An example of network steganography is the use of information concealing methods to hide data during normal transmissions of data. Network steganography takes advantage of communication protocols' control elements and internal functionality to encrypt data, as opposed to the typical steganographic methods that use digital media (images, audio and video files) as a carrier for hidden information. such techniques are harder to detect and eliminate[1]

In most cases, network steganography involves modifying the properties of one protocol, which can either be the PDU (Protocol Data Unit), the time relationships between the exchanged PDUs, or both (hybrid methods).

The use of Voice over Internet Protocol (VoIP) has become more popular as a way to practice Steganography, hiding a secret message in voice data. Here is an example:

During these new Eras of Steganography, instead of using the actual carrier, co-conspirators are using the protocols governing carriers' path through the Internet.

As the communicators converse, they can send a longer secret message (or a more detailed secret image) the longer the conversation lasts.

Furthermore, the hidden payload cannot be detected due to ephemerality inherent in data. The concealment takes place within data that lasts only for a short time, making the hidden payload nearly impossible to detect, much less stop.

D. Digital Steganography

Digital Steganography involves hiding bits or bytes into digital media such as images, audio, and video files, and then transmitting that media via network. In digital steganography there are several methods of concealing information. Currently, there are more than 800 known digital steganography tools available at little or no cost. In digital steganography, there are various methods to conceal information. The most common are LSB and injection.[8].

Steganography process :

Cover-media + Hidden data + Stego-key = Stego-medium

Cover media:

- It is the file in which the secret information can be stored.
- Image or audio files can be used as cover-media.

stego-key:

- stego-key can be used to encrypt cover-media

stego-medium:

- The stego medium file is the output of the following technique.
- SB bits are being replaced with data bits.

1101001**0**

MSB LSB

LSB = Least Significant Bit

MSB = Most Significant Bit

Modifying the LSB bit merely affects sensory attention by shifting the byte value one higher or lower than the original value.

In the least significant bits of an image, information can be hidden. For example, we can hide 3 bits in each pixel (1 bit / Byte) in a 24-bit image of 1024x768 pixels, so 1024x768x3 bits = 29.5 KB can be hidden in this 2.3 MB file. Types of Steganography

Types of Steganography :

Images

- LSB
- DCT encoding LSB of MS Byte
- Spread Spectrum

Audio

- LSB (added noise can be heard)
- Phase Coding
- Spread Spectrum
- Tone Insertion
- Echo Data Hiding

III. DIGITAL STEGANOGRAPHY METHODS

A. Images

The idea of steganography in images is to hide certain secret information within pictures. One can just think of an image file as a binary representation of the colour of each pixel as picture element of the picture composing the image.

Images are usually eight-bit or 24-bit. Steganography is best performed with Bitmap (BMP) images, which use the 8-bit color scheme. Bitmap images use red, green, and blue values as the three primary colors in the image. This binary color representation is used for steganography. Information is hidden using LSB, where the last bit or two of each RGB value is replaced with a bit of the secret message. Suppose you have a secret message stored as plain text; you might be able to read those bits in twos, and then force the next RGB value of that pixel to match those bits.[1] However, humans are unlikely to notice an overall change in the image despite the change of pixel color.[3]

With this method, you can encode the entire secret message into the image with minimal impact on the image. Peripheral recipients can decode the message by combining the last bit(s) from each RGB value to derive the secret message.

Although Steganography can be performed on other image files types such as Jpegs, it is more difficult than with Bitmap image file types. This is thanks to the very fact that Jpegs use “lossy” compression to scale back the disk size of the general file, which suggests that the expanded image is extremely nearly the same because the original but not a particular duplicate. Jpegs don't store RGB values for every pixel within the image. In the case of jpegs, the easiest way to do this might be to change an entire pixel’s value to match that of the secret method. As long as the method of selecting the pixels to control is known by both sender and receiver, the tactic will work even as well [4].

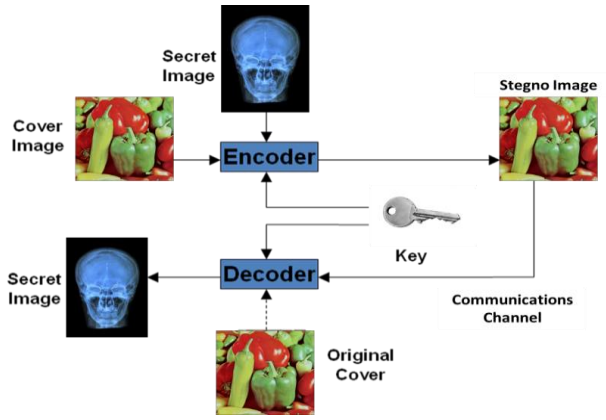

FIG. 2 IMAGE STEGANOGRAPHY

Despite the fact that Steganography can be performed on other picture records types like Jpegs, it is more troublesome than with Bitmap picture document types. This is because of the way that Jpegs use "lossy" pressure to lessen the plate size of the general record, which implies that the extended picture is practically equivalent to the first however not a precise copy.

There are many good examples everywhere of how Steganography is used in images. Figure 2 below may be a map of the Burlington, Vermont, airport This image has been embedded into various images including the photographs below (Figure 3 and Figure 4) [5].

Jpegs don't store RGB esteems for every pixel in the picture. On account of jpegs, the most effortless approach to do this may be to change a whole pixel's worth to coordinate with that of the mysterious strategy. However long the technique for picking the pixels to control is perceived by both sender and collector, the strategy will work similarly also [4].

There are numerous genuine models wherever of how Steganography is utilized in pictures. Figure 2 beneath is a guide of the Burlington, Vermont, air terminal This picture has been implanted into different pictures including the photos underneath (Figure 3 and Figure 4) [5].

B. Audio

Adding information in sound records is similar to inserting pieces/bytes in image documents. [2] However, the goal is to avoid noticeable perceptible deformity in this case.

Disguising data within sound documents can be accomplished in a variety of ways[8].

- Low Bit Encoding: This method is similar to the LSB strategy used in images. The main problem with this approach is that it is primarily directed at the human ear.
- In audio files, steganography is essentially the same as it is in image files, i.e. packing bits/bytes. The goal here, though, is to avoid perceptible distortion. There are a variety of ways that can be used to hide information in audio recordings.
- Spread Spectrum: The data is covered up within a carrier medium and conveyed across the periodicity range, which incorporates adding irregular commotion to the sign.

1) LEAST SIGNIFICANT BIT (LSB)

Least Significant Bit (LSB) is a method utilized in computerized Steganography. The most un-huge bit term comes from the numeric meaning of the pieces in a byte. The high-request or most huge bit is the one with the most noteworthy number juggling esteem (i.e., 27=128), [9]though the low-request or least huge bit is the one with the most reduced math esteem (i.e., 20=1).

The most un-huge pieces are the weak spaces of the record and are the playing ground for Steganography. These pieces/bytes can be subbed with the data to be covered up without altogether modifying the document [2].

A straightforward illustration of LSB substitution[2]; to cover the person 'G' across the eight bytes beneath of a transporter document (the most un-huge pieces are underlined):

10010101 00001101 11001001 10010110

00001111 11001011 10011111 00010000

A 'G' is addressed in the American Standard Code for Information Interchange (ASCII) as the double string 01000111. [8] These eight pieces can be kept in touch with the LSB of every one of the eight transporter bytes as follows:

10010100 00001101 11001000 10010110

00001110 11001011 10011111 00010001

Infusion

As the name recommends, this technique includes just infusing the data to be stowed away in the transporter document (a record which contains stowed away data) [11]

2) Comparison with Cryptography

Steganography is not be confused with Cryptography. The goal of Cryptography is to prevent an unintended recipient from determining the meaning of the secret message. The practice involves scrambling the message thereby rendering it illegible to the unintended recipient. The goal Steganography is to prevent the unintended recipient from eve suspecting that a secret message exists. The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key. In steganography, the message itself may not be difficult to decode, but most people would not detect the presence of the message.

TABLE II. STEGANOGRAPHY V/S CRYPTOGRAPHY

Steganography	Cryptography
Passing of an unknown message	Passing of a known message
Steganography keeps the existence of communication from being discovered.	Encryption protects the contents of a communication from being discovered by an untrusted source.
Technology that is not widely known	Technology that is widely used
For several formats, technology is still being developed.	Familiar with the majority of the algorithms.
Once a message has been detected, it is known.	Strong current algorithm is resistant to attacks ,larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography modify the construction of the message

When Cryptography is combined with Steganography, it creates a strong kind of security that is difficult to detect. The ultimate in private communication is achieved by first encrypting a secret message and then concealing it in a carrier medium. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable, will arouse suspicion. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

IV. CONCLUSION

According to the findings of this study, steganography technology has improved the security of e-commerce. The steganography technique can be customized to fit the needs of each individual e-Commerce system. Furthermore, one can choose an encryption technique to encrypt the data based on the execution time. This research proposes a Steganography method for sending data securely via the internet. This technology provides a very safe way of communicating data to the user by using a steganography method to obscure information. By integrating various cryptographic approaches with steganography, data can be transmitted more securely and confidentiality can be increased. It can also be utilised in Facial and Human Computer Interaction for Steganographic Authentication.

REFERENCES

[1] Kocher, Paul, et al. "Self-protecting digital content." *CRI Content Security Research Initiative, Tech. Rep* (2003).

[2] Devi, R. Ramya, and D. Pugazhenthi. "Ideal sampling rate to reduce distortion in audio steganography." Procedia Computer Science 85 (2016): 418-424.

[3] Gou, Hongmei, Ashwin Swaminathan, and Min Wu. "Noise features for image tampering detection and steganalysis." *2007 IEEE International Conference on Image Processing*. Vol. 6. IEEE, 2007.

[4] Odeh, Ammar. Robust Text Steganography Algorithms for Secure Data Communications. Diss. 2015.

[5] Judge, James C. "Steganography: past, present, future." *SANS white paper* 30 (2001).

[6] Fridrich, Jessica. Steganography in digital media: principles, algorithms, and applications. Cambridge University Press, 2009.

[7] Gutub, Adnan, and Faiza Al-Shaarani. "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons." *Arabian Journal for Science and Engineering* 45.4 (2020): 2631-2644.

[8] Wu, Junqi, et al. "Audio steganography based on iterative adversarial attacks against convolutional neural networks." *IEEE Transactions on Information Forensics and Security* 15 (2020): 2282-2294.

[9] Ali, Ahmed Hussain, et al. "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain." *Multimedia Tools and Applications* 77.23 (2018): 31487-31516.

[10] Saravanan, M., and A. Priya. "An Algorithm for Security Enhancement in Image Transmission Using Steganography." *Journal of the Institute of Electronics and Computer* 1.1 (2019): 1-8.

[11] Yang, Zhongliang, et al. "Aag-stega: Automatic audio generation-based steganography." *arXiv preprint arXiv:1809.03463* (2018).

[12] Bansal, S. "Data Security by Steganography: A Review." International Journal of Scientific Research in Network Security and Communication 7.1 (2019): 10-12.

[13] Narayana Rao, T. Venkat, Karnati Yashwanth Reddy, and Ganji Dinesh Kumar. "Securing Transactions in E-Commerce using Visual Cryptography and Steganography." *International Journal of Advanced Research in Computer Science* 8.3 (2017).

[14] Welpulwar, Awanika, et al. "Securing E-Transaction Using Cryptography & Steganography." (2018).

[15] Jagtap, Santosh Tukaram. "effective steganographic mechanism for transactional e commerce to manage cyber security." (2019).

[16] Mastkar, Nishi S., et al. "Survey Paper on Securing Online Transaction Using Cryptography & Steganography." (2018).

[17] Chakraborty, Suman, and Anil Bikash Chowdhury. "Steganography Based on Human Perception." *Oriental Journal of Computer Science and Technology* 10.4 (2017): 817-823.

[18] Ramya, G., P. P. Janarthanan, and D. Mohanapriya. "Steganography based data hiding for security applications." *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*. IEEE, 2018.

[19] Kumar B, Manoj, Gopi Sailesh C, and Ravi Kumar CV. "Secure Data Communication With Cryptography and Steganography." *International Journal of Electrical Engineering and Technology* 11.3 (2020).

[20] Jamra, Resty Kurnia, et al. "Systematic Review of Issues and Solutions for Security in E-commerce." *2020 International Conference on Electrical Engineering and Informatics (ICELTICs)*. IEEE, 2020.

[21] Pelosi, Michael, and Chuck Easttom. "Identification of LSB image Steganography using Cover Image Comparisons." *Journal of Digital Forensics, Security and Law* 15.2 (2021): 6.