International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5841-5844

Comprehensive Survey on Image Stegnography Using LSB With AES

In-depth study of various requirements in the process of embedding, encrypting and extracting of text data

Amit Kumar Agrahari[1], Mayank Sheth[2], N. Praveen[3]

[1]Undergraduate Student, Computer Science Engineering, SRM Institute of Science and Technology
[2]Undergraduate Student, Computer Science Engineering, SRM Institute of Science and Technology
[3] Asst. Professor (S G), Computer Science Engineering, SRM Institute of Science and Technology

Abstract

With fast development in the computerized advertise, Steganography will build its significance by which the exponential improvement and private correspondence of potential PC clients are moreover expanded over the web. It can likewise be very much characterized as the investigation of unknown undetectable correspondence, that for the most part manages the diverse methods for hiding the presence of the conveyed message. More often than not, the information installing is gotten in correspondence, for example, picture, content, voice or mixed media content for copyright and furthermore in military correspondence for validation furthermore, numerous other diverse purposes. In picture Steganography, the unknown concealed correspondence is acquired through insert a message into a cover picture which is utilized as the medium to implant message into the picture and produce a stego picture which is a created picture which is conveying a mystery concealed message. In this paper we propose a way to conceal unknown data in mix of AES and LSB system. The picture quality are chosen by the clients and in light of that the mystery messages length are chosen. Consequently client has full appropriate to choose any size yield in light of necessities.

Keywords-Image Steganography; Cover Image; AES Cryptography; Least Significant Bit(LSB)

INTRODUCTION

In the web Technology, Security is turning into a major issue for the world because of the quick development of web clients step by step. In the event that a web client needed to impart his own data to other web client by utilizing the social applications, at that point programmers can assaulted on these social applications and they can hack all the individual data about the web client. In this way to shield all the individual data from an unapproved individual we require security components.

"Steganography" is a Greek word which signifies "concealing composition". Steganography word is the mix of two sections: Steganos which signifies "protected" and Graphic which signifies "script". Steganography is a security component of concealing touchy data among the bits of a cover record, for example, a picture, content, a sound record and video document such that exclusive sender and recipient think about the shrouded message inside the cover document.

Cryptography originates from a Greek word importance covered up or mystery composing for secure Communication in the nearness of an unapproved individual. Cryptography incorporates encryption and unscrambling procedure of a message. Cryptography is the specialty of ensuring delicate data by encoding it into an incomprehensible arrangement called encoded Text .The individual who has a mystery key can decode the message in to Plain content. In any case, the transmission of encoded message isn't sheltered so the scrambled message may effectively excite aggressor's doubt what's more, might be blocked or assaulted effectively. At some point steganography won't cover the aggregate security of mystery knead. So an extra security need to the mystery knead. So AES framework is employed with Steganographic framework.

STEGANOGRAPHY

Concealing the data in some other host protest is called Steganography. It has been utilized since antiquated time by the general population. In old time, data is placed at back of the wax, the scalp of the slaves, in rabbits, and so forth. With progressing of time, the utilization of steganography and its region has progressed toward becoming extended. With the present digitization period, digital steganography has risen as the new device to shroud the data subtly. Script, advanced picture, digital sound and computerized video have turned into the host protest for information covering up.

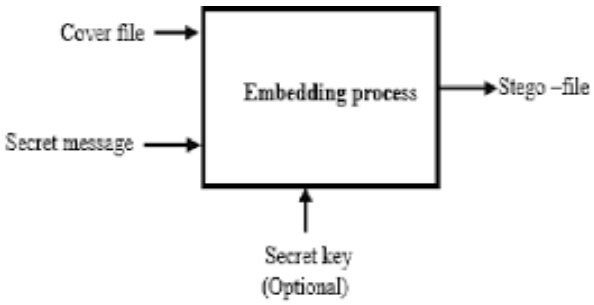

Figure 1: Steganography Model

The following are a portion of the regular term which is important to see any steganography framework:-

- Stego-Key: An optional key utilized in inserting or extricating data from cover and stego-pictures.
- Message: Data utilized for stowing away inside pictures. Message can be a normal content or some picture.

- Cover-Image: Picture which is utilized as a means for concealed data.
- Stego-Image: Cover picture having concealed message.

TYPES OF STEGANOGRAPHY

Different kinds of steganography include:

a) Image Steganography:

The technique for concealing mystery data in an image such that there won't be any changes is called as image steganography. Customary picture steganography method is LSB.

b) Audio Steganography:

The technique for concealing mystery data in a sound is known as sound steganography. There are different strategies for concealing mystery information in a sound, for example, LSB, Phase Coding and so on.

c) Video Steganography:

The strategy for concealing mystery data inside video is called as video steganography. It contains pictures and sound. Consequently, the two pictures and sound steganography can be utilized for this steganography.

d) Text documents Steganography:

The strategy for concealing mystery data inside Text is called Text steganography. This uses less storage for Text documents, so it is easier for exchanging between PCs. Text steganography isn't normally utilized as content records containing huge measure of excess information.

e) Network Steganography:

When taking a cover protest as Network convention, for example, TCP, IP, etc. where convention is utilized as bearer, is known as Network steganography. TCP/IP fields consists of header bits that can be utilized for this steganography.

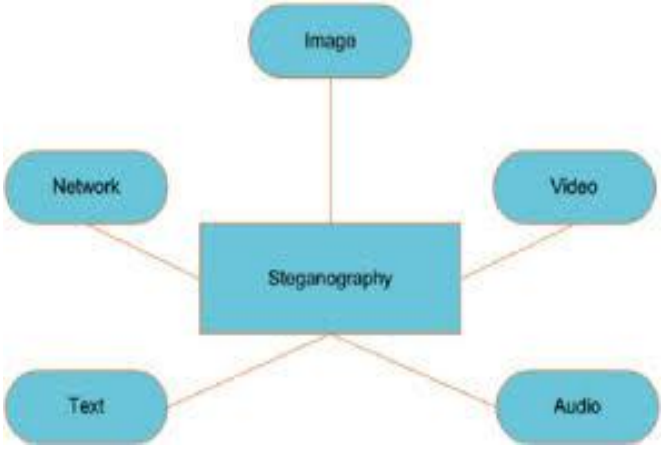

Figure 2: Types of Steganography

TECHNIQUES OF STEGANOGRAPHY

Spatial Domain Methods: - Changing the bits value of a pixel in an image for enforcing data hiding can be used in spatial steganography. To conceals mystery information inside the pixel without presenting numerous recognizable bends Least Significant Bit Technique is used.

Least Significant Bit (LSB):-

Suppose we want to hide the data inside an image, so for that we will replace the bits value of the pixel with our secret code data bits value. This is known as Least Significant Bit where last bit of the pixel value is replaced. To hide the data minimum of 8 bit of an image is required. This can be suited for both color and grey scale image as well. There are many variations in it such that LSB-1, LSB-2, Random-LSB and so on depending upon the pixel selection for data hiding as well as number of bits selected.

Transform Domain Technique: - To concealing information in a picture, this method is much more perplexing. Different systems and change are utilized on the picture to conceal information in it. Transform Domain Technique can be named as an area of embedding systems for which various methods have been proposed. The way toward embedding information in the frequency domain of a signal is considerably more grounded than embedding rules that work in the time domain. A large portion of the capable steganographic frameworks today work in Transform Domain. This strategy is having favorable position over other systems because data is concealed where picture is less presented for compression and cutting. A few methods of Transform Domain don't appear to be reliant on the picture configuration and they may surpass lossless and lossy arrangement transformations.

Distortion Techniques: - In this technique the encoding is done by adding a grouping of replaces in the picture to hide the data by replacing the information. The encoded image is resulted in rough or distorted image. To get back the native image, decoding is done and amid the deciphering procedure contrasting between native and deform image is resulting the capacity of Decoder.

Masking and Filtering: - It is like a method where data is shrouded in the picture like same as watermarking is done. The strategies of watermarking can be connected without the dread of picture loss because of lossy compression as they are more incorporated into the picture. It is done for the sensitive data.

CRYPTOGRAPHY

Concealing the data in such a manner so that a pass key is required to access it is called Cryptography. This is done by hiding the data using some password or key to convert it into encoded text. After that this encoded text is decoded using the same password or key to get back the data. In case if you don't know the key, it's not possible for anyone to recover the data or plaintext. Cryptography assumes a basic part in numerous administrations, as: privacy, key trade, validation and non-

revocation. Cryptography gives these administrations for secure correspondence crosswise over unreliable channels.

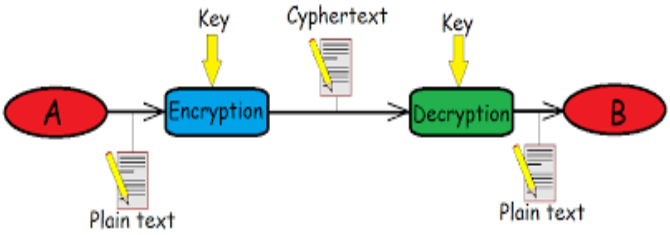

Figure 3: Cryptography Model

Open key cryptography employs 2 distinctive keys open key, and private key. This is a property which set this conspire not quite the same as symmetric encryption. On the off chance that encryption is done employing sender's open key then decoding ought to be done utilizing beneficiary's private key and the other way around. Open key cryptography calculation that is being used today for a key trade/advanced mark incorporate RSA, Diffie-Hellman, DSA, ElGamal, ECC and so on.

Hash work additionally called message process and 1-way scramble are calculated that employs no key. A settled length hash esteem is registered in view of the plain content that makes it outlandish for either substance or length of plain content to be recouped. Hash Technique are employed to give advanced unique mark of a documents files. Illustrations incorporates MD, SHA, RIPEMD, Tiger and so forth.

IMAGE STEGANOGRAPHY USING LSB WITH AES BY DIFFERENT METHODS

V. Dhaka, A. Dhamija [1] proposed a method by joining cryptography and steganography to shroud the information. In the cryptography procedure, they proposed a viable system for information encryption utilizing one's supplement strategy, that they called as SC-MACS. It utilized symmetric key strategy in which sender and recipient having a similar key for encoding and decoding. LSB strategy is employed for steganography.

Nouf A. Al-Otaibi et al. [2] outlined another framework called 2-layer security framework for concealing the touchy data on PCs. They separate the framework in two layer in particular cryptography layer and steganography layer. For steganography layer LSB calculation is utilized and for cryptography layer AES calculation is used. This framework is outlined on visual essential stage. Nouf A. Al-Otaibi et al have likewise done examination on enhancing concealed limit by directed a few tests. They utilize 1 to 2 bits of LSB to insert mystery message in cover picture. 30 distinct sorts of fixed size pictures are utilized as a part of their examination to investigate the information reliance and security of this technique. They reason that impact of 1LSB and 2LSB is insignificant in stego picture however with 3LSB, 4LSB, 5LSB, 6LSB and 7LSB the picture is mutilated to noticeable levels and have low nature of stego picture which isn't perfect for picture steganography.

M. R. Islam et al. [3] proposed another enhanced variant of LSB picture steganography in view of productive filtering strategy utilizing status bit. For another layer of security AES encoding is used. Now for LSB steganography, Bitmap image is used because of its uncompressed nature. In this strategy first mystery information is encoded and this encoded information is implanted into picture utilizing steganographic process. Enhanced version of steganographic technique is proposed where more mystery data can be used. filter is done with the help ofbased calculation and for the filtering reason MSB of bitmap picture is used. Proposed work likewise makes utilization of status bit for checking inclusion and extraction of mystery messages. Test shows that this strategy has high inserting limit than essential LSB calculation. PSNR esteems are likewise high as a result of high stego picture quality. All the test comes about demonstrate that this strategy is more proficient than customary LSB technique for concealing the information in bitmap pictures.

Vijaya Lakshmi Paruchuri, Dr. R. Sridevi, K. S Sadasiva Rao [4] proposed the paper where Least Significant bit procedure is applied for hiding data inside an image. The AES is used for better security.

Mihir H Rajyaguru [5] proposed research paper in which client enters information like secret key and username. A programmed key generator gadget produces an interesting key after some time. Now this key and mystery message is encoded such that encoded message is created and implanted into cover picture to generate stego picture.

M.V. Khandare, M.S Sutaone [6], research paper exhibits a strategy for encoding and decoding a secret document which inserts into picture record, utilizing arbitrary LSB addition strategy where information are stored into picture bit by bit haphazardly. A key is employed for creating these arbitrary numbers.

Sumod Tom Philip, Shery Elizabeth Thomas, Sumaya Nazar, Niya Joseph, Ashams Mathew [7], information can be covered up in any sound, video or picture that gives greater security. SHA-1 hashing is used for key and secret information is first encoded utilizing AES so that attacker is not able to attack it easily. figure information in picture, video or sound is utilizing Least Significant Bit method. Similar key is used by recipient that is used in hashing.

CONCLUSION

The paper shows an extensive audit of the conventional methodologies and strategies employed as security of transmitted information over the information Network has been given. The study has been done identified with cryptography and steganography that guarantees security however needs some alternate way so that it proves security standards. It also shows various strategy employed for the least significant bit depending upon the efficiency as well as encryption standards used.

REFERENCES

[1] Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICG-CIoT), 2015 International Conference on. IEEE, 2015, pp. 346-351.

[2] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV),May 2014, pp. 1-6.

[3] N. A. Al-Otaibi, and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, June 2014, pp. 151-157.

[4] R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, ISSN: 22773061, Vol.9, July 2013, pp. 976- 984.

[5] Mihir H Rajyaguru, "Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.

[6] M.S Sutaone., M.V. Khandare, "Image Based Steganography using LSB Insertion Technique", IEEE Xplore, Jan 2008, pp. 146-151.

[7] Shery Elizabeth Thomas, Sumod Tom Philip, Sumaya Nazar, Ashams Mathew, Niya Joseph, "Advanced Cryptographic Steganography using Multimedia Files", International Conference on Electrical Engineering and Computer Science (ICEECS), May 2012, pp. 239-242.

[8] Islam, Rashedul & Siddika, Ayasha & Uddin, Md. Palash & Kumar Mandal, Ashish & Delowar Hossain, Md. (2014)." An Efficient Filtering Based Approach Improving LSB Image Steganography using Status bit along with AES Cryptography" 2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014. . 10.1109/ICIEV.2014.6850714.

[9] Hussain, Mehdi. (2013). "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology. (IJAST),. 54. 113-125.

[10] Beenish Siddiqui, Sudhir Goswami, "A SURVEY ON IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION TECHNIQUE", International Research Journal of Engineering and Technology (IRJET), Vol. 4, ISSUE 5 MAY 2017.

[11] NutanManwade,SwatiNigam "LSB Image Steganography with DES Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 7, July 2015.

[12] Divyanshu Tripathi , Yash Kumar Singh , Rohit Singh. "A Survey on Image Steganography With its Related Techniques and its Types", IJSART – Volume 2 Issue 4–APRIL 2016.

[13] Md. Khalid Imam Rahmani, Kamiya Arora , Naina Pal "A Crypto-Steganography: A Survey", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014.

[14] Aishwarya Pandey,Jharna Chopra "Steganography Using AES and LSB Techniques", International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 6, Issue 6, June 2017.