IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

An analytical study of Cryptography and Steganography technique for robust Security and integrity of the data

Hitendra Donga[1*], Kishor Atkotiya[2]

[1]Dept. of CS IT, Shree M. & N. Virani Science College(Autonomous), Rajkot
[2] Department of Statistics, Saurashtra University, Rajkot

Available online at: www.ijcseonline.org

Accepted: 26/Sept/2018, Published: 30/Sept/2018

***Abstract*:** As we all know the data security is the biggest concern for all the domains and it has very deep impact on the data and its security. Here in this paper we have tried to carry out the analytical study of the different cryptography and steganography technique which is used to maintain the integrity of the data. Any type of cover object can be taken that may be text, image or video to embed the secret information. In this paper a brief analysis of different image stegnography techniques and their comparison is done.

***Keywords*:** Steganography, Embedding, LZW, Stego-Key, PSNR

1. INTRODUCTION

The rise of internet plays an important role in information technology. Nowadays use of internet has been increasing day by day. Providing security has also become important issue due to the use of internet. Cryptography and Steganography are the ways to provide the security to the information. Cryptography is used to encrypt the message so that it is protected from any third parties. Steganography is a method that is used to hide information in a cover so that nobody can guess it. The cover can be any image, text, audio or video. Steganography defines from Greek word 'Stegnos' means secret and 'Graphy' means writing so overall means secret writing. The goal of Steganography is to hide the information whereas cryptography is used to protect the information from intruder or hacker. Due to the availability image file has been popularly used as the carrier.

Embedding data

Embedding data which is to be hidden requires two files first
is innocent-looking image that will hold the hidden information, called the cover image. The second file is the message the information to be hidden [10]. Firstly the cover image and hidden message are combined to form stego image. A stego key is used to hide the message and then to extract the message. Most Steganography software use lossless 24 bit images such as BMP rather than JPEG. Each pixel is represented as a single byte in 8 bit GIF files. Pixel value is between 0 and 255.Pixel. Data is index to the color palette with 256 possible colors.

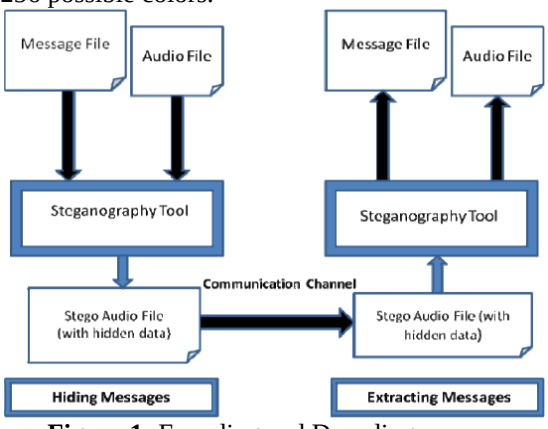

Figure 1: Encoding and Decoding process

File Compression

Two types of file compression are lossy and lossless. In lossless compression the original image integrity is maintained. The compressed image is exactly same as the original image. It is preferred more in steganography system as main goal of steganography is to hide the message in image without degrading its quality. GIF, BMP image format use lossless compression technique. On other hand lossy compression also saves the storage space but does not maintain the integrity of original image. The JPEG format use lossy compression which means not exact copy of original image.

1.1 Need of Steganography

As we know the main purpose of Steganography is to hide the data into another data such as hiding data in other text or image file. Steganography hide the information in such a way that only sender and receiver can know it. The two concepts that are closely related to Steganography are watermarking and fingerprinting that is mainly used for protection of property. Research in Steganography has been gain due to the lack in cryptographic system. It is used in way to hide the password to reach that information.

1.2 Different types of visual Steganography

There are many suitable steganography techniques based on type of cover object used.

Image Steganography: When image is taken as carrier for hiding secret information then it is called image Steganography. In this technique to hide the information we use pixel intensities.

Text Steganography: By altering certain characteristics of textual elements or by altering the text formatting we can achieve text Steganography. Text Steganography is not used often as it has very small amount of redundant data.

Audio Steganography: In audio Steganography audio is taken as carrier for hiding the secret information. It is very significant medium and uses various formats such as MPEG, WAVE, and AVI etc.

2.DIGITAL IMAGE STEGANOGRAPHY

As previously discussed coding secret messages in digital images are most widely used today. An image is an array of numbers that represent the intensities at various pixels. Generally in this technique intensity is used to hide data.

2.1Terms used in Image Steganography

Cover- image: An image which act as carrier for hiding secret information.
Stego- image: Embedding the message into cover image will generate the stego image.
Message: Original information that is used to be hidden.
Stego-Key: For embedding or extracting the messages from cover and stego images a key is used.

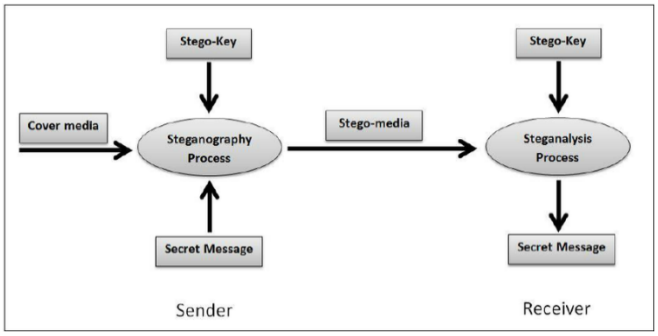

Figure 2: Framework of Steganography model

This Figure depicts the basic framework of Steganography model. The two main concept used here is embedding and extracting process. Embedding process is used hide the secret message in the image as a cover object. A stego key is used to embed the message and no one can extract the information without processing this key. As in extracting process stego image is obtained that is actual image that is holding the secret massage .As the key is used in embedding process it is also used in extracting process. Basically encoding is done at sender side to obtain stego image and decoding at receiver side to obtain secret information.

2.2 Image Steganography techniques

Image or spatial domain: In spatial domain technique the information is embedded directly into intensity of original image pixels. This technique is easy to apply due to the simplicity. This technique is dependent on the image format to be used as cover [11].We have two methods under this technique that is Least significant bit and Pallet Based LSB. In LSB secret message is hidden in the LSBs of pixel value. It usually considers BMP files as they use lossless data compression [11]. In Pallet Based LSB image consist of color lookup table and for every pixel anindex to color is stored in the pallet. It mainly uses GIF files as the cover image. A Palette based image can be represented by 256 different colors.

Transform or frequency Domain: In this technique firstly transform the cover image and then embed the secret message in significant areas. Basically there are many kinds of transform levels i.e. discrete cosine Transform, discrete wavelet transform and discrete Fourier transform. The process of embedding data in frequency domain of a signal is much stronger than embedding principles that operate in time domain. Transform domain is better than image transform as transform domain hide the information in cover image that are less exposed to cropping, compression. Discrete cosine transform (DCT) technique is mainly used in JPEG images.

Spread Spectrum: In spread spectrum technique hidden data is spread throughout the cover image so that it is difficult to detect. In spread spectrum general criteria is spreading the bandwidth from narrowband to wideband of frequencies. Embed the secret message in noise and then combine it with cover image to produce the stego image. Secret is impossible to perceive as the power of embedded signal is low than the power of the cover image.

Patchwork: Patchwork is a statistical technique that embeds the secret message using redundant pattern encoding. Redundancy is added to the secret data and then scatters it throughout the image. If consider two patch intensity of pixel in first patch are increased with some constant value and other patch is decreased by same constant value. The changes are so small that it is imperceptible to predict. The limitation of this technique is that it can embed only one bit. If more bits are to be embedded then divide the image in sub-image. The advantage is that if one patch is destroyed other will survive as the secret message is distributed throughout the image. Patchwork is most suitable for small amount of information.

Masking and Filtering: This technique is used hide the information by marking an image in the same way as to paper watermarks [12]. Information is embedded in more significant areas. Watermarking techniques can be applied without any destruction of image. This technique is sturdy and strong in form than LSB replacement. By changing the luminance of particular area mask the secret data over original data.

Distortion Technique: In this technique secret messages are stored by signal distortion .In order to restore secret message it needs to know the original message during the decoding process. After applying modifications to cover image a stego object is created. In this technique we need to check that whether the cover image and stego image is different or comes out to be similar then according to that we can set message bit '1' or '0'.There is one limitation in every technique that cover image should never can be used more than once as then attacker can easily tamper the stego object. In some cases the change can be reversed as when message is encoded with error correcting information and original message can be recovered.

3. EVALUATION CRITERIA FOR DIFFERENT TECHNIQUES

a) **Invisibility:** The invisibility of steganography algorithm is the first requirement, since the strength of steganography lies in its ability to unnotice by the human eye [8].The algorithm is compromised if the image is tampered.
b) **Payload capacity:** Steganography aims to hide the communication as watermarking that embeds the copyright information. So payload capacity also needed for embedding the information.
c) **Robustness:** After embedding data should be remain as it even if cropping, filtering is applied to the stego-image. Steganography algorithms should be robust against any changed made to the image.

d) **Independent of file format:** Only one type of file format is used between two parties that seem to be suspicious. The strong steganography algorithms has the ability to
embed data in any type of file means it is independent of
any file format. So there is no problem of finding the image in right format to use as cover image.
e) **Unsuspicious files:** This requirement includes all characteristics of a steganography algorithm that may result in images that are not used normally and may
cause problem [8].Abnormal size is example of unsuspicious file which will further result in examining the image.
f) **Security:** It should be impossible for attacker to detect the information even if it knows the existence of information. It is measured in terms of Peak signal noise ratio by using eq. 1. PSNR is used to analyze the quality of image. High PSNR high is the security as little difference in cover image and stego image.
g) Mean square Error is first calculated to calculate peak signal noise ratio.MSE represents the error between original image and compressed image. The error is lower if value of MSE is lower.

……..(1)
h) Where R=maximum value and MSE =Mean square error.

4. LITERATURE REVIEW

In [1] author has proposed a new technique of Hash-LSB with RSA algorithm that uses hash function in order to provide more security. Message has been encrypted before embedding it into a cover image. In this new technique two methods are combined that is cryptography and Steganography. Under cryptography RSA algorithm and under Steganography LSB insertion method is used. Hash function is used to find the position where to hide the data bits. In this technique a true color image of size 512*512 is used. According to least significant bit hash will returns hash value? Message is encrypted using RSA algorithm and hash function is applied to get the position where to hide the message. The Mean square error and Peak signal values of hash LSB technique is better than other technique.

In [2] author has proposed a new approach to hide the text file in image in order to maximize the storage capacity. Compression algorithm is used to increase the storage capacity. In this proposed algorithm hide the secret data based on components. First red component is replaced with first character of secret message, secondly green component is replaced with second character and then blue component is replaced with third character of secret message. This algorithm is best suited for .bmp images.

In [3] author has used two methods for hiding the information that is based on LSB Steganography and other is based on Discrete Cosine Transform Steganography. Comparison has been done between LSB and DCT based Steganography on basis of Peak signal noise ratio and Mean square error. By analyzing and comparing the values of LSB and DCT author found that PSNR is high in case of LSB. So LSB is best for security purpose.

In [4] author has proposed the new method in LSB technique that hides the secret message based on searching identical values between secret message and image. Whereas firstly the simple technique is used which hide the secret message directly in least significant bits which make the image easy to attack? Proposed method hiding every six bits of secret message in one pixel of the image Proposed method is more efficient as it first search for identical values and then start hiding. Proposed method doesn't affect the resolution as the change in the bits is quite low.

In [5] author proposed a new method for hiding the information that is instead of hiding data only in least significant bit, hide the data in combination of LSBs. Pairs of bits has been selected to replace with the data bits. Performance of a new method is evaluated by some parameters like PSNR, MSE and Standard deviation. LSB(1,2) bit pair is better than LSB(2,3) as secret message is less visible in LSB(1,2) and by analyzing the values of various parameters quality is also better than LSB(2,3) .

In [6] author proposed scheme for data hiding using compression and Steganography. In proposed scheme first the secret data is preprocessed using LZW (Lempel-ziv- welch) technique a lossless data compression technique. After the secret data is embedded into the LSBs of the cover image.LZW a lossless data compression technique is used for preprocessing of data. In this technique first dictionary is initialize then longest string in the dictionary matches with input data and represent the total size of the secret message into 16 bit binary. Scan the secret input data till no longest string is found in the dictionary. In this technique we can embed the large data into cover image without compromising the quality of image. Proposed algorithm has high embedding capacity and provides more security to the data.

In [7] author proposed a new approach to hide the multiple secret image in one color image using Transform domain technique that is Integer wavelet transform. For lossless compression IWT is more efficient. Two grey scale images of size 128*128 as secret image and 256*256 color images are used as cover. YcbCr is one of the color image representation in which Y is luminance component and Cb, Cr are chrominance component. In this proposed method represent cover image as YcbCr color space. Obtain IWT of secret image and then obtain sub-bands from transformed matrix to hide the different secret images. With the help of this technique secret images can be regenerated without actually storing the image. This approach has high PSNR which result in high quality of image as compared to other methods. But if we use spatial domain technique then this approach is easy susceptible to noise.

In [8] author provides overview of image Steganography and its technique. Author fully analyzed that which technique is best for high level of invisibility. Comparison of different image steganography algorithm has been discussed based on certain requirements. Some technique lacks in robustness while other lacks in payload capacity. While some techniques provide more security and some become difficult to implement.

In[9] author introduce scheme to generate cross platform that can effectively hide a message in digital image. In this approach selected pixel value is used to represent character instead of a color value. Loading and saving bitmap files, Bit manipulation are two operations used in this scheme. Firstly at sender side data is converted into its ASCII equivalent which then converted into bytes. Then embed the message in digital image. The LSB technique is used to hide the secret message.LSB techniques uses BMP images and they use lossless compression so for hiding the data they need large cover image. As the input message is converted into byte before embedding it into cover image so this approach provides more security and prevent from any loopholes.

In [10] author proposed edge detection method to hide the data into the color images. In this method edge detection, Randomization of edge, encoding text data, decoding text data were the four phases to be performed. Edges were detected using 3*3 window and encode text data into the blue component of sorted edge pixels. Text data can be recovered from encoded image. This method comes under spatial domain technique and result in high data embedding capacity. Edges could hide more data without losing the quality of image. This method also results in good quality of encoded image I.

5. COMPARATIVE STUDY OF THE NOVEL STEGANOGRAPHY TECHNIQUE

Table1 Comparison of Steganography Technique

Lit. Ref.	Image Steganography Techniques	Description	Advantage
[1]	Extension of LSB (Least significant bit)	Compression algorithm is used to maximize storage capacity.	Robust and efficient for hiding text and works efficiently for .bmp images.
[2]	Hash-LSB	Uses a hash function to generate a pattern for hiding data bits in LSB.	Hash-LSB with RSA increases the security of secret message.
[3]	LSB and DCT (Discrete Cosine Transform)	Comparative Analysis of two techniques based on security,PSNR.	Peak signal to noise ratio is improved using LSB but security wise DCT is best
[4]	Modified LSB	Hides secret message based on searching about identical bits.	More efficient, simple, Appropriate and accurate.
[5]	Combinations of LSB	Hiding the data in LSB bit pairs of pixels and comparison between two bit pairs.	Less visible to human eye that is quality of image is better.
[6]	LSB with compression technique	Preprocess data is embedded into the LSBs of the pixels.	High image embedding capacity, sufficient payload and high security
[7]	IWT (Integer Wavelet Transform)	Hide multiple secret images and keys in cover image.	High quality of the stego image and having high PSNR values.
[9]	LSB replacement	Generate cross platform and use selected pixel value to represent character.	Increase message security and reduce the distortion rate.
[10]	Edge Detection	Edges hide the data without altering the quality of image	High embedding capacity and high quality of encoded image.

6. CONCLUSION

In this paper different image Steganography techniques and their comparison were discussed so that one can choose best method for hiding the secret information. Different proposed techniques in the literature have been discussed and some of techniques results in high quality of image while some are more secure another. By analyzing all the techniques we found that performance of the Hash-LSB would be more secure than other techniques as earlier discussed, Hash-LSB is combination of two technologies one from cryptography and another from Steganography. RSA algorithm itself is very secure that no one can break it easily.

REFERENCES

[1] V.Sharma and S. Kumar,"A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in computer science and Software Engineering, vol3, pp 701-708,2013.G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB and DCT", International Journal for Science and Emerging Technologies, vol4, pp 36-41, 2012.

[2] Kumar and R. Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in computer science and Software Engineering, vol3, pp 363-372,2013.

[3] G. Kaur and A. Kochhar,"A Steganography Implementation based on LSB and DCT", International Journal for Science and Emerging Technologies, vol4, pp 36-41, 2012.

[4] A.M.AL-Shatnawi, "A New method in Image Steganography with improved Image Quality", Applied Mathematical Sciences, vol6, pp 3908-3915, 2012.

[5] R. Kaur, B. Singh and I. Singh, "A Comparative Study of Different Bit Positions in Image Steganography", International Journal of modern engineering research,vol2, pp 3835-3840,2012.

[6] R. Jain and N. Kumar, "Efficient data hiding scheme using lossless data compression and image Steganography", International journal of engineering science and technology, vol4, pp 3908-3915,2012

[7] Hemalatha S, U Dinesh Acharya, Renuka A and PriyaR. Kamath, "A Secure and High Capacity Image Steganography Technique", International Journal (signal and image processing), vol4, pp 83-89, 2013.

[8] T. Morkel J.H.P Eloff, M.S. Olivier, "An overview of Image Steganography", information and computer security architecture research group department of computer science, 2005.

[9] S.Singh and G.Aggarwal, "Use of image to secure text message with the help LSB replacement", International Journal of applied engineering research, vol1, pp 2010.

[10] S. Arora, S. Anand, "A Proposed method for Image Steganography using Edge Detection", International Journal for emerging technology and Advanced Engineering, vol3, pp 296-297,2013.

[11] Neil F. Jonhson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", pp 26-34, IEEE 1998.

[12] P. Kumari, C. Kumar, Preeyanshi and J. Bhushan, "Data Security Using Image Steganography and Weighing Its Techniques", International Journal of Scientific and Technology,vol2, pp 238-241, 2013.

[13] H.S. Majunatha Reddy and K.B. Raja, "High capacity and security Steganography using discrete wavelet transform", International Journal of Computer Science and Security, pp. 462-472,2009.

[14] Niels Provos and Peter Honeyman,"Hide and Seek: An Introduction to Steganography", pp 32-44, IEEE 2003. [15] S.Channalli and A .Jadhav, "Steganography an art of Hiding Data", International Journal on Computer Science and Engineering, vol1, pp 137-141,2009.

