ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Image Steganography Techniques in Security

Swati P. Mane [1], Bharati Kale [2]

ME Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

ABSTRACT: Steganography is the technique of hiding secret messages into image, audio, video or text files. The steganography can conceal plain data as well as encrypted data. Hiding more secret data into images and increasing PSNR value are these two major issues having in steganography. Some ethical hackers or third party members access the secret data so security is also a major issue. To solve these issues many users use various algorithms and technique. Some users created new approach by combining two or more algorithms. The algorithms like OutGuess, JSteg, Parity coding, 4LSB, Phase Coding are used for steganography. New algorithms are created by using LSB, MSB methods. In this paper we propose the survey of steganography techniques, algorithms used in communication and security.

KEYWORDS: Steganography, LSB, MSB, Parity coding, Phase coding, 4LSB, OutGuess, Jsteg, LaTEsteg.

I. INTRODUCTION

The data security is major concern in today's world. There are different data securities techniques are used such as cryptography, steganography etc. Most of the organizations, governments, military, business, private citizens use steganography for security purpose. Steganography is the technique of hiding the data into some other data. So if we are transferring data by using steganography techniques it would becomes difficult to know the third party user that the secret data is concealed in the appearing image or data. The music and movie industries use steganography for remarking early distribution of screenings movie, the internet becomes prime factor for communication and recently cyber crime increases exponentially so to avoid such computer forensic techniques are used [1]. Many of the steganography algorithms takes original image as cover image, which is expense of embedding secrete messages into cover image that leads to the image distortion of generated stego image [2]. Hiding a message inside another median and then again hide it another median increases some complexity and make more deceptive to third party and it enhances the protection level of original data [3]. The performance of steganographic technique is needed to improve the level of protection of data which leads to us to develop new algorithms with strong security, capability and imperceptibility [4]. The most popular object of the steganography are images, there are two groups having of image steganography techniques are divided first spatial domain and second transform domain [5]. It's very important thing to select suitable cover image that stores the secrete message. The cover image should not present on websites because intruders can easily compare the generated stego image and cover image [6]. The digital image is group of data about pixels. The images are large as compare to messages which is hidden therefore we always prefer digital image as cover medium for secrete information send [7]. The steganography can be applied on different media such as image, text, and audio, video we called it as a cover objects. The audio steganography hides the secrete message inside an audio signal. The message is concealed by slightly changing the binary sequence of sound file [8]. Long term evaluation has very popular technique in wireless networking and this offered cellular system transmission like high video transmission or video on demand. Growing with such popularity Long Term Transmission becomes perfect carrier for steganography [9]. In digital scenario to happen communication in secure manner common technique is used that is cryptography. The method used above the cryptography for secure information transmission is the steganography [10].

As shown in (Fig 1) the steganography technique takes original image and secret data as input. Steganography technique hides the secret data behind the image and it produce the stego image as output. The generated stego image is given as input to desteganography. Desteganography generates the original data. This process happen between two users steganography done at sender side and desteganography done at receiver side.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

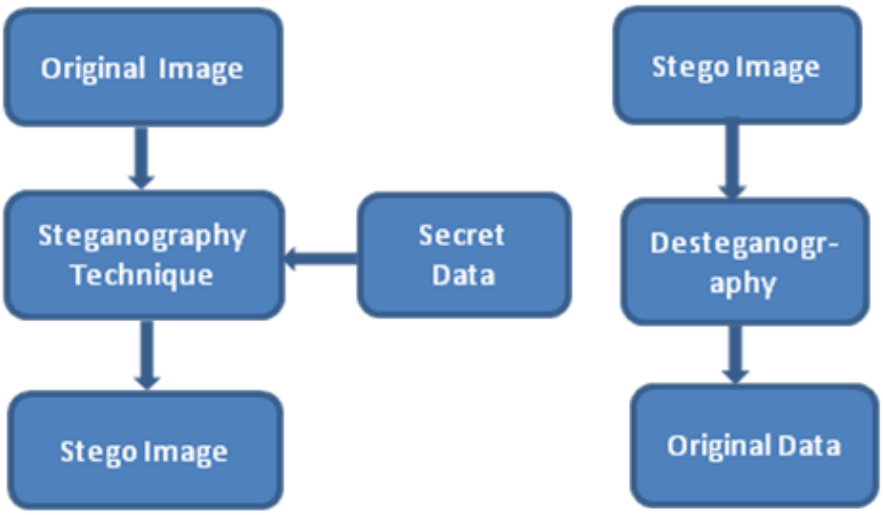

Fig. a Fig. b

Fig. 1. Architecture for Image Steganography

II. SURVEY

In [1] authors used the method audio-video cryptosteganography. This method is the mixture of audio and image steganography. This steganography is done by using anti forensics technique as tool for authentication. The objective of this technique is to hide secret information behind the audio and video file. 4least significant method is used for video steganography and phase coding for audio steganography. The data is triple secured with this technique. It provides strong security and privacy of data by using computer forensics technique. In [2] authors developed the new approach for steganography using a reversible texture synthesis. By giving original texture as input the reversible texture synthesis generate huge stego synthetic texture concealing secret message. As per the authors knowledge they are the first that can elegantly intertwine the steganography into conservative patch based texture synthesis. The newly proposed approach provides reversibility to retrieve the original source texture from stego synthetic texture by making possible second round of texture synthesis if required. The benefit of offered algorithm is stout and safe against RS steganalysis attack. The disadvantage of this approach is does not support for other kind of texture synthesis. There are so many algorithms are available for steganography with their benefits and disadvantages. The user has the responsibility to select the appropriate algorithm based on their idea. By combining two or more algorithms the security level is increased. In [3] authors combined the two steganography algorithms JSteg and OutGuess. First the secret message is hidden in original image by using JSteg algorithm and the generated stego image is concealed inside second image by using OutGuess algorithm. This increases the level of security by hiding original hidden image. The benefit of it becomes difficult to third party to suspect conceal of secret image and even makes difficult to decode it. The disadvantage of it is becomes more complex when two algorithms combined. In [4] authors advanced MSB steganography method with random pixel selection. This algorithm embeds a large amount of secret data inside color image. This proposed algorithm is based on different size image segmentations (DSIS) algorithm and modified least significant bits (MLSB) algorithm. The DSIS algorithm is applied to conceal secret image randomly rather than serially. The DSIS approach is applied before of hiding secret data. The benefit of this algorithm is working on timid channel and against attack by generating undetectable stego image for both low and high payload. In [5] authors advanced the LSB steganography technique by using parity checker. In this method all the pixels of cover image can be used but secret data bits are stored in LSB of three color components Red (R), Green (G) and Blue (B). The data is embedded based on parity of three LSBs of R, G, and B mechanism of 24 bit color image. The advantage of this method is to hide large amount of secret data and make it difficult to access unauthorized user. In [6] authors proposed steganography method based on similarity technique. This technique divides the cover image into different blocks and these blocks are tested that can be obtain blocks that are most closely resembling message. Then in every block locate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

two channels that provide the maximum resemblance to a secret message and consider left over channel as indicator. So the indicator may be dissimilar in every block. The indicator is represented one bit if there is no concealed data in extracted pixels of block. This method provides high level of protection because data is not stored serially and it based on similarity standard so it provides high quality stego image. In [7] authors used pixel pattern based steganography. This method conceals the secret data inside an image by using existing RGB values. Along with image key will also send to decrypt the message at receiver side. To provide more security the secret message and key both are encrypted by using same or different keys. The benefit of it as it can be easily shared by any method. In [8] authors used different steganographic techniques such as LSB, parity coding and phase coding for audio steganography. It hides the digital data in audio file. Here in this multi level steganography the three messages can be send rather than one message. It increases the level of difficulty to decode the message by using three traditional methods. In [9] authors used steganography in long term evolution systems. The LaTEsteg method is designed for long term evolution systems. This method is evaluated on three parameters performance, cost and security. This method uses physical layer padding of packets which is sent over LTE networks. The advantage of LaTEsteg method is that it does not produce any changes to the LTE system. In [10] authors used steganography in spatial domain based on security and randomization. Spatial domain image steganography is having well-suited with image so it is used for this work. The least significant bit steganography is included in this method. So it LSB bit uses to conceal the data in images. The benefit of this method is it has a great capacity of concealment of data and easy realization.

III. PERFORMACE REVIEW

Performance analysis shows the behaviour and performance of each algorithm. We have done performance review of the different algorithms used in survey section of this paper. The below table includes Paper Reference Number, Algorithms or techniques, Parameters achievement and Working & Use of algorithms. The table is created after analysis of paper results and algorithms. Table (1) contains algorithm which is used in that specific paper and parameter achievements and working and use of that specific algorithm. This table gives the easy way of consider performance of algorithms used by developers.

RP No.	Algorithms	Parameters Achievement	Working And Use
1.	Anti Forensics, 4LSB & Phase coding algorithm	1.Better capacity 2.High Security 3.Prevent visual attack	1.Hiding text data into audio & video file 2.Strong Authentication
2.	Reversible Texture Synthesis	1.Prevent RS steganalysis attack 2.Security	1.Conceal source texture image and embeds secret messages
3.	Combined Approach: JSteg, OutGuess	1.High Security 2.PSNR value more than 50db	1.Secret image is first hidden in an image and then the resultant stego image is further hidden in another image 2.Tricky & deceptive to third party
4.	MLSB,DSIS,AES	1.High payload capacity 2.Prevents attack	1.Hides secret image randomly instead of serially 2.Highly imperceptible
5.	LSB, Even Odd Parity	1.Robust 2.High Reliability	1.Message bits are stored in LSB one of three colour components(RGB) 2.Increase size of message to embed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

6.	Modified LSB, Indicator Method	1.High quality stego image 2.High embedding capacity	1.Dividing bmp image into blocks & obtain a block which is closely resembling to a secret message 2.It embeds five bits in each pixel
7.	Pixel pattern	1.Secret data encrypted with key 2.Confidentiality	1.Secret message bit embedded in image metadata fields 2.Small secret messages are transferred
8.	Layering approach: LSB, Parity coding, Phase coding	1.High confidentiality 2.Consistency clarity in audio signal	1.Three secret messages can be transferred 2.Hides presence of communication
9.	LaTEsteg method	1.High throughput 2.Low cost	1.Does not generate changes to LTE system 2.Safe & effective hidden transmission
10.	MSB randomization	1.High capacity 2.Secure 3.Imperceptability	1.MSB of the randomly selected pixel used as indicator 2.Compatible with images

Table 1. Performance Review Table for Different Algorithms

IV. CONCLUSION AND FUTURE WORK

Steganography use different approaches to secure the communication. Many developers combine different algorithms or modify the original algorithm to generate a new algorithm. The newly generated algorithms come up with more benefits. In this paper we do the survey of different previous papers. Many developers used the LSB, MSB, Parity Coding Phase Coding and 4LSB steganography techniques to hide the secret data. Finally we conclude that data hiding in audio-video steganalysis by anti forensics technique is the best technique to hide the secret messages. The data is triple secured with this technique and it provides strong authentication. The drawback of this technique is its time complexity is more as compared to other techniques. In future work we have doing a survey of the more steganography technique and develop a new stronger, secure and easy algorithm for hiding secret information.

REFERENCES

1. Qingzhong Liu, Andrew H. Sung,Mengue Qiao, "Secure Data Hiding in Audio-Video Data Steganalysis by Anti Forensics Technique", IEEE Transactions On Information Forensics and Security, Vol.4 No.3 July 2015.
2. Kuo-Chen Wu and Chung-Ming Wang, *Member, IEEE* , "Steganography Using Reversible Texture Synthesis", Ieee Transactions On Image Processing Vol: 24 No: 1 Year 2015
3. Odai M. Al-Shatanawi1 And Nameer N. El. Emam2 "A New Image Steganography Algorithm Based On Mlsb Method With Random Pixels Selection", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015
4. Hamdan Lateef Jaheel And Zou Beiji, "A Novel Approach Of Combining Steganography Algorithms", International Journal On Smart Sensing And Intelligent Systems Vol. 8, No. 1, March 2015
5. Tahir Ali, Amit Doegar, "A Novel Approach Of Lsb Based Steganography Using Parity Checker", International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 5, Issue 1, January 2015
6. Abdul Monems.Rahma , Matheel E.Abdulmunim, Rana J.S. Al-Janabi, " New Spatial Domain Steganography Method Based On Similarity Technique ", International Journal Of Engineering And Technology, Volume 5 No. 1, January, 2015
7. R. Rejani1, D. Murugan2 And Deepu V. Krishnan3., " Pixel Pattern Based Steganography On Images", Ictact Journal On Image And Video Processing, February 2015, Volume: 05, Issue: 03
8. Kamalpreet Kaur, Deepankarverma, " Multi-Level Steganographic Algorithm For Audio Steganography Using LSB, Parity Coding And Phase Coding Technique", International Journal Of Advanced Research In Computer Science And Software Engineering, Volume4, Issue 1, January 2014
9. Iwona Grabska, Krzysztof Szczypiorski, "Steganography In Long Term Evolution Systems", 2014 IEEE Security And Privacy Workshops
10. Namitatiwari, Dr. Madhu Sandilya ,Dr. Meenu Chawla ,"Spatial Domain Image Steganography Based On Security And Randomization", International Journal Of Advanced Computer Science And Applications, Vol. 5, No. 1, 2014