# A Study on Spatial Domain and Transform Domain Steganography Techniques used in Image Hiding

**L.Baby Victoria***
Ph.D Research Scholar, Department of Computer Science,
Erode Arts & Science College (Autonomous), Erode
Email: victoriaerode@yahoo.co.in
**Dr.S.Sathappan**
Research Supervisor & Associate Professor
Department of Computer Science, Erode Arts & Science College (Autonomous), Erode, Tamil Nadu, India.
Email: devisathappan@yahoo.co.in

**Abstract— Steganography is the art of hiding a secret message within a larger one in such a way that an observer cannot detect the presence of contents of the hidden message. The Steganography used to transport information from one place to other place through public channel in covert way. Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. The art of information hiding has received much attention in the recent years as security of information has become a big concern in this internet era. Steganography is a technology where modern data compression, information theory, spread spectrum, and cryptography technologies are brought together to satisfy the need for privacy on the Internet. This paper analyses the Spatial Domain and Transform Domain techniques of Steganography which are used for Image Hiding.**

**Keywords— Steganography, Spatial Domain, Transform Domain, Image Hiding, DCT, DWT**

## 1. INTRODUCTION

Steganography is the art and science of invisible communication. It is accomplished by hiding information in other information, thus hiding the existence of the information. Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. The idea and practice of information hiding has a long past. In Histories the Greek historian Herodotus writes of a Nobleman, Histaeus, who needs to communicate with his son-in-law in Greece, has shaved the head of one of most trusted slave and tattooed the message onto the slave’s scalp. When the slave’s hair grew back he sends slave with the hidden message and when slave reaches to the destination again he shaved his scalp and retrieve the message [1].

In the Second World War the Germans introduces new data hiding technique which is known as Microdot technique. In this the information, like photographs, was reduced in size until it was the size of a typed period. It was Extremely difficult to detect a hidden information, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information[2].

Today Steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Although related to cryptography, they are not similar. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message in such a way that it cannot be understood[3].

Steganography and cryptography are techniques used to protect information from unwanted parties but neither technology alone is perfect . Once the presence of hidden information is revealed or suspected, the reason of Steganography is partly defeated. The strength of Steganography increases by combining it with cryptography. The Steganography has been categorized into (i) Spatial domain Steganography: It mainly includes LSB Steganography and Bit Plane Complexity Slicing (BPS) algorithm. Spatial domain is frequently used because of high capability of hidden information and easy realization. (ii) Transform domain Steganography: The secret information is embedded in the transform coefficients of the cover image. Steganography used for wide range of applications such as defiance organizations for safe circulation of secret data, intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient’s details are embedded within image providing protection of information and reducing transmission time.

## 2. REVIEW

This paper analyses the various papers on Spatial Domain and Transform Domain of Steganography techniques which are helped to understand the topic and its importance.

**i. Spatial Domain:** These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step.

Namita Tiwari et.al [4] article the authors proposed a commonly used method LSB and randomization. LSB based Steganography methods Stego One Bit, Stego Two Bit, Stego Three Bit, Stego Four Bit are used. The Stego One Bit changes only single LSB of the pixel, it should have very less effect. The advantage of Stego Two Bit is that twice as much information can be stored. By Using Stego Three Bit, three LSBs of the Colours in the RGB value of the pixels will be used to store message bits. By using Stego Four Bit the data hiding capacity is 4 times the storage capacity of Stego 1. For encryption and hiding used Triple-A Randomization. This paper has achieved highest capacity among all existing method without any distortion in image.

G.S.Sravanthi, B.Sunitha Devi, S.M.Riyazoddin and M.Janga Reddy[5] have proposed a new method of information hiding in digital image in spatial domain. They used Plane Bit Substitution Method technique in which message bits are embedded into the pixel value of an image. They proposed steganography transform machine (STM) for solving binary operation for manipulation of original image with help to least significant bit (LSB) operator based matching.

Madhu et al., in [14] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency.

Fahim Irfan Alam et. al [15] the authors suggest noise filtering in the beginning before embedding. After extraction at receiving end, ARQ (Automatic Repeat Request) is used for error detection & correction. For secure transmission of data, encryption & data hiding are combined in a single step. Host image and secret data are converted into bit stream. Before encryption of secret data median filtering is used. The input values are converted to ASCII and then to binary, the host image RGB values are converted to binary. Substitution is performed character by character using encryption key. The LSB of every pixel octet is replaced by secret bit stream. Error detection and correction ensures correct transmission of data.

**ii. Transform Domain Technique:** This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

Transform domain techniques are broadly classified into:

1.Discrete Fourier transformation technique (DFT).
2.Discrete cosine transformation technique (DCT).
3.Discrete Wavelet transformation technique (DWT).
4.Lossless or reversible method (DCT)
5.Embedding in coefficient bits

S. Hemalatha, U. Dinesh Acharya, A. Renuka and Priya R.Kamath[17] have provided a novel image steganography technique to hide both image and key in color cover image using Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). There is no visual difference between the stego image and the cover image. The results are compared with the results of similar techniques and it is found that the proposed technique is simple and gives better PSNR values than others.

M. Chaumont et al., in [18] have proposed a DCT based data hiding method. It hides the color information in a compress gray-level image. It follows the color quantization, color ordering and the data hiding steps to achieve image steganography. The purpose of method is to give free access to gray-level image to everyone but restricted access of same color images to those who have its stego-key. It has high PSNR plus with noticeable artifact of embedding data.

K. S. Babu et al., in [19] proposed hiding secret information in image steganography for authentication which is used to verify the integrity of the secret message from the stego-image. The original hidden message is first transformed from spatial domain to discrete wavelet transform (DWT); the coefficients of DWT are then permuted with the verification code and then embedded in the special domain of the cover image. The verification code is also computed by special coefficient of the DWT. So this method can verify each row of the image of modified or tampered by any attacker.

Po-Chyi et.al. article [20] the authors compare the advantage of embedding in JPEG 2000 images with the previous approach of embedding in JPEG images. Most of the steganographic methods are based on JPEG because as a block DCT codec JPEG lends itself a good candidate for information hiding due to its fixed block structure. JPEG 2000 which is an upcoming still image coding standard can be used to hide high volume data. If information is embedded in the output of tier-2 coding, i.e. the JPEG 200 packets, it can be guaranteed that all the embedded information will be received without error and in correct order. But, difficulty lies in the modification of packets for embedding, since the bit-streams are compactly compressed by the arithmetic coder. Careless modification would result in failure of expanding compressed image. In the embedding process the image is decomposed using wavelet transform. Lazy Mode Coding is used for embedding.

Prosanta Gope et. al. article [21], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

**Table 1: Spatial Domain Based Steganography Method**

| S.No. | Author | Year | Method Used | Advantage |
|---|---|---|---|---|
| 1 | Namita Tiwari, Madhu Sandilya and Meenu Chawla | 2014 | LSB Based Steganogrphy Methods | High Capacity and good MSE and PSNR |
| 2 | G.S.Sravanthi, B.Sunitha, S.M.Riyazoddin & M.Janga Reddy | 2012 | Plane Bit Substitution Method | Sufficient to discriminate analysis of stego and cover image |
| **3** | V. Madhu Viswanatham and J. Manikonda | 2010 | LSB Insertion Mechanism, Random Number Generation Algorithm | Secure transformation of data |
| 4 | Fahim Irfan Alam et al. | 2011 | Noise Filtering before embedding combined with encryption | Error detection & Noise free transmission |

**Table 2 : Transform Domain Based Steganography Method**

| S.No. | Author | Year | Method Used | Advantage |
|---|---|---|---|---|
| 1 | Hemalatha S, U Dinesh Acharya, Renuka A and Priya R.Kamath | 2013 | Discrete Wavelet Transform & Integer Wavelet Transform | Simple and better PSNR Value |
| 2 | M. Chaumont and W. Puech | 2007 | DCT based Data Hiding | Compress images with a WWW standard format |
| 3 | K.S. Babu et.al. | 2008 | Discrete Wavelet Transform | verify each row of the image of modified or tampered by any attacker. |
| 4 | Po-Chyi et.al. | 2003 | Lazy Mode Coding | Hide High Volume Data |
| 5 | Prosanta Gope , Anil Kumar and Gaurav Luthra | 2010 | Enhanced JPEG Steganography | High Security |

## 3. CONCLUSION

In this paper the various articles which are used spatial domain and transform domain for image hiding were studied and categorized. Now- a – days many new areas are identified like Cloud Computing, Mobile Computing and Online Services ( Online Banking , E-Commerce, E-Ticket etc.). The steganographic principles will guide us to improve its applications in the new areas.

## 4. REFERENCES

[1] Jarno Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006Volume : 13, Issue : 5, pp. 285- 287.

[2] K..M. Singh, L.S. Singh, A.B. Singh and K.S. Devi,"Hiding Secret Message in Edges of the Images", Information and Communication Technology, 2007. ICICT '07, pp. 238-241.

[3] Ahn, L.V. and N.J. Hopper, 2004. Public-key steganography. In Lecture Notes in Computer Science.Vol. 3027 / 2004 of Advances in Cryptology - EUROCRYPT 2004, pp: 323–341. Springer-Verlag Heidelberg.

[4] Namita Tiwari, Dr.Madhu Sandilya and Dr. Meenu Chawla, " Spatial Domain Image Steganography based on Security and Randomization ", (IJACSA) International Journal of Advanced Computer Science and Applications ,Vol. 5 No. 1, 2014.

[5] G.S.Sravanthi, B.Sunitha Devi, S.M. Riyazoddin and M.Janga Reddy, " A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology, Vol. 12 (2012).

[6] M. Bashardoust, G. B. Sulong, and P. Gerami, "Enhanced LSB image steganography method by using knight tour algorithm, vignere encryption and LZW compression", International Journal of Computer Science Issues, vol.10, no.2, pp.221-227, 2013.

[7] R. S. Gutta, Y. D. Chincholkar, and P. U. Lahane, "Steganography for two and three LSBs using extended substitution algorithm", ICTAT Journal on Communication Technology, vol.4, no.1, pp.685-690, 2013.

[8] A. Gangwar, and V. Srivastava, "Improved RGB-LSB steganography using secret key", International Journal of Computer Trends and Technology, vol.4, no.2, pp.85-89, 2013.

[9] W. Hong, T. S. Chen, and C. W. Luo, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system", The Journal of Systems and Software, vol.85, pp.1166-1175, 2012.

[10] Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, and C.P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing", Information Sciences, vol.191, pp.214-225, 2012.

[11] A. Ioannidou, S. T. Halkidis, and G. Stephanidis, "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, vol.39, pp.11517-11524, 2012.

[12] S. Kaur, and S. Jindal, "Image steganography using hybrid edge detection and first component alteration technique", International Journal of Hybrid Information Technology, vol.6, no.5, pp.59-66, 2013.

[13] J.K.Mandal, and D. Das, "Color image steganography based on pixel value differencing in spatial domain", International Journal of Information Sciences and Techniques, vol.2, no.4, pp.83-93, 2012.

[14] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[15] Fahim Irfan et. Al.'s (2011) "An Investigation into Encrypted Message Hiding through Images Using LSB ", International Journal of EST.

[16] Gurmeet Kaur and Aarti Kochhar, “Transform Domain Analysis of Image Steganography”, IJSETT International Journal for Science and Emerging Technologies with Latest Trends 6(1), 29-37 (2013).

[17] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R.Kamath, “ A Secure Color Image Steganography in Transform Domain “, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013.

[18] M. Chaumont and W. Puech, “DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image”, 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[19] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, “Authentication of secret information in image steganography”, IEEE Region 10 Conference, TENCON-2008, November, pp. 1-6.

[20] Po-Chyi & C.-C.Jay Kuo, Fellow, IEEE(2003) “Steganography in JPEG 2000 Compressed Images”, IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, pp 824-832.

[21] Prosanta Gope, Anil Kumar and Gaurav Luthra , (2010) “An Enhanced JPEG Steganography Scheme with Encryption Technique”, International Journal of Computer and Electrical Engineering , Vol.2.No.5, pp924-930.