ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

A Survey on Steganography Techniques Achieving Security

Bavani M[1], Charulatha A R[2]

PG Scholar, MSc(Information Technology), Department of Computer Science, Stella Maris College, Chennai, India[1]

Assistant Professor, Department of Computer Science, Stella Maris College, Chennai, India[2]

ABSTRACT: Steganography is a technique of hiding messages in such a way that only the intended user can view and able to suspects the reality of the message, a form of security through anonymity. Another definition of Steganography is hiding one chunk of information inside some other information. The different Steganography algorithms like Discrete Wavelet Transform system (DWT), Least Significant bit algorithm (LSB), Blowfish algorithm and Sparse Matrix Encoding which are used for improvement of security strength for hiding the information are discussed in thispaper.

KEYWORDS*:* Cryptography, Steganography, Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), PSNR, Blowfish, Steganalysis, Sparse Matrix Encoding.

I. INTRODUCTION

Cryptology is the science underlying cryptography, cryptanalysis, steganography and steganalysis.

1.1 Cryptography

Cryptography is used to encrypt the plaintext data, transfer the cipher text over the insecure network and decrypt the cipher text to extract the plaintext at the receiver side. It is the technique for securing transmission and data in the existenceofantagonist.Cryptanalysisisthe methodofsmashingtheencrypteddatabydivulgingthedecryptionkey.

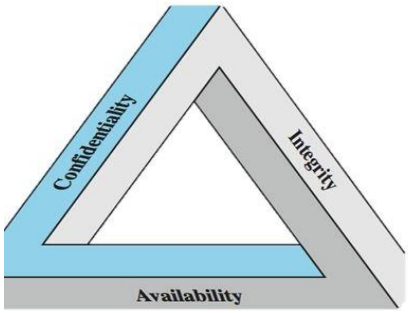

Figure 1: Cryptography Goals.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

1.2 Steganography

Steganography is the technique and practice of exchange of information by hiding confidential or restricted data into a cover object to keep safe from harm or attack from the unsanctioned access, a process of invisible communication which conceals the existence of the message. The hidden information and cover objects may be plain text, images, audio, video, text that holds themessage.

Figure 2: Steganography.

Types of Steganography

a) TextSteganography:

It is the great method in steganography which hides the message (text) behind the cover text file. It hides the HTML and CSS coding of the web pages.

b) AudioSteganography:

The method of hiding the alive of the secret message by cover up it into another carrier file such as anaudio file.

c) ImageSteganography:

The popular method in steganography techniques where we can hide the data within the cover image which prevents the message from attackers.

d) VideoSteganography:

The method of hiding any kind of information into digital video format which is used for hiding the carrier message.

1.3 Steganalysis

Steganalysis is the technique of divulging the existence of hidden information in the stego-media and it can lead to the intercept of devastating security occurrence.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

1.4 ImageSteganalysis

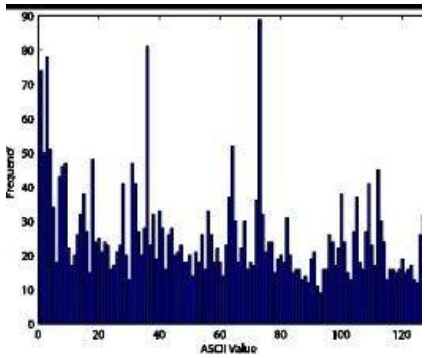

Figure 3: (a) Original Image Steganalysis

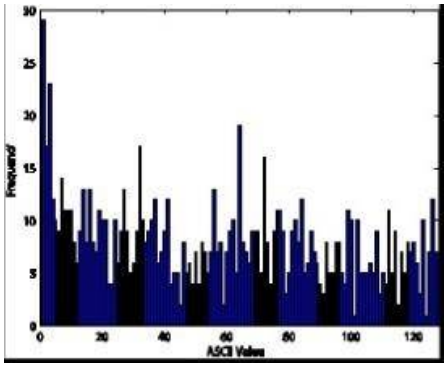

Figure 3: (b) Modified (Encrypted) Image Steganalysis

The transfer of information is so easier and faster using the internet which is promptly emerging in existing generation and security is essential since the shared information should not be hacked by the unauthorized person and make it pointless to acquire information. In this paper, the various Steganography algorithms and methods are surveyed which provides the enhancement of security of the data from attacks.

II. LITERATURESURVEY

The study of cryptography, which begins as a simple encryption technique has widened to areas like authentication, availability, confidentiality, integrity, non-acknowledgment of information. The cryptographic methods are lean on the confidentiality of encryption algorithm. Digital images are the techniques used for communication in steganography as it hides information in the image as multimedia data in such a way that does not draw scrutiny among billions of images over the web and only authorized user can view and get the reality of the message. The embedded and extraction process on cover carriers and the confidential image is achieved with LSB and DWT techniques.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

1.5 Lightweightcryptography

In [1], Lightweight cryptography is a balance achieved between lightweightness and security that provides the resistant hardware and software security which runs on a device with very low computing power, memory, storage and energy that will directly impact the system. The common issues addressed in cryptographers are by ciphers, block ciphers, hash functions and one-pass authenticated encryption. A good block cipher must be fast and secure. The cost of accomplishing the decryption should be freight to an increase of the area where it requires its own rationale. The purpose of lightweight cryptography can cause to conflicting perceptive concerning the essentials of counter-measure to move on such attacks.

1.6 Caesarcipher

In [4], Caesar cipher is a substitution cipher which is the earliest known simplest ciphers. In this ciphers, each letter in the plain text is repositioned with the certain number of places towards the alphabet. The Diffie-Helman method is a technique for providing the secret keys which is shared among the particular recipients in such a way the data cannot be noticeable as it doesn't share the information in a key. It is the public key protocols,the symmetric key in firmly sharing the cryptographic secret keys among the public networks. In Caeser cipher it can add many keys in one method for security purpose and can add more algorithm which provides the extra safeguard ciphers for communication.

1.7 Latticecryptography

In [2], Lattice cryptography is one of the most interesting areas of mathematical cryptography as a revolutionary to more established solutions based on number theoretic cryptography. A Lattice is a set of points in which n- dimensional space with periodic structure. In Lattice cryptography, the keys are randomly chosen, so that it will be hard to break it. It also provides much stronger cryptography of security with average case and worst case to secure against the quantum computers and cryptographic applications. The Lattice cryptography using short Integer Solution (SIS), Problem and Learning with Errors (LWE) provides more security compared to Diffie-Helman key exchange protocol. This Lattice based cryptography provides the greater amount of security level for the high quality of cryptography.

1.8 Least Significance Bit(LSB)

In [3], Least Significance Bit (LSB) algorithm methods are used to embed the information in images. In LSB method each byte of 24-bit images that can be encoded in each pixel, embedding the secret key inside the cover image. Here, Least Significance Bit (LSB) methods come under the spatial domain that modifies the cover image in steganography techniques that are used to change the image pixels for hiding the data by embedding the secret information. Least Significance Bit (LSB) is easily broken down by which the embedded information hidden inside it.

For enhancing the security of the algorithm from the attacker the Block based Least Significance Bit (LSB) algorithm has been used to provide the 'n' blocks are converted into 'n' image files using LSB algorithm so that the images can be randomly selected and sent. We can also hide a large number of data in one image to execute but it takes more relative time according to the size of the data and space. Therefore, Block based Least Significance Bit (LSB) provides more security to the embedded information from attackers.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

1.9 Discrete Wavelet Transform system(DWT)

In [8], Discrete Wavelet Transform (DWT) based steganography is also used for hiding the data like text in the image file.DWT in the frequency domain is used to transform the discrete time which signals the set of wavelets to discrete wavelets representation. Discrete Wavelet Transform (DWT) is used to decompose into levels of resolutions of the image and frequency domain is used to embed the frequency components of the cover carrier image. Hence, Discrete Wavelet Transform (DWT) method is extremely a powerful method which is used to hide a huge amount of information with outrageous safety with no loss of confidential information while extracting the hidden message.

a) Peak Signal-to-Noise Ratio(PSNR)

Peak Signal-to-Noise Ratio (PSNR) is the most common methods used for evaluation of image quality and provides a great importance as it involves the processing of the image. For measuring, the quality of the reconstructed image as compared to the original image.

The PSNR is defined as: PSNR=10*log10*(MAX / RMSE)
MAX is the maximum pixel value of the image and RMSE is the positions of the pixels in the image.

b) Lorenz ChaoticEncryption

Lorenz Chaotic Encryption method is used to encrypt the RBG color images pixel values as well locating the image pixel. It can be 2D-chaotic and 3D-chaotic sequences which are used for transforming the DNA sequences. The Chaotic algorithm is the method which is used to provide more security to the image transmission process for both encryption and decryption techniques between the reconstructed and original image.

c) VisualCryptography

Visual Cryptography is the distinctive type of cryptographic methods in which two transparent images are used to hide the information by using encryption techniques, in such a way only the authorized key person to decrypt it by human sight reading. In these techniques, the images and its pixels will be broken into several pieces and predefined to the appropriate participants who bags and decodes the black and white secret images or the message. Thus the visual cryptography methods are very potential useful techniques for secure computation against cheating.

1.10 Blowfishalgorithm

In [6], Blowfish algorithm is a private key block cipher encryption based algorithm in which each block is divided into the fixed variable length of a block cipher, where the same private key has been used for both encryption and decryption of hidden information. Blowfish algorithm is appropriate for the real time applications like communication links where the private key does not alternate frequently. A Fiestel Network is a symmetric structure which is used to build the block ciphers. Blowfish algorithm uses Fiestel Network which encrypts 64-bits of data at a time. It is faster than any DES algorithm and also runs at very small memory space. Thus blowfish algorithm provides stronger security and can't break easily by the attackers compared to LSBtechnique.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

1.11 Content Adaptive Steganographyalgorithm

In [7], Content adaptive steganography algorithm is used to embed a communication which shrinks the distortion to the cover image for complex texture image region. This technique boosts the Steganalysis of highly adaptive strategy compared to characteristics removal from the whole image, especially for small payloads. These two algorithms are spatial domain based steganography schemes HILL and S-UNIWARD. The HILL embedded algorithm is to redesign new embedding methods to spread the data. When embedding the same message, it is more secure for rough areas than the image with smooth areas. The UNIWARD is the steganography embedded algorithm that deploys a ubiquitous distortion between the cover image and stego image. The spatial design that hides information in pixel values called S-UNIWARD.

1.12 Sparse MatrixEncoding

In [9], Sparse Matrix is the matrix used to hold the huge amount of zero-valued elements and stores only a few numbers of nonzero elements with structured and unstructured meshes which can be considerable loads of speed and memory for processing the data. Sparse matrix encoding algorithm splits the image into non-overlapping image chunks in which a portion of an image block that extends over another image blocks. It stores every single element in memory regardless of value. For this reason, it provides us significantly reduces the amount of memory required for the data. Therefore, the Sparse Matrix Encoding based algorithm to increase the security of the information in steganography by hiding the data before encodingit.

II. COMPARATIVESTUDY

A. The comparative study of steganography in [5], based on the algorithms of LSB and DWT premise of its specifications like PSNR, MSE for the different images in Figure 5 and evaluated based on the high ratio of PSNR value in the below Table 1 and Table2.

Figure 4: Jet and Baboon.

Cover image	PSNR(dB)	MSE(dB)
Jet	52.7869	.58505
Baboon	53.7558	.52329

Table 1: LSB Substitution Technique

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

Cover image	PSNR(dB)	MSE(dB)
Jet	44.76	1.4741
Baboon	44.96	1.4405

Table 2: DWT Transform Technique

Features	LSB	DWT
Invisibility	Low	High
Payload capacity	High	Low
PSNR	Medium	Low
MSE	Medium	High

Table 3: Parameter analysis of steganography Techniques

B. The comparative study of DCT with LSB algorithm and Blowfish algorithm in [6] , a premise of its specifications like PSNR, MSE with the cover images with various sizes and evaluated based on the high PSNR value which provides the better quality of theimage.

Data Bytes	Image Size	PSNR in DB	MSE
656	600*450(im1)	72.7508846	0.004122
	800*600(im2)	71.7508846	0.004379
800	600*450(im1)	72.3669633	0.003800
	800*600(im2)	71.0083669	0.004127
1104	600*450(im1)	69.7184170	0.006993
	800*600(im2)	70.2059991	0.006250

Table 4: Experimental results of Blowfish algorithm

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

	PSNR(db)
Using DCT	48.131
Using DWT	50.134
Using Proposed Method(DCT with LSB)	71.251

Table 5: Comparative results of PSNR values for DCT with LSB

C. The comparative study of steganography based algorithms of LSB and Sparse Matrix encoded algorithms in [9] premise of its specifications like PSNR , MSE for the Time and PSNR comparison and evaluated based on the high ratio of PSNRvalue

Time Comparison			
Proposed (Text size = 1 kb)	0.51 seconds	LSB (Text size = 1 kb)	0.50 second
Proposed (Text size = 10 kb)	1.27 seconds	LSB (Text size = 10 kb)	1.26 seconds
Proposed (Text size = 100 kb)	8.33 seconds	LSB (Text size = 100 kb)	8.33 seconds

Table 6: Time Comparison

PSNR Comparison			
Proposed (Text size = 1 kb)	77.14	LSB (Text size = 1 kb)	77.14
Proposed (Text size = 10 kb)	71.31	LSB (Text size = 10 kb)	77.30
Proposed (Text size = 100 kb)	63.25	LSB (Text size = 100 kb)	63.27

Table 7: Size Comparison

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

LSB embedding for image steganography

Figure 5 (a): Original Image.

Figure 5 (b): Steganography Image

The embedded values are from [3], which is based on the LSB algorithm optimization for PSNR and MSE value between the above Figure 5a & 5b are 77.45 and 0.012

III. CONCLUSION

This paper discusses the overview of different steganography techniques its types, features, and drawbacks. In modern era transfer of information using the internet is essential. This paper discussed the use multi layersecurity by applying cryptography and steganography together and different steganography algorithms and evaluation for the table value with different ratios have been done from the previously proposed paper. From the comparative analysis of DWT and LSB, PSNR value is high for LSB. This proves that DWT is powerful method compared to LSB and provides additional security to the data. From the comparative study, Blowfish algorithm is better compared to LSB with DWT in terms of distinct image parameters. Blowfish algorithm is a more robust method that provides better security and it can't be easily broken by hackers. From the comparative study of sparse matrix encoding algorithm and LSB, Sparse matrix encoding gives the greatest amount of security to the algorithm in terms of speed memory for processing the data and also the time and size comparison in which the PSNR values also producing the additional security to the algorithm. Therefore, I conclude that Sparse Matrix Encoding based steganography algorithm provides the maximum security to the hidden information over the internet and is the best algorithm in terms of processing data speed andmemory.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 11, September 2017

REFERENCES

[1] Sadanandan, S., &Mahalingam, R. (2008). Light weight cryptography and applications. Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics, 484-488.
[2] Micciancio, D., &Regev, O. (2009). Lattice-based cryptography. In Post-quantum cryptography (pp. 147-191).
Springer Berlin Heidelberg.
[3] Kamdar, N. P., Kamdar, D. G., &Khandhar, D. N. (2013). Performance evaluation of lsb based steganography for optimization of psnr and mse. Journal of information, knowledge and research in electronics and communication engineering, 2,505.
[4] Imran, E. I., &Abdulameerabdulkareem, F. (2014). Enhancement Caesar Cipher for Better Security. IOSR Journal of Computer Engineering (IOSR-JCE), 16(3), 01.
[5] Vanitha, T., Souza, A. D., Rashmi, B., & Dsouza, S. (2014). A review on steganography-least significant bit algorithm and discrete wavelet transform algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 2(5), 89-95.
[6] Gunjal, M., &Jha, J. (2014). Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm. International Journal of Computer Trends and Technology (IJCTT)–volume, 11, 144-150.
[7] VahidSedighi and Jessica Fridrich,RemiCogranne,Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model,In SPIE/IS&T Electronic Imaging (pp. 94090H- 94090H). International Society for Optics and Photonics.
[8] Banik, B. G., &Bandyopadhyay, S. K. (2015, December). Secret sharing using 3 level DWT method of image steganography based on Lorenz chaotic encryption and visual cryptography. In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on (pp. 1147-1152). IEEE.
[9] Shah, V. (2017). Sparse Encoded Matrix based Steganography algorithm, International Research Journal of Engineering and Technology (IRJET), Vol 04, Issue 04, Apr -2017.