Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 07, July -2018

IMAGE STEGANOGRAPHY TECHNIQUES – A SURVEY

ISHITA RANA

Assistant Professor K.J. Institute of Engineering & Technology Savli Gujarat

Abstract— *In today's era, due to advancements in the field of information technology, the need for information security is highly increasing day by day. Steganography plays a major role in secret data communication. It is nothing but to communicate in such a way that not only the contents are hidden but also the existence of message is kept secret which makes it different from cryptography which concerns only with keeping the contents secret. Steganography can be accomplished by hiding the information in other information, and for that, many different carrier file formats are used such as text, image and audio/video. The most popular carrier for steganography is the image because of their frequency on the internet, so hiding the data behind image file is known as image steganography. To hide data using image steganography, there are many techniques based on spatial domain, transform domain, masking and filtering and distortion. The Least significant technique of spatial domain is most commonly used which directly deals with the pixels of the image file. In this paper, different parametric comparison of many recent image steganographic techniques based on spatial and transform domainis carried out.*

Keywords—*Secret data communication; Image Steganography; Spatial domain; Least significant bit technique*

I. INTRODUCTION

In today's technology era, due to many advancements in the area of information hiding, the need of information security is highly increasing day by day. The security of our data has always been a prominent issue. Our secret data needs to be so secure and safe so that it can only access by the authorized person. The amount of data sharing on the internet from one place to another is increasing day by day and that amount is beyond our imagination. So with rising of data sharing, the need for security of data is also increased. Steganography plays a major role in secret data communication. It is nothing but to communicate in such a way that not only the contents are hidden but also the existence of message is kept secret which makes it different from cryptography which concerns only with keeping the contents secret. Steganography and cryptography they both have the same purpose that is, to provide security to our data. But, they have a different approach. Steganography deals with making the data unseen and cryptography deals with making the data unreadable. So finally,we can say that the cryptography deals with the privacy of data and steganography deals with the secrecy of data. However, steganography method is not intended to substitute or replace the cryptography method but rather to complement cryptography. What if we combine both? We can provide more security to our data, right?. So, using cryptography along with the steganography provides more security to our data, that is because of two layer security.

The term "Steganography" comes from a Greek word "Steganos", means "covered" and the word "graphein", means "writing", so combining both words we can say that steganography is covered, hidden or concealed writing. Steganography mainly aims to hide the data in a cover medium so that no one can suspect the existence of secret information which is hidden behind it. For this purpose, many different carrier file formats are used such as audio, video, text, and image. The most popular carrier for steganography is the image because of their frequency on the internet, so hiding the data behind image file is known as image steganography. Secret data hiding in digital images has drawn much attention in recent years.

II. RELATED WORK

Different algorithms of image steganography are :

a) Dynamic Approach of Frequency Based Image Steganography : uses image compression and it is based on transform domain. Advantage is that the process of data hiding is done by randoming approach. Limitation is that it has high MSE and stego image quality is minor changed after embedding.

b) Skip position approach : It is a spatial domain technique that deals with MSB, LSB and middle bit. Advantages are high payload capacity, security and the process of data hiding is done by randoming approach.

c) Segmentation and block based using OPAP : It is a spatial domain based technique that uses OPAP approach to find less distorted area. Advantages are it has high PSNR, low MSE, high payload capacity and security. Limitation is it uses sequential approach to hide data.

d) XOR based approach : It is a spatial domain based technique that uses XOR operation. Advantages are it has high PSNR, low MSE, high payload capacity and security. Limitation is it uses sequential approach to hide data.

e) Improved technique with high image quality : It is a spatial domain technique based on XOR with MSBs. Advantage is that it has higher invisibility and randoming approach but it is having limitations of moderate security and PSNR value.

f) LSB array based approach : It is a spatial domain based technique that uses 4 LSB arrays. Advantages are it has high PSNR, low MSE, high payload capacity and security and it used randoming approach to hide data.

g) Index based chaotic approach : It is a spatial domain based technique that uses indexed based chaotic approach to hide data. Advantages are it has high PSNR, low MSE, high payload capacity and security and it uses randoming approach to hide data. Limitations are it has moderate PSNR and MSE value.

h) LSB based approach : It is a spatial domain based technique that deals with LSBs of image.. Advantages are it has higher PSNR, lowest MSE, high payload capacity and security, It is having some limitations as moderate payload capacity and in sequentially manner the data is hidden.

i) LSB and MSB based method : It is a spatial domain based technique that uses LSBs and MSBs to hide data. Advantages are it has high PSNR, low MSE, high payload capacity and security and it uses randoming approach to hide data. Limitation is that it has moderate PSNR value.

All these algorithms have different strong and weak points. Hence, we need to design such technique which is highly undetectable and provides more security. Survey of some recent techniques of image steganography and parametric comparison of them is carried out in next sections.

III. THE EXISTING TECHNIQUES OF IMAGE STEGANOGRAPHY

Before moving to some existing techniques of image steganography, let’s take a look on various carriers used for steganography.

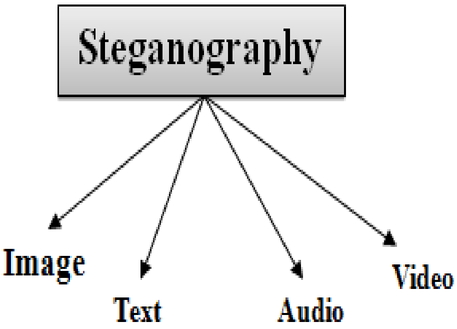

Fig. 1. Carriers for Image Steganography[10]

Different carriers for image steganography are as below :

- Text steganography :Text steganography deals with hiding the information in the text. It hides the secret information in every letter of every word of the text file. This method is not most commonly used because the text files which is used for information hiding have very small amount of redundant data.

- Image steganography :Images steganography deals with hiding the information in images. Images are used as the most popular carrier medium objects for steganography because they have many redundant bits. A message is embedded in a digital image by using an embedding algorithm, using the secret key for protecting it. The final-stego image after data is hidden behind it, is sent to the receiver. On the receiver side, hidden data is extracted by the extraction algorithm using the same key which one have used for encryption. During the transmission of the stego image, people can only observe the transmission of an image file but they cannot detect the existence of the hidden message behind the image file, this is the strength of steganography.

- Audio steganography : Audio stenography deals with hiding the information in audio file formats. It is nothing but is masking, which exploits the properties of the human ear to hide secret information that is unnoticeable.

- Video Steganography : Video(combination of images) Steganography deals with hiding the information into digital video format.

To hide data using image steganography, there are many techniques based on spatial domain, transform domain, masking and filtering and distortion. The Least significant technique of spatial domain is most commonly used which directly deals with the pixels of the image file.

A. Types Of Image Steganography Techniques

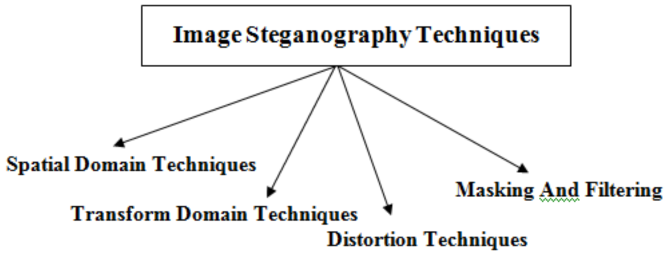
Image Steganography Techniques
Spatial Domain Techniques
Transform Domain Techniques
Distortion Techniques
Masking And Filtering

Fig. 2. Types Of Image Steganography Techniques

A lot of Research has been carried out on Image Steganography. The main purpose of this summary is to present a survey on various steganography techniques used in recent years based on different parameters such as security, robustness against visual and statistical attacks, PSNR and MSE, Stego quality, payload capacity, encryption used or not and invisibility.

a. In 2016, authors S. Guha, D. K. Sarmah, in their work “Dynamic Approach of Frequency Based Image Steganography[1]”, proposed a new technique for image steganography based on transform domain. In which, the cover image is first splitted into n blocks each having 8*8 dimension. The number of bits in secret message is calculated, let the number be m. Minimum number of secret bits that can be embedded in each block is calculated as m/n. After that, DCT is enforced on each block. The transformed blocks with DCT coefficients are quantized using JPEG quantization matrix which determines high frequency coefficients that are undetectable to human eye.

b. In 2016, authors Anusha P. and D. Bhattacharyya, in their work “A Steganographic Method for Images by ‘Skip Position’[2]”, proposed a new technique based on skip position approach. In this technique, secret data is embedded into LSB, MSB and middle bit. For inserting into middle bit, two things about skipping the position need to be consider. If byte is in even line, then place it on fifth bit and if byte is in odd line, then place it to forth bit. Skipped position matrix will store all the information about bits which are skipped. Thus, in main cover image, half pixels contains main message to be sent and second half pixels contains matrix of skipped positions.

c. In 2015, authors S. Kaur and N. Goel, in their work “Segmentation and block based image steganography using optimal pixel adjustment process and identical approach[3]”, proposed a new technique for steganography based on LSB and optimal pixel adjustment process. OPAP is used to adjust the pixel value after LSB technique. The cover image is divided into number of blocks, data which need to be embedded is divided into segments with multiple of four of image blocks. Then data is embedded using OPAP and identical approach into all image blocks after checking the less distorted image blocks. The block number is stored in jump table. This process is repeated until whole data segments are hidden into image blocks.

d. In 2015, authors K. Joshi, P. Dhankhar, and R. Yadav, in their work “A new image steganography method in spatial domain using XOR[4]”, proposed a new method in spatial domain based on XOR. In this method, two MSBs and two LSBs are extracted (i.e. bit 1,2,7 and 8, where bits 1 and 2 are LSBs and bits 7 and 8 are MSBs), then XOR operation is done between 1 and 7, 2 and 8, result will be stored in X1 and X2 respectively (where X1 and X2 are temporary variables). Then values of X1 and X2 is compared, if they are same, 0 is inserted and if not, we have to make them identical by adding or subtracting 1 from LSB. For inserting 1, insert if X1 and X2 are not same, if they are same then make them unequal by adding or subtracting 1 from LSB.

e. In 2015, authors L. Sumit and R. Roy, in their work “An improved image steganography scheme with high visual image quality[5]”, proposed a new scheme based on genetic algorithm and XOR. In this technique, two bits from MSB side of first pixel of the secret image is taken and XOR-ed respectively with 6th and 7th bit of each pixel of cover image and result is stored into corresponding pixel of the stego image. This process is repeated for all the pixels of the secret image, taking two bits at a time of the pixel of the stego image.

f. In 2015, authors S. Gandharba, and S. K. Lenka, in their work “A novel steganography technique by mapping words with LSB array[6]”, inntroduced a new technique which is based on LSB arrays. In which, 4 arrays namely LSB0, LSB1, LSB2 and LSB3 are generated. LSB0 is formed by taking one LSB from each pixel (i.e. the 8th bit of pixels). LSB1 is formed by taking two LSBs of the pixels. LSB2 array is formed by taking 3 LSBs of the pixels and LSB3 array is formed using 4 LSBs of the pixels. After that, one of these arrays will be chosen for embedding the different words of secret message in it. If our message is longer, the LSB3 array can be chosen for better matching. Then the length of each word is computed and is stored in an array E. Then E is encrypted by RSA algorithm and compressed by ZIP compression say E1, then E1 is embedded.

g. In 2015, authors S. Kumar et al., in their work “Image Steganography using Index based Chaotic Mapping[7]”, proposed a new way of hiding information in images based on index based chaotic mapping. In this, 1D chaotic logistic map is used to generate pseudo random numbers which are nothing but the positions in which we can embed our data.

h. In 2015, authors T. Al-Tamimi and A. A. Alqobaty, in their work "Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm[8]", proposed a novel algorithm for image steganography using LSB technique. In this, stego key of 32 bits which is generated randomly is used. Secret message is embedded in the pair of three bits (i.e. message block of 24 bit). LSBs of 24 sub-pixels of the next 8 pixels are replaced by the corresponding message block. This technique provides high PSNR and low MSE and thus making it more secure.

i. In 2015, author Mr. Gaurav, in their work "A New Method for Image Steganography Using LSB and MSB[9]", introduced a novel method for hiding information in images using LSB and MSB. In which, the cover image is converted into grayscale, then pixel location is obtained in cover image from secret key. Then first and last bit of pixel is extracted, if we want to embed 0, and if bits are 00 or 11, then insert. If not, make them 00 or 11 by adding or subtracting 1. If we want to embed 1, and if bits are 10 or 01, then insert. If not, make them 10 or 01 by adding or subtracting 1.

Various parameters for image steganography is given in next section and based on that comparison of existing image steganography techniques is done.

IV. ANALYSIS OF EXISTING IMAGE STEGANOGRAPHY TECHNIQUES

As stated earlier, most popular carrier for steganography is the image because of their frequency on the internet. Images are made up of pixels. All the algorithms for image steganography have many different weak and strong points, and it is very important to ensure that one uses the most suitable algorithm for steganographic purpose. However, the most important requirement is that for a steganographic algorithm has to be imperceptible.

The various criterias for judging an image steganography algorithm are as follows:

- Payload capacity : Steganography aims at hidden communication and, therefore, it requires sufficient embedding capacity. Payload capacity refers that how much amount of data it can carry.

- Robustness : In the communication of a stego image, the image may goes through some changes by an active attacker in an attempt to extract the hidden information. Many Image manipulation ways, such as cropping or rotating, can be performed on the image before it reaches its destination. Steganographic algorithms need to be robust against many manipulation techniques[11].

- Invisibility : The invisibility of a steganographic algorithm is the most important requirement because the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been altered or some what changed, the algorithm is compromised[11].

- Independent of file format : There are many different types of image file formats used on the Internet, If only one type of file format is continuously communicated with many parties , then it might seem suspicious[11].

- Robustness against statistical attacks : Many steganographic algorithms leaves an unique 'signature' when embedding of secret information that can be easily detected by performing statistical analysis. Steganographic techniques should resist against different statistical attacks and needs to be undetected [11].

- MSE(Mean Square Error) : It is the difference between cover image and stego image. Its value should be low.

- PSNR(Peak Signal To Noise Ratio) : PSNR is defined as peak signal to noise ratio where peak signal is the referred to the signal of the original image. Noise is the secret bits added to the image[1].

- Stego Quality : It is the quality of stego image after data is embedded into it.

- Randoming Type : The data which we want to embed is done by sequential or random manner.

- Encryption : It is the process to encrypt the data with some secret key before embedding them into the cover file.

- Compression : Compression is usually done in transform domain. It is the process of compressing the file before embedding the data into it.

- Image type : It shows the type of image supported by the existing techniques. Usually done in 2 types, loseless and lossy, that is, colour images or gray scale images.

Following table shows parametric comparison of some of the existing techniques of image steganography based on parameters discussed above.

TABLE 1. Parametric Comparison of Image Steganographic Techniques

Evaluation Parameters	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Domain Method (Spatial/Transform)	Transform	Spatial	Spatial	Spatial	Spatial	Spatial	Spatial	Spatial	Spatial
Image Type Supported (Gray/Colour)	Gray	Colour	Colour	Gray	Gray	Colour	Colour	Colour	Gray
Compression used?	Yes	No	No	No	No	Yes	No	No	No
Encryption used?	No	No	No	No	No	Yes	No	Yes	No
Randoming Type (Sequential/Random)	Random	Random	Sequential	Sequential	Random	Random	Random	Sequential	Random
Robustness (against statistical and visual attacks)	Low	High	High	High	Low	High	High	High	High
Security	Moderate	High	High	High	Moderate	High	High	High	High
Invisibility	Moderate	High	High	High	High	High	High	High	High
Stego Quality(Changed or not?)	Minor Changed	Not Changed	Not Changed	Not Changed	Not Changed	Not Changed	Not Changed	Not Changed	Not Changed
MSE	High	Not given	Low	Low	Not given	Not given	Moderate	Lowest among all	Low
PSNR (in db)	Moderate	Not given	High	High	Moderate	High	Moderate	High	Moderate
Payload Capacity	High	High	High	High	High	High	High	Moderate	High

As can be seen from the comparison, the technique “Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm[8]” by T. Al-Tamimi and A. A. Alqobaty has the high PSNR ratio and lowest MSE amongst these all techniques which makes it to provide 3 layer higher security. All of these make the process of steg-analysis more complex even with using a computer works at10^6 extractions/micro second which takes 2.4 *10^{24} years to exhaustively search a half of the number of stegakeys. However, payload capacity of this technique is moderate.

V. CONCLUSION

There are many different techniques for Image Steganography exists and continue to be developed, we have seen that the most widely used mechanism is the least significant bit technique of spatial domain. However, a simple LSB technique is less secure and robust as compared to LSB which is having use of cryptography also. In this paper, survey on various techniques for image steganography is carried out. To conclude, we can say that the best technique will provide higher security against different attacks that are visual and statistical attacks (Such as image cropping, compression, image manipulation, by applying steganalysis).

References

1. S. Guha, D. K. Sarmah, “Dynamic Approach of Frequency Based Image Steganography”, International Journal of Applied Engineering Research, ISSN 0973-4562, Vol.11, No.11 , pp.7478-7482, 2016.
2. Anusha P. and D. Bhattacharyya,“A Steganographic Method for Images by ‘Skip Position’” International Journal of Security and Its Applications, Vol.10, No.7, pp.51-58, 2016.
3. S. Kaur and N. Goel, “Segmentation and block based image steganography using optimal pixel adjustment process and identical approach”, 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS). IEEE, pp.1-5, December 2015.
4. K. Joshi, P. Dhankhar, and R. Yadav, “A new image steganography method in spatial domain using XOR”,Annual IEEE India Conference (INDICON). IEEE, pp.1-6, December 2015.
5. L. Sumit and R. Roy, “An improved image steganography scheme with high visual image quality”, Computing, Communication and Security (ICCCS), 2015 International Conference on. IEEE, pp.1-6, December 2015.
6. S. Gandharba, and S. K. Lenka, “A novel steganography technique by mapping words with LSB array”, International Journal of Signal and Imaging Systems Engineering, Vol.8, Nos.1-2, pp.115-122, January 2015.
7. S. Kumar et al., “Image Steganography using Index based Chaotic Mapping”, IJCA Proceedings on International Conference on Distributed Computing and Internet Technology, ICDCIT, Vol.1, pp.1-4, 2015.
8. T. Al-Tamimi and A. A. Alqobaty, “Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm”, International Journal of Computer Science and Information Security, Vol.13, No.1, January 2015.
9. Mr. Gaurav, “A New Method for Image Steganography Using LSB and MSB”, International Journal of Recent Research Aspects, Vol. 2, Issue. 4, pp.169-174, December 2015.
10. Sandeep Kaur, Arounjot Kaur, Kulwinder Singh ,“A Survey of Image Steganography” , Ludhiana in IndiaInternational Journal of Computer Applications Technology and Research Vol.3,No.7,pp. 479 - 483, 2014.
11. Solanki R, Chuahan M, Desai M, “SURVEY OF IMAGE STEGANOGRAPHY TECHNIQUES”, in “International Conference on: “Engineering: Issues, opportunities and Challenges for Development”, 2015.