DATA HIDING TECHNIQUES IN DIGITAL MULTIMEDIA

Girish Kumar BS[1], Prof (Dr) Ajay Rana[2]
[1]*M Tech Scholar Computer Science & Engineering,*
ASET, Amity University, Noida, India
bsgirishkumar@gmail.com
[2]*Director ATPC, Amity University, Noida, India*
ajay_rana@amity.edu

***Abstract*— "Digital Image Watermarking" is the software technique for hiding data called as Steganography. It is derived from the Greek words meaning, "Covered writing", In short it is the art of information hiding in ways that its detection is prevented. It is a method of covert and invisible communication, which adds another step in securing data. Any message in cipher form may arouse suspicion while an invisible message is not. Digital stenography makes use of a host data or message known as a "Container" or "Cover" to hide another data or message in it. The normal way of protecting information data was to use a encryption. Steganography is also used to place a hidden text in images, audio, and video, a technique referred to as watermarking. The information to be hidden is embedded into the cover object which can be a text, image, or audio /video file in such a way that the existence of the message is not detected and the appearance of the resulted exactly matches the original. The main aim of steganography is to hide the data in the message present in the transmission medium. To ensure secrecy or privacy of communication between two parties, various methods are being developed. Cryptography is one of main methods. Also, there are various different techniques that can be implemented to attain security of a certain level. Here we study various techniques for data hiding in images, known as Digital Image Steganography.**

***Keywords*— Include at least 5 keywords or phrases**

I. INTRODUCTION

This document is a template. Steganography [34] is the art of hiding information within innocuous cover carriers in ways such that the hidden message is undetectable. In Greek, "stego" means „covered" or "secret" and "graphy" means "to write" and therefore, steganography becomes "covered or secret writing".The information to be hidden is embedded into the cover object which can be a text matter, some image, or some audio /video file in such a way that the very existence of the message is undetected by maintaining the appearance of the resulted object exactly same as the original. The main aim of steganography is to hide the data in the message present in the transmission medium.

Cryptography [35] is the science of encrypting data such that one cannot understand the message, whereas in steganography the mere existence of data is hidden such that its presence cannot be noticed. Using cryptography techniques leads to suspicion whereas in steganography the existence of encrypted message is invisible and hence data is secure. steganography can be thought of as an extension of cryptography, and it is commonly used where encryption is not allowed.

Steganography on the basis of cover object may be of many types like the Image Steganography, Video Steganography and the Audio Steganography, etc. The most common is Image Steganography because of popularity of digital image transmission over the internet. Image Steganography makes use of redundancy in the digital image [2, 11] to hide the secret data. It may be divided into two categories. The first one is spatial-domain methods and the second one is frequency-domain ones. In the spatial domain, the secret data are embedded in the image pixels directly. In the frequency-domain, however, the cover image is first transformed to frequency-domain, and then the secret messages are embedded in the transformed cover image.

II. SPATIAL DOMAIN TECHNIQUES

LSB substitution [3, 4] method uses fixed k Least Significant Bits in each pixel of cover image to embed secret message. This method is the easiest method to hide message in an cover image. However, it is easy to uncover a stego-image produced by the Least Significant Bit insertion method.

In distortion technique method few pixel property of the cover image is changed according to data

information. The deflection of distorted from original image contains secret information.

III. TRANSFORM DOMAIN TECHNIQUES

On embedding information in spatial domain, encrypted image may be subjected to losses if the image undergoes any image processing technique like compression, cropping etc. To overcome this losses problem, transform domain techniques are made use of. Here we embed the information in frequency domain such that the secret information is embedded on the significant frequency values while higher frequency part is omitted.

Frequency transformation is carried out to the image and then data is hidden by changing the values of the transformation coefficients with respect to data information accordingly. There are three types of transformation techniques:

1) Fast Fourier Transform: In 2D FFT cover image is first converted to the frequency transform domain and then secret data bits are embedded on the significant coefficients. FFT includes the complex term also, hence more mathematical computations is required to be computed. In FFT method time complexity is higher than in DCT method.

2) Discrete Cosine Transform: In 2D DCT is used for transforming the cover image [5, 6]. DCT though is derived from the FFT, it requires fewer multiplications than the FFT as it works only with real numbers. The DCT produces fewer significant coefficients than FFT in its result, leading to greater compression. DCT is the popular technique in the field of steganography [17]. If after DCT transformation, quantization step is also undertaken as in Joint Photographic Experts Group (JPEG) compression [1] then it becomes robust to JPEG compression and is called as JPEG steganography [26].

3) Discrete Wavelet Transform: In DWT [9-12] is used to separate high frequency components from the low frequency components. It replacing the high frequency part by the required secret data. The maximum capacity of embedding in this technique is much greater than DCT steganography [23].

IV. CHALLENGES IN STEGANOGRAPHY

The major challenges faced in achieving high effectiveness in steganography are:-

A. Security of Hidden Communication

Steganography techniques should be able to produce high imperceptibility in order to avoid raising suspicions. The hidden data contents should be invisible from both perceptually and statistically point of view.

B. Size of Payload

Watermarking needs only a small amount of copyright information to be embedded whereas in steganography large amount of data is embedded. Hence Steganography requires sufficient embedding capacity for hidden communication. The requirements of higher payload and secure communication do not go together and hence are often contradictory. Therefore a tradeoff is sought depending on the specific application scenarios.

c. obuRstness

Robustness to image processing techniques like compression, cropping, resizing etc. i.e. is required to be overcome by the Stego-image. when any of the above techniques are performed on stego-image, secret data should not be lost completely. No single technique of steganography exists which provide all the three properties at high level. There is always a trade-off between the maximum capacity of the embedded data and the high robustness to certain attacks, while still keeping the perceptual quality of the stego-medium at an acceptable level. Attaining high robustness to signal modifications and high insertion capacity at the same time [30] is not possible to be achieved.

V. PERFORMANCE EVALUATION MATRICES

The information providing parameters on the performance of the Steganography techniques are as follows:-

A. Embedding Capacity

It is the maximum capacity of the secret data that can be embed in cover image without being noticeable or degrading the integrity of the cover

image. It is represented in bytes or Bit Per Pixel (bpp).

B. Mean Square Error (MSE)

It is defined as the square of error between cover image and the encrypted stego-image [33].The image distortion with respect to coverimage can be measured using MSE and is calculated using Equation 1.

$$MSE=\left[\frac{1}{M*N}\right]^2 \sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij}-X'_{ij}\right)^2 \quad \ldots\ldots\ldots(1)$$

Where:

X_{ij}: The intensity value of the pixel in the cover image.

X'_{ij}: The intensity value of the pixel in the stego image.

M*N: Size of an image.

C. Peak Signal Noise Ratio (PSNR)

It is defined as the ratio of peak square value of pixels and the MSE. Decibel is the unit it is expressed. It measures the statistical difference between the coverimage and stego-image, and is calculated using Equation 2.

$$PSNR=10 \log_{10}\frac{255^2}{MSE} \text{ db} \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

D. Histograms

Histogram is a measure of the number of occurrence of pixels with respect to a particular pixel value [29]. During embedding pixel value changes the number of pixel having a particular pixel value changes. These changes are used to detect steganography. If lower is the difference of histograms between coverimage and stego-image results in more resistivity to detect the data information in stego-image.

VI. TECHNIQUES USING TRANSFORM DOMAIN

JPEG steganography is implemented using Discrete Cosine Transform by converting image into frequency domain. JPEG steganography is just the modified version of JPEG compression.

A. JPEG Compression

The Joint Photographic Experts Group developed the JPEG [1] algorithm to address the problems, specifically the fact that consumer-level computers had enough processing power to manipulate and display full color photographs. Full color photographs requires a tremendous amount of bandwidth to transfer over a network connection, and requires just as much space to store a local copy of the image. Other compression techniques has major trade offs. They have either very low amounts of compression, or major data loss in the image. The JPEG algorithm was created to compress photographs with minimal data loss and high compression ratios. The image is divided into 8 x 8 pixel blocks and a DCT is applied to each block to convert the information from the spatial domain to the frequency domain. The frequency information is then quantized to remove redundant information. Finally, the standard compression techniques compresses the final bit stream.

B. JPEG Steganography

JPEG steganography is more important and popular because stego-image produced are robust to jpeg compression by these techniques. The secret data is embed after quantization phase of JPEG compression. The secret its modify only significant quantized DCT coefficients. Subsequent steps are similar to JPEG compression. In this way stego-image is produced in .jpg format directly. Some JPEG steganography techniques are as given below:

VII. STEGANOGRAPHIC TOOLS

A. Jpeg-Jsteg

In Jpeg–Jsteg, the secret messages are embedded in LSB of quantized DCT coefficients. Its execution steps are described briefly as follows.

First, JPEG partitions a cover image into non overlapping blocks of 8*8 pixel, and then it uses DCT to transform into DCT coefficients each block. The DCT coefficients results are scaled according to a quantization table. The embedding sequence employed in Jpeg–Jsteg is in the zigzag scan order. After embedding the secret message in each block, to compress each block Jpeg–Jsteg uses coding methods such asRun-Length coding, Huffman coding, and DPCM of JPEG entropy coding.

Finally, JPEG stego-image is obtained from Jpeg–Jsteg but has limited message capacity. Most important coefficients are located around the low-frequency part in DCT transformation. The quantized DCT coefficients in the low-frequency part are modified by Jpeg–Jsteg. Therefore, when the cover-image undergoes a high compression ratio, the image quality of Jpeg–Jsteg is degraded. The advantages are it is robust to JPEG compression and it has Less bandwidth requirement for stego image transmission because of its reduced size. The disadvantages are that the embedding of secret messages in cover image is limited and the high detectability as it introduces characteristic artifacts into the first order statistics (histogram) of DCT coefficients.

B. Steg-Hide

Graph-theoretic approach to steganography is used by Steghide. It embeds by swapping Discrete Cosine Transform coefficients and thus avoids changing the histogram. The embedding done by exchanging pixel values implies that the first-order statistics (i.e. the number of times a color occurs in the picture) is not changed. The sender splits the cover-image in 8 x 8 pixel blocks during the encoding process; each block encodes exactly one secret message bit. A pseudorandom block bi is used to code the ith message bit in the embedding process. Both sender and receiver agree on the location of two Discrete Cosine Transform coefficients, which is used in the embedding process Before the communication starts; we denote these two indices by (u1,v1) and (u2,v2). The two coefficients correspond to cosine functions with middle frequencies; this ensures that the information is stored in significant parts of the signal (hence the embedded information will not be completely damaged by JPEG compression). The advantages are that it cannot be detected by steganalysis which uses first order characteristics, because histogram is preserved [27] and itt provide Robustness to JPEG compression. The disadvantages are that its embedding capacity is less than Jsteg too and the cover size in which message embedded is always multiple of 8 which can be used to detect the presence of secret message.

VII. CONCLUSION AND FUTURE SCOPE

Spatial domain techniques embed information in easy ways, but they are very highly vulnerable to even small cover modifications. Therefore the size of stego-image cannot be reduced. By simply apply signal processing techniques the secret information can be destroyed entirely. The small changes resulting out of lossy compression systems yield even to total information loss in many cases. Transform domain methods are used to hide messages in significant areas of the cover image which are more robust to attacks. As a result lossy compression such as Jpeg compression can be performed and size of stego-image can be reduced. But the disadvantage is that only few messages can be embedded in the cover-image. The embedding capacity is also very less than spatial domain techniques. High PSNR, high perceptual quality and high embedding capacity are provided by the spatial domain techniques but these not provide robustness. On the other hand robustness while providing very less embedding capacity, low PSNR and low perceptual quality are provided by transform domain.

Trade Off between the three properties, perceptuality, embedding capacity and robustness exists. New techniques should be developed to maintain these three properties at very high level. The few areas which are new in steganography are to increase the embedding capacity while maintaining the robustness of Stego-image Wavelet transform can be used. To reduce the impact of steganography i.e.to increase the PSNR, Hamming coding or Matrix coding can be used. Cryptography techniques like RSA, AES and hash functions can also be used with steganography to provide more security.

REFERENCES

[1] Wallace, G. K., *The JPEG Still Picture Compression Standard, Communications of the ACM*, vol. 34, no. 4, 1991, pp. 30-44.

[2] Kurak, C., and J. McHughes, "*A Cautionary Note On Image Downgrading*," in IEEE Computer Security Applications Conference 1992, Proceedings, IEEE Press, 1992, pp.153-159.

[3] Bender, W., D. Gruhl, and N. Morimoto, "*Techniques for data hiding*", IBM Systems Journal, vol. 35, no. 34, 1996, pp. 131-336.

[4] M¨oller, S., A. Pitzmann, and I. Stirand, "*Computer Based Steganography How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best, in Information Hiding*" First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 7-21.

[5] Cox, I., et al., "*A Secure, Robust Watermark for Multimedia*," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 185-206.
[6] O. Runaidh, J. J. K., F. M. Boland, and O. Sinnen, "*Watermarking Digital Images for Copyright Protection*," in Electronic Imaging and the Visual Arts, Proceedings,Feb.1996.
[7] DerekUpham:Jsteg,1997,.http://www.tiac.net/users/korejwa/jsteg.htm
[8] Swanson, M.D., B. Zhu, and A. H.Tewfik, "*Transparent Robust Image Watermarking*," in Proceedings of the IEEE International Conference on Image Processing, vol. 3, 1996,pp. 211-214.
[9] Xia, X., C. G. Boncelet, and G.R. Arce, "*A Multiresolution Watermark for DigitalImages*," in Proceedings of the IEEE International Conference on Image Processing(ICIP'97), 1997.
[10] Sandford, M. T., J. N. Bradley, and T. G. Handel, "*Data Embedding Method*," in Proceedings of the SPIE 2615, Integration Issues in Large Commercial Media Delivery Systems, 1996, pp. 226-259
[11] Johnson, N. F., and S. Jajodia, "*Exploring Steganography Seeing the Unseen*, IEEEComputer , vol. 31, no. 2, 1998, pp. 26-34.
[12] J.J. Chae & B. S. Manjunath, "*A Robust Embedded Data from Wavelet Coefficients*",SPIE: Storage and Retrieval for Image and Video Databases VI, 3312, San Jose, CA, Jan.1998, 308-317.
[13] Luby, M., and C. Racko, "*How to Construct Pseudorandom Permutations from Pseudorandom Functions*, SIAM Journal on Computation, vol. 17, no. 2, 1988, pp. 373-386.
[14] Naor, M., and O. Reingold,"*On the Construction of Pseudorandom Permutations Luby-Racko Revisited*, Journal of Cryptology, vol. 12, no. 1, 1999, pp. 29-66
[15] Andreas Westfeld: The Steganographic Algorithm F5, 1999. http://wwwrn.inf.tu-dresden.de/westfeld/f5.html
[16] AndreasWestfeld, Andreas Pfitzmann: *Attacks on Steganographic Systems, in AndreasPfitzmann (Ed.)*: Information Hiding. Third International Workshop, LNCS1768, Springer-Verlag Berlin Heidelberg 2000. pp. 61–76.
[17] J.R. Hernandez, M. Amado, & F. PerezGonzalez, "*DCTDomain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure*", IEEETrans. Image Processing, 9, Jan. 2000, 55-68.
[18] Provos, N. *Defending Against Statistical Steganalysis. Proc. 10thUSENIX* SecuritySymposium. Washington, DC, 2001
[19] J.Fridrich,M.Goljan,and R. Du, "*Detecting LSB Steganography in Color and Gray-Scale Images*", Magazine of IEEE Multimedia Special Issue on Security, pp. 22-28,October-November 2001
[20] J. Fridrich, M. Goljan, and R. Du, "*Reliable detection of LSB steganography in color and gray scale images*," Proc. ACM Workshop on Multimedia and Security, pp. 27–30, 2001.
[21] A.Westfeld, "*F5- A steganographic algorithm: high capacity despite betterssteganalysis*", Lecture Notes in Computer Science, vol.2137, pp.289-302, 2001
[22] B. Chen and G.W.Wornell, "*Quantization index modulation: A class of provably good methods for digital watermarking and information embedding*", IEEE Trans. On Information Theory, vol.47, no.4, pp.1423-1443, 2001.
[23] P. Meerwald & A. Uhl, "*A Survey of Wavelet-Domain Watermarking Algorithms*", SPIE Symposium, Electronic Imaging, San Jose, CA, USA, 2001.
[24] J. Fridrich,M. Goljan, "*Practical Steganalysis of Digital Images –State of the Art*", Proc.SPIE, Photonics West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, pp. 1-13, January, 2002.
[25] Fridrich, J., Goljan, M., and D. Hogea. *Steganalysis of JPEG Images: Breaking the F5Algorithm.* 5th Information Hiding Workshop, Noordwijkerhout, Netherlands, Oct. 2002
[26] J.J. Eggers, R. Bauml and B.Girod, "*A communications approach to imagesteganography*", Proceedings of SPIE, vol.4675, pp.26-37, 2002.
[27] J. Fridrich, M. Goljan and D. Hogea, "*New methodology for breaking steganographictechniques for JPEGs*", Proceedings of SPIE, vol.5020, pp.143-155, 2003.
[28] .J. Fridrich, M. Goljan, and T. Holotyak, "*New Blind Steganalysis and its Implications*",in Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII,vol. 6072, pp. 607201, Jan. 2006
[29] K. Solanki,K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran,"*Provably Secure Steganography : Achieving Zero K-L Divergence using Statistical Restoration*"in proc.ICIP,2006 pp.125-128
[30] Hong-Juan Zhang, Hong-Jun Tang,"*A Novel Image Steganography Algorithm Against Statistical Analysis*", Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007
[31] Mahendra Kumar and Richard Newman,"*J3: High Payload Histogram Neutral JPEG Steganography*", Eighth Annual International Conference on Privacy, Security and Trust, 2010
[32] Shailender Gupta, Ankur Goyal, Bharat Bhushan,"*Information Hiding Using Least Significant Bit Steganography and Cryptography*",I.J.Modern Education and Computer Science, 2012, 6, 27-34
[33] Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, "*Steganography: Dct Coefficient Replacement Method and Compare With Jsteg Algorithm*" International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, August 2012
[34] "*Steganography in Digital Media: Principles, Algorithms and Applications*", Jessica Fridrich.
[35] "*Cryptography and Network Security principles and practices*", William Stallings, pearsons education, first Indian reprint 2003