# LWT BASED ENCRYPTED PAYLOAD STEGANOGRAPHY

H S Manjunatha Reddy[1], N Sathisha[2], S Deepa[2] and K B Raja[3]

[1]Department of ECE, Global Academy of Technology, Bangalore, India
[2]Department of ECE, Govt. S K S J Technological Institute, Bangalore, India
[3]University Visveswaraya College of Engineering, Bangalore, India.
manjunathareddyhs@rediffmail.com, raja_kb@yahoo.com

**Abstract:** Steganography is used in covert communication for transportation of secrete information. In this paper we propose LWT based Encrypted Payload Steganography (LEPS). The payload is segmented into two parts say block 1 and block 2. The LWT is applied on block 2 to generate four sub bands. Payload block 1 is retained in the spatial domain itself. The values of approximation band coefficients of block 2 and spatial domain intensity values of block 1 are compressed. The LWT is applied on cover image to generate wavelet sub bands and considered only diagonal sub bands (XD). The XD band is decomposed into three parts. The key values are embedded into first part of XD band. The compressed payload is embedded in second and third blocks of XD adaptively. The payload can be retrieved at the destination by adapting reverse process of embedding. It is observed that the values of PSNR and capacity are better in the case of proposed algorithm compared to existing algorithm.

**Keywords**: Steganography, Lifting wavelet transforms, Payload, Cover Image, Adaptive

## INTRODUCTION

Steganography is a method of information hiding techniques [1] for secure communication and to protect confidential data while transferring by concealing the existence of information within cover image or object. It is a method of embedding the secret information into an unrelated plain digital media, such as an image, video or audio files and then transmitted to the intended recipient without attracting illegal observers' attention, so that the recipient can get the messages secretly. The Steganography consists of cover image, informationand keyword. Cover image is a carrier in which the information is embedded for the purposes of hiding the presence of the message. Information is the data, that the sender wishes to retain it confidential and it can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. The keyword ie., stego key, which ensures that only receiver who knows the corresponding decoding key will be able to extract the message from a cover image. The cover image with the secretly embedded message is called the stego image.

## LITERATURE SURVEY

Marghny Mohamed et al., [2] have proposed a scheme with a genetic algorithm to solve the problem of hiding important data in the rightmost k LSBs of the cover image when k is large. However, it works poorly if k is greater than 3 because the number of all possible keys permutations will grow exponentially as k increases. Tanmay Bhattacharya et al., [3] have proposed DWT based Steganographic technique. The cover image is decomposed into four sub bands LL, LH, HL and HH using DWT. The secret images are embedded within the HL and HH sub bands respectively. The secret images which are embedding are dispersed within each band using a pseudo random sequence and a Session key. The Secret images are extracted using the key and the size of the images. ElhamGhasemi et al., [4] have present novel Steganography scheme using Wavelet Transform and Genetic Algorithm. They employ a genetic algorithm based mapping function to embed data in 4x4 blocks of Wavelet Transform coefficients on the cover image. The optimal pixel adjustment is performed after embedding the message and also to obtain an optimal mapping function in order to reduce the error difference between the cover and the stego image.

RajkumarYadav et al., [5] have proposed a method for data hiding using gray level images in spatial domain. This technique uses 5th, 6th and 7th bits of pixel value and if decimal value of 5th, 6th and 7th bits are 0, 2, 4 or 6 then insert 0 at these locations and if not then add or subtract 1 at that location for making decimal value of 5th, 6th and 7th bit 0, 2, 4 or 6 for insertion of 0. Similarly, insert 1 at a pixel location if decimal value of 5th, 6th and 7th bit at that location is 1, 3, 5 or 7. If decimal value of 5th, 6th and 7th bit at that location is not 1, 3, 5 or 7 then we add or subtract 1 at that location for making decimal value of 5th, 6th and 7th bit 1, 3, 5 or 7 for insertion of 1. For retrieval of message, again check decimal value of 5th, 6th and 7th bit. If the decimal value of 5th, 6th and 7th bit at the selected location is 0, 2, 4 or 6, then 0 is the message bit else message bit is 1. Wien Hong and Tung-Shou Chen [6] propose a data hiding method based on Pixel Pair Matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit.

## PROPOSED EMBEDDING MODEL

The flow chart of the proposed LEPS Embedding algorithm is as shown in Figure 1.

### Cover image

The cover image of size (a*a) is resized to Mc x Nc to attain optimum PSNR. Where Mc = Nc = n * p
n is the even value and P is the number of rows in the payload.

### Payload

It is the secret image which is to be embedded in a cover image. If 'P' is the number of rows in the payload and it must be an even number. The size of the payload is (P*1.5P) as shown in Figure 2.

### Lifted Wavelet Transform 2 (LWT2) using dB2

Daubechies wavelet transform is applied to the resized cover image to generate XA, XV, XH and XD bands. The XD band is divided into three parts say XD0, XD1 and XD2 of sizes (Mc/4 x Nc/4), (Mc/2 x Nc/4), and (Mc/4 x Nc/4) respectively as shown in Figure 3 to accommodate the bits of spatial and transformed domain payload properly. Daubechies wavelet gives a good precision of 4 digits after decimal point.

### Segmentation

Original payload of size P*1.5 P decomposed into two blocks viz., (i) the first block of size is original rows of payload and 1/3rd of columns of pay load (P*0.5P) and (ii) the second block of size the original rows of pay load and 2/3rd columns of original payload (P*P).
Payload Block 1: The payload image sixe of P*0.5P is retained in the spatial domain itself.

Payload Block 2: The payload image size of P*P is converted into wavelet domain using LWT2 Harr wavelet to generate four sub bands say XA, XV, XH and XD.

### Lifted Wavelet Transform 2 (LWT2) using Haar

The Harr wavelet is applied to payload block 2 to generate four sub blocks XA, XV, XH and XD. The low frequency band XA coefficients are considered to be embedded into cover image.

### Compression on payload

The pixel intensity values of payload block 1 and XA coefficients of payload block 2 are divided by the maximum intensity value 255 to reduce actual values and compute percentage of obtain values to generate percentage value between 0 and 100. The percentage values are scale down further by dividing the values by

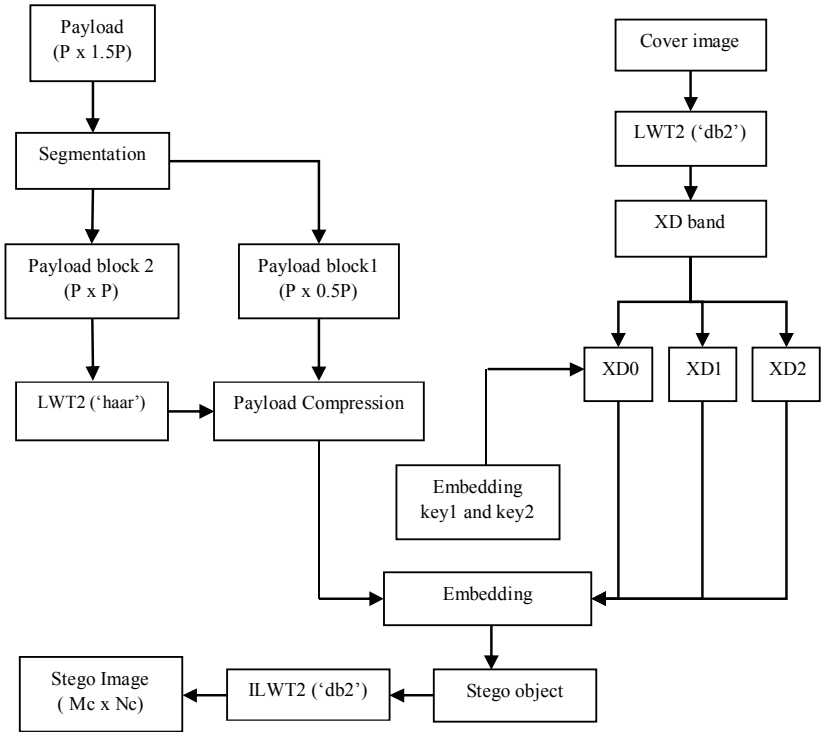


**Fig 1:** Embedding flowchart of proposed LEPS algorithm

15 to generate values between 0 and approximately 7. The maximum scale down value 7 is represented by only 3 bits in binary. The fractional part of each scale down values is also considered and embedded in to cover image. The two level scales down improve the security level to payload and also the 8 bit binary of each pixel is converted into 3 bits which improves capacity. The two keys are used viz., (i) Key1 for first level scale down value 255 and (ii) Key2 for second level scale down value 15. As each pixel of payload are represented by only 3 bits in binary instead of 8 bits in binary for original payload. All 3 bits can be embedded in to the cover image hence retrieval of payload quality improves.

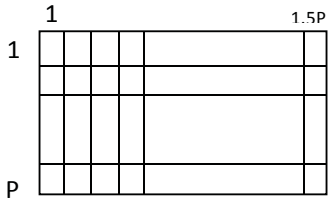


**Fig2.** Payload dimensions

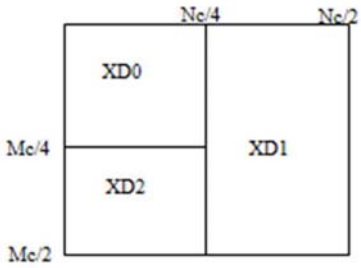


**Fig3.** Regions of XD0, XD1 and XD2 of XD band

**Embedding Algorithm**

The Key1 and Key2 values are embedded into first 3 coefficients of XD0 of cover image by replacing 3 LSB bits in each pixel. The payload blocks 1 pixel with 3 bits for integer parts are embedded into XD1 band of cover image by replacing LSBs of each coefficient. The payload block 2 coefficients with 3 bits are embedded into XD2 band of cover image by replacing LSBs of each coefficient. The embedding process is performed based on size of the cover image

(i) If n = 2, ie., the size of the cover image is 2P*2P, then embed payload continuously in every pixels of cover image.

(ii) If n = 4, ie., the size of the cover image is 4P*4P, then embed payload in alternative pixels of rows and columns.

(iii) If n = 6, ie., the size of the cover image is 6P*6P, then embed payload in alternative pixels with a gap of two rows and two columns.

**Inverse Lifted Wavelet Transform 2 (ILWT2)**

Inverse LWT2 is applied on stego object to convert into spatial domain stego image.

**ALGORITHM**

*Problem definition:* The encrypted payload in spatial and transform domain is embedded into cover image to generate stego image for secure communication.

*Assumptions:*

(i) Both cover and payload objects are gray scale images with different dimensions.

(ii) The stego image is transmitted over an ideal channel.

The objectives are: (i) To increase capacity, (ii)To increase PSNR

The embedding algorithms of LEPS is shown in Table 1

| Input: Cover image, payload, Output: Stego image |
|---|
| 1.Apply LWT2 using dB2 wavelet on the cover image. |
| 2. XD band is segmented into into XD0 (Mc/4 x Nc/4), XD1 (Mc/2 x Nc/4) and XD2. (Mc/4 x Nc/4). |
| 3. Key1 and key2 is embedded into XD0. |
| 4. Payload is segmented into block 1 (P x 0.5P) and block 2 (P x P). |
| 5. Apply LWT2 (Harr) on block2. |
| 6. Payload block1 pixel values and payload block2 XA coefficient values are divided by key1 and 2 and multiply by 100 to compress eight bits of payload to three bits. |
| 7. Payload bits of block1 and block2 are embedded into XD1 and XD2 to generate stego object. |
| 8. Apply ILWT2 (dB2) on stego object to generate Stego image in spatial domain. |

**Table 1:-** Embedding algorithm of LEPS

**PERFORMANCE ANALYSIS AND DISCUSSIONS**

Cover image (CI) of different sizes and formats viz., JPEG, PNG, TIFF, GIFF and BMP images are considered for performance analysis. The payload (PL) Pepper is embedded into the cover image Barbara to generate stego image Barbara.

The Table 2 gives PSNR and capacity values for different sizes of cover image and payload of size 256 x 384. The value of PSNR increases as the size of the cover image increases but capacity decreases.

| Cover image (JPEG) | PSNR (stego to cover Image) | Capacity (bpp) |
|---|---|---|
| 512 x 512 | 48.4534 | 0.375 |
| 1024 x 1024 | 54.2509 | 0.09375 |
| 1536 x 1536 | 57.6576 | 0.04166 |
| 2048 x 2048 | 60.0901 | 0.02343 |

**Table 2** PSNR for different sizes of cover image

Table 3 shows the comparison of PSNR for the existing Pixel Bit Manipulation for Encoded Hiding - An Inherent stego (BMEH) [7] and the proposed algorithm LEPS. It is observed that the PSNR is higher in the case of proposed algorithm compared to the existing algorithm for all image formats due to the payload splitting and the use of Daubechies wavelet transforms.

| Method | Size | PSNR |
|---|---|---|
| Existing method [7] | CI: 128 * 128<br>PL: 64 * 64 | 40.719 |
| proposed method (LEPS) | CI: 512 * 512<br>PL: 256 * 384 | 48.453 |

**Table 3**.Comparison of PSNR of proposed algorithm with existing method [7]

## CONCLUSION AND FUTURE WORK

The Steganography is an effective means of data hiding that protects data from unauthorized persons. In this paper the Steganography technique LEPS is proposed. LWT2 (dB2) is applied on cover image to generate diagonal sub bands say XD0, XD1 and XD2. The payload is segmented into two blocks of different sizes. The wavelet coefficients of block 2 and spatial domain block 1 are compressed. The key1 and key2 are embedded into XD0 band. The three binary bits of payload block 1 and block2 are embedded adaptively based on cover image size into XD1 and XD2 of cover image respectively by replacing three LSB bits to generate stego object. The ILWT2 (dB2) is applied on stego object to create stego image in spatial domain. It is observed that values of PSNR and capacity with different image formats are improved in the proposed technique compared to the existing method. In future Dual Tree Complex Wavelet Transform (DTCWT) can be used with different compression techniques.

## REFERENCES


[1]Shouchao Song, Jie Zhang, Xin Liao, Jiao Du and Qiaoyan Wen, "A Novel Secure Communication Protocol Combining Steganography and Cryptography*," Procedia* Engineering 15, pp. 2767–2772 (2011).

[2]Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, "Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation," International Arab Journal of e-Technology, vol. 2, no. 1, pp.11-17, January (2011).

[3]Tanmay Bhattacharya, NilanjanDey and S R BhadraChaudhuri, "A Novel Session Based Dual Image Encoding and Hiding Technique Using DWT and Spread Spectrum," International Journal on Computer Science and Engineering, vol. 3, no.11, pp.3510-3517, (2011).

[4]ElhamGhasemi, JamshidShanbehzadeh and NimaFassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", International Multiconference of Engineers and computer scientist, vol.1, (2011).

[5]RajkumarYadav, Ravi Saini and Kamaldeep, "A New Image Steganography Approach for Information Security Using Gray Level Images in Spatial Domain," International Journal on Computer Science and Engineering, vol. 3, no. 7, pp.2679-2690, (2011).

[6]Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method using Adaptive Pixel Pair Matching," IEEE Transactions on Information Forensics and Security, vol.7, no.1, pp.178-184, (2012).

[7]Siva Janakiraman, Anitha Mary, JagannathanChakravarthy, RengarajanAmirtharajan, K.Thenmozhi and John BoscoBalaguruRayappan, "Pixel Bit Manipulation for Encoded Hiding - An Inherent stego," International Conference on Computer Communication and Informatics, (2012).