DIFFERENT TYPES AND TECHNIQUES OF STEGANOGRAPHY-REVIEW

[1] Prof.Sheela Bankar, [2]Prof.KomalJagdale, [3]Prof.Sonali Khairnar
[1]Assistant Professor, [2]Assistant Professor , [3]Assistant Professor
[1]Computer Department ,
[1]ISB&M School of Technology, Pune, India

Abstract : Steganography is nothing but study of invisible communication. Steganography is method of hiding communicated data .secresy is achived by embedding data into image . There are different types of steganography techniques. In this paper we review these methods with its strength and weaknesses.

***IndexTerms* - Cryptography ,encryption ,decryption, steganography,LSB,MSB**

I. INTRODUCTION

In the modern era of technology everyone wants to secrecy and safety of communicating data .In day to day life we are using so many methods of transfer data from one place to another place but every method is not secure like Internet, telephonic conversation etc. There are different methods of communication verbal communication, written communication by means we transfer data verbally or in written. There are two mechanisms to secure your data ,cryptography and steganography . In cryptography text or data is converted into cipher text so no one can recognize the original data without cipher key. But drawback of cryptography is any one can get the cipher or encryption key and decode the data .To overcome this drawback steganography have been developed.

.

II. TYPES OF STEGANOGRAPHY

1. Text steganography :- In this type information is hidden in text file .
2. Image steganography:- Information is hidden in the cover image.
3. Audio steganography:- It involves hiding data in audio file.
4. Video steganography:- In this technique digital video format is used for hiding data.

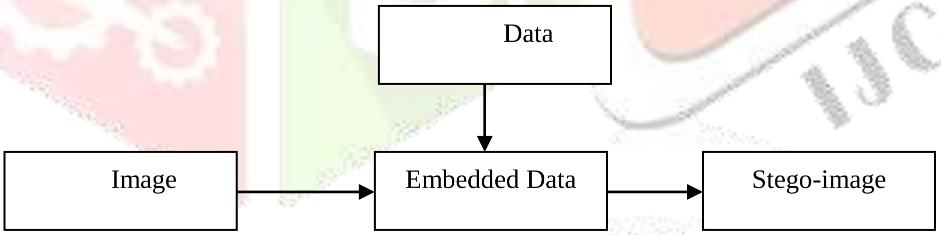

Fig.1 Steganography

III. CLASSIFICATION OF STEGANOGRAPHY

- Pure steganography where there is no stego key. It is based on the assumption that noother party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication. This is most suspectible to interception.
- Public key steganography where a public key and a private key is used for secureCommunication.

IV. STEGANOGRAPHY TECHNIQUE

1. Spatial Domain method
2. Spread spectrum Technique
3. Statistical Technique

4. Transform Domain Technique
5. Distortion Technique
6. Masking and filtering

Spatial Domain method

Image steganography is a method for secure data transfer over the internet using image. In S.Shanmuga Priya et. al's [1] The proposed method extracts two LSBs and two MSBs of the selected pixel value. Then perform the XOR operation on first and last bit and second bit and seventh bit. On the basis of result of these two XOR operations every bit of secret data is embedded one by one on LSB of selected pixel value.

Spread spectrum Technique

[2] In telecommunication and radio communication, **spread-spectrum techniques** are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately **spread** in the frequency domain, resulting in a signal with a wider bandwidth.

Statistical Technique

In Tomas Filler et. al.'s work [4], these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation

Transform Domain Technique

[3]These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking. Similar techniques can also realize large capacity embedding for Steganography

Distortion Technique

In M.B.Ould MEDENI et.al.'s article [6], It require original cover image during decoding process where decoder functions to check for differences between original cover image and distorted cover image in order to restore secret message. Encoder, adds a sequence of changes to cover image. So, information is described as being stored by signal distortion

Masking and filtering

In this paper[5] we propose a new form of multimedia steganography calleddata masking. Instead of embedding a secret message into a multimedia object, as in traditional multimedia steganog-raphy, we process the entire secret message to make it appear statistically similar to a multimedia objectitself. Thereby we foil an eavesdropper who is primarily applying statistical tests to detect encrypted com-munication channels.

V. CONCLUSION & FUTURE WORK

In this paper we studied different types and technology of Steganography. These technology we can use in different day to day life example like mobile communication security, online transaction etc. In future we can identify new area of application and different method also.

REFERENCES

[1] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp.2632-2637.

[2] https://www.science.gov/topicpages/s/statistical+steganography+techniques.html

[3]Sarita Nain, Sunil Kumar"Steganography and Its Various Techniques" International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463Vol. 3 Issue 6, June-2014, pp: (241-245), Impact Factor: 1.252,

[4] Tomas Filler, Student Member, IEEE, Jan Judas and Jessica Fridrich, Member, IEEE, (2010) "Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article, pp.1-17.

[5] REGUNATHAN RADHAKRISHNAN, MEHDI KHARRAZI AND NASIR MEMON Polytechnic University, Brooklyn, NY 11201, USA" Data Masking: A New Approach for Steganography?" Journal of VLSI Signal Processing 41, 293–303, 2005c©2005 Springer Science+Business Media, Inc. Manufactured in The Netherlands.DOI: 10.1007/s11265-005- 4153-1

[6] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "Steganography and Error Correcting Codes",International Journal of

Computer Science and Information Security, Vol.8.No.8, pp147-149.

[7] Eric Cole, Ronald D. Krutz, Consulting Editor (2003), Hiding in Plain Sight, Steganography and the Art of Covert Communication, Wiley Publishing, Inc.

[8] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.

[9] Fabien A.P.Petitcolas, Ross J.Anderson and Markus G.Kuhn, (1999) "Information Hiding – A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, pp.1062-1078.

[10] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[11] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) "Pattern Based 3D Image Steganography", 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[12] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) "Steganography Based OnRandom Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.

[13] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[14] B. Sharmila and R.Shanthakumari, (2012) "Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392.

[15] Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, (2011) "A New Steganography Technique Based on Amendment in Blue Factor ", International Journal of Electronics Communication and Computer Engineering, Vol.2, Issue 1, pp.52-56.