THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-35-December-2019

Analytical Study On Security Issues In Steganography

Sabyasachi Pramanik

Research Scholar of Sri Satya Sai University

Dr. S. Suresh Raja

Research Supervisor

ABSTRACT

Information or data is vital asset to us. Steganography is the specialty of secured, or hidden, writing. The reason for steganography is undercover communication to hide the presence of a message from a third party. This proposed framework manages executing security-utilizing Steganography. The mediums are typically images, video, audio and so forth., wherein explicit bits or the general space is normally 'corrupted' with 'significant' data. In this technology, the end user recognizes an image which is going to go about as the bearer of data. The data file is encrypted and authenticated. This message is hidden in the image. The image whenever hacked or translated by a third party user will open up in any image previewer yet not showing the data. This shields the data from being imperceptible and consequently be secure during transmission. The user in the less than desirable end utilizes another bit of code to retrieve the data from the image.

Keyword: Steganography, Cryptography, Privacy, Security, Authentication

INTRODUCTION

Data or information is extremely significant to any association or any distinct individual. None of us prefers our discussion being caught as it contains the capability of being abused. Security and authentication techniques like computerized watermarks; stenographic strategies and other data installing calculations have contributed a lot to improve the different security highlights and to save the protected innovation. In this regard, stenographic techniques have been the best in supporting stowing away of basic information in manners that forestall the recognition of hidden messages. Steganography is commonly progressively favored media in view of its innocuousness and fascination.

While cryptography scrambles the message with the goal that it can't be comprehended, steganography hides the data so it can't be watched. Various kinds of steganographic techniques utilize color composition, luminance, surprising arranging of color palettes, misrepresented noise, and connection between colors lists and so on. The fundamental goals of the security or steganographic calculations ought to be, for example, to give classification, data integrity and authentication.

ISSN:0971-1260
Vol-22- Issue-35-December-2019

The significant downsides of steganography are that one can hide next to no information in the media chose. A few techniques are following

- Encoding secret message in text/documents
- Encoding secret message in audio
- Encoding secret message in images

TYPES OF STEGANOGRAPHY

Steganography might be delegated pure, symmetric and asymmetric while pure steganography needn't bother with any trade of information, symmetric and asymmetric need to trade of keys earlier sending the messages. Steganography is profoundly subject to the kind of media being utilized to hide the information. Medium being commonly utilized incorporate text, images, audio files, and network conventions utilized in network transmissions.

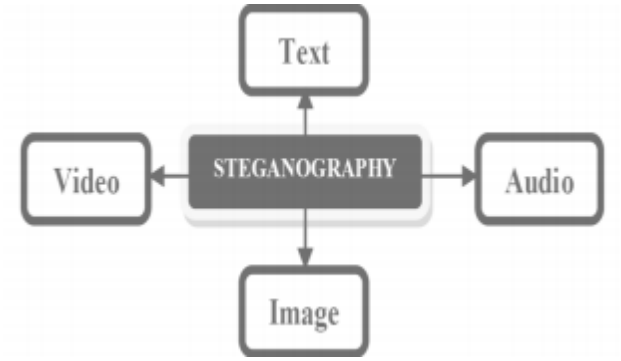


Figure 1: Types of Steganography

LITERATURE REVIEW

Richa Gupta, Sunny Gupta, Anuradha Singhal (2014) Information or data is exceptionally essential asset to us. Along these lines securing the information turns into even more fundamental. The communication media through which we send data doesn't give data security, so different strategies for securing data are required. Information concealing assumes an extremely urgent job today. It gave strategies to encrypting the information with the goal that it gets unreadable for any unintended user. This paper audits the techniques that exist for data covering up and by what means can these be joined to give another degree of security.

Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar (2014) In numerous associations like FBI and RAW offer private and significant data on any network. Hackers are consistently in sit tight for it. They hack the data and use it for their advantage. These people groups attempt to utilize these data to hurt somebody, they deal these significant data to adversary nations. In either case, message sender or

ISSN:0971-1260
Vol-22- Issue-35-December-2019

collector needs to address the cost. To shield from these unfortunate demonstrations, we can utilize Steganography and cryptography together to guarantee security of the message. One of the most effective and secure calculations is RSA Algorithm for changing over text message to figure text. Steganography is the craftsmanship and study of writing hidden messages so that nobody separated from the sender and planned beneficiary even acknowledges there is a hidden message and Cryptography is a component to change over message or data in non readable structure.

RonakDoshi, Pratik Jain, Lalit Gupta (2012) Steganography is a strategy for secretively communicating. Steganography is a procedure that includes concealing a message in a proper transporter for instance an image or an audio file. The bearer would then be able to be sent to a collector without any other individual realizing that it contains a hidden message. This is a procedure, which can be utilized for instance by social liberties associations in oppressive states to communicate their message to the outside world without their very own administration monitoring it Steganalysis is a recently developing part of data preparing that looks for the recognizable proof of steganographic covers, and if conceivable message extraction. It is like cryptanalysis in cryptography. The technique is antiquated developing beast that has increased changeless notification as it have recently entered the universe of computerized communication security. Objective isn't just to forestall the message being read yet additionally to hide its reality.

RupaliGawade, PriyankaShetye, VaibhaviBhosale, P N. Sawantdesai (2014) Steganography is characterized as the workmanship and study of concealing information, which is a procedure that includes concealing a message in a proper bearer for instance an image file or IP Header. The transporter would then be able to be sent to a collector without any other individual realizing that it contains a hidden message. In this venture we present a plan to send message indistinctly between focuses over Internet utilizing any encryption calculation which is utilized to encrypt mystery message, and afterward installs the balanced message into recognizable proof field of IP header. This proposition examines the presence of clandestine directs in PC networks by investigating the vehicle and the Internet layers of the TCP/IP convention suite. Two methodologies for data covering up are distinguished: parcel header control and bundle arranging. The bundle arranging approach is reenacted at the network layer which gives a plausibility of parcel arranging under differing network conditions.

Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara (2016) In spite of the fact that cryptography and steganography could be utilized to give data security; every one of them has an issue. Cryptography issue is that, the figure text looks trivial, so the aggressor will intrude on the transmission or make increasingly cautious minds the data from the sender to the beneficiary. Steganography issue is that once the nearness of hidden information is uncovered or even suspected, the message is gotten known.

ISSN:0971-1260
Vol-22- Issue-35-December-2019

As per the work in this paper, a blended technique for data security has been proposed utilizing Cryptography and Steganography techniques to improve the security of the information. Right off the bat, the Advanced Encryption Standard (AES) calculation has been changed and used to encrypt the mystery message. Besides, the encrypted message has been hidden utilizing strategy. In this manner, two degrees of security have been given utilizing the proposed cross breed technique. Furthermore, the proposed technique gives high embedding capacity and excellent stego images.

PROPOSED SYSTEM

The algorithm present in the current framework was fairly entangled. In cryptography, the importance of data has been changed. Along these lines, it makes goal to the hacker to hack or devastate the data. In our proposed framework, we executing another technology called steganography for data security, it change the importance of data as well as hides the nearness of data from the hackers. The fundamental target of this framework is concealing enormous measure of encrypted and authenticated data regardless of the size, measurements of the image and without upsetting the lucidity of the image.

ENCRYPTION

In the encryption procedure from the message every single printable character involves 7 bits and the last piece esteem is 0. In the initial step I am taking 8 characters one after another from the data file and the last character 7bits are changed in accordance with its past 7 characters and these 7 characters are kept up independently in another file. Like that each 8 characters are changed over in to 7 characters and all these encrypted characters are kept up independently in another file (say encr1). After that by utilizing an arbitrary capacity we create a 4 piece polynomial. Take 4 characters from the encrypted file and by utilizing this polynomial perform modulo-2 division activity on these 4 characters then we will get a rest of 3bits. In the second step of encryption these 4 characters, polynomial and the rest of balanced in 5 bytes. These five bytes are kept up independently in another file (say encr2). Like for each 4 characters of first encrypted file subsequent to performing modulo-2 division activity, 5 bytes are kept up in the file encr2.

A. Data embed

This method manages distinguishing the (encrypted data) figure text with key (encr2) and the image to install the data before it very well may be transmitted. Open the given image files in the binary mode and locate the size of the first image. This size is kept up in the image itself by utilizing a unique mark which is helpful to retrieve the data from the image. Presently include figure text from the file encrc2.cmp to the image. Presently the image is ready to transmit. In the event that the image already

ISSN:0971-1260
Vol-22- Issue-35-December-2019

contains a few data you can't include some more data for a similar image. So before embedding data check whether the image contains data or not.

B. Data retrieve

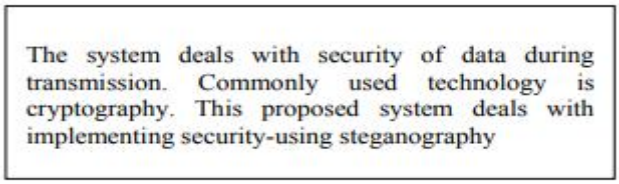
Subsequent to getting the image through certain media, the end user additionally opens the image in the binary mode and checks whether the image contains the extraordinary mark or not. On the off chance that mark discovered, at that point image contains data. At that point get the first size of the image from that mark. Presently with the exception of unique data of the image separate data from the image up to the uncommon mark. This is encrypted data (figure text). This data is kept up in a file say decypt2. For this data check authentication whether data is corrupted or not and afterward unscramble the data to get the first message. Take five characters from the retrieved data file (decypt2.) and distinguish the key from the fifth character and by utilizing this key perform modulo 2 divisions on these five characters. On the off chance that the rest of zero, at that point there is no corruption in the data generally data is corrupted. On the off chance that the data isn't corrupted, at that point expel key and leftover portion from the five characters and organize the bits in 4 bytes to get the encrypted data. These 4 bytes are kept up independently in an uncommon file say dect1. Like that for each 5 bytes from decypt1. Subsequent to evacuating key and leftover portion the 4bytes are kept up in the file dect1.cmp.This is the encrypted file without key.

C. Decryption

Take 7 bytes from the encrypted file decypt1. what's more, unscramble these bytes so that take last bit from these 7 bytes and orchestrate them in another byte. Make the last bit estimation of these 7 bytes just as the new byte as 0. Presently keep up these 8 bytes in unique file say data1. This is the unscrambled data. Like that for each 7 bytes from the encrypted file structure 8 bytes and keep up these bytes in the file data1. This file contains the original data.

SAMPLE TEST RESULTS

A. Encoding: Sample – 1 (image pc1.jpeg)



Plain text (175 bytes)

ISSN:0971-1260
Vol-22- Issue-35-December-2019

Thå óùóåí dåái wéth óãõòétù f
äatá uòinç ôánsíióóïn® Cïïïniy õóä ôåcèîlogy
éscòypõïçaphù. Ôéó ðrïðseä óùóåí
dåái wéôh éðleíeîônç sâãõiôù-uóég óôeçáography

Encrypted data (156 bytes)

y+B£O/ŸÏŸ +!lK½g
MC§M —¯›}Ë§LK! 3K-
§O;sO•Kw¥ ›Okš}sw Ÿ oz{Ïcw}O'Ÿ©K/¥
K{gwE IË={Ï"™O? £ OËC*ƒ* N¥t{—
…žK+Ÿ‡~OÏ™!Io/ g+" §K½O‡ME{/k+c ;w§
uO+™ Ï£O¬ O›-o § >K ;.{*ƒ*
":IËF

Encrypted data with key(195 bytes)

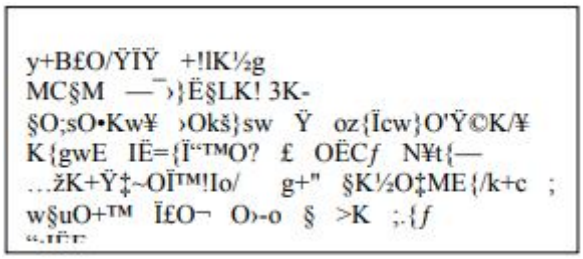
Figure 2: Actual image (pc1.jpeg) 160 × 120

B. Decoding

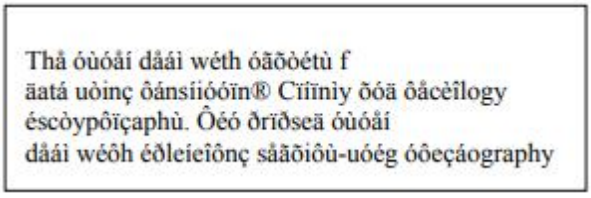
Retrieved data from the image pc1.jpeg

Figure 3: Stego image (pc1.jpeg) 160 × 120

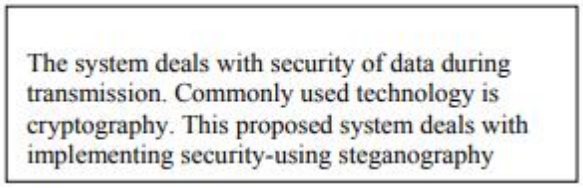
ISSN:0971-1260
Vol-22- Issue-35-December-2019



Retrieved data from stego image(195 bytes)



Authenticated data (encrypted data) (156 bytes)



Decrypted data (175 bytes)

RESULTS ANALYSIS

We have tested our method for various arrangements of images just as messages. For every single ordinary jpeg and the bmp images the proposed method is working fine. The analysis for various data is appeared in the beneath table1.

TABLE 1: Stego Image Size

Image Size (bytes) IS	Data size (bytes)	After encryption Size (bytes)	Encrypted data with key (bytes) ES	Stego image size (bytes) IS+ES+10	Data retrieved from stegoimage (After decryption) (bytes)
4,608	1	4	5	4,623	4
4,608	2	4	5	4,623	4
4,608	3	4	5	4,623	4
4,608	4	4	5	4,623	4

CONCLUSIONS

Steganography is an intriguing and successful method of concealing data that has been utilized since forever. Methods that can be utilized to reveal such naughty strategies, yet the initial step are mindfulness that such methods even exist. There are

ISSN:0971-1260
Vol-22- Issue-35-December-2019

numerous valid justifications too to utilize this sort of data stowing away, including watermarking or an increasingly secure focal stockpiling method for such things as passwords, or key procedures. In any case, the technology is anything but difficult to utilize and hard to identify. The more that you think about its highlights and usefulness, the more ahead you will be in the game.

In this framework the planned tool manages giving simple and secure information. The data is encrypted with key and embedded with an Image which is ready to send through communication channels. It will be solid and secure. At the less than desirable end, the tool checks the accessibility of data and authenticates the data. It retrieves data from the stego image and decrypts it. This bundle contains two sessions. The main sessions manages Embedding, Retrieving and Authentication of data. The subsequent sessions give the utilities to encryption and decryption of data.

REFERENCES

[1] Richa Gupta, Sunny Gupta, Anuradha Singhal (2014), 'Importance and Techniques of Information Hiding : A Review', International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 5– Mar 2014

[2] Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar (2014), 'Enhance Security in Steganography with cryptography', International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014

[3]RonakDoshi, Pratik Jain, Lalit Gupta (2012), 'Steganography and Its Applications in Security', International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638

[4]RupaliGawade, PriyankaShetye, VaibhaviBhosale, P N. Sawantdesai (2014), 'Data Hiding Using Steganography For Network Security', International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

[5]Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara (2016), 'Data Security Using Cryptography and Steganography Techniques', (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016

[6] Xuping Huang, Ryota Kawashima, NorihisaSegawa, Yoshihiko Abe. ―The Real-Time Steganograph Based on Audio-o-Audio Data Bit Stream‖,Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[7] Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287.

ISSN:0971-1260
Vol-22- Issue-35-December-2019

[8] EktaDagar, Sunny Dagar Comparative Study of Various Steganography Techniques International Journal of Emerging Engineering Research and Technology Volume. 2, Issue 2, May 2014,

[9] Latika, YogitaGulati A Comparative Study and Literature Review of Image Steganography Techniques IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015

[10] Steganography Techniques - Data Security Using Audio and Video HilalAlmara'beh International Journal of Advanced Research in Computer Science and Software Engineering, volume 6, Issue 2, February 2016 ISSN: 2277 128X