Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 117 (2018) 50386-50388

ISSN: 2229-712X

# A Survey on Image Hiding Scheme Using Haar DWT, Data Compression and Encryption Techniques

Shrikant P Mudnur, Satish Raj Goyal and K.N.Jariwala

Department of Computer Engineering, National Institute of Technology, Surat, India 395007.

**ARTICLE INFO**

**Article history:**

Received: 1 March 2018;

Received in revised form:

27 March 2018;

Accepted: 7 April 2018;

**Keywords**

Steganography,
Haar Wavelet Transform,
Encoding,
Encryption,
PSNR,
RGB.

**ABSTRACT**

Steganography techniques are helpful to hide the secret information in cover media and thus aid in enhancing the security of sensitive data during transmission and storage. Applying discrete wavelet transform helps to convert the image to the frequency domain. Haar wavelet transform is used to obtain the low frequency approximate (LL) detail and three high frequency detailed (LH, HL, HH) details. As the detailed sub bands have less sensitive information these are used for embedding the secret information. The secret information in the form of image can be reduced to one fourth size using haar transform. Encoding methods can be used to reduce the size of the image and encrypting the compressed data with the known key can help to enhance the security. The quality of stegoimage is measured using PSNR. The hiding capacity can be measured to compare with the other techniques of steganography.



## I. Introduction

As the use of digital media has increased in this modern era, the threats and attacks to the digital information has increased. Hence it has become a great essence to transfer and store the data with higher security.Steganography or cryptographic techniques can be used to transfer and store the data with better security[2].Steganography is the art or technique to hide the data in a cover media so that the middle person or attacker does not notice the secret information that is hidden in the cover media. Every steganography techniques consist of three files, the file consisting of secret information, the cover media in which secret information will be hidden and the stegofile which consist of the secret information hidden in the cover media file. In the cryptography techniques rather than hiding the information in the cover media the readable information is converted into the cipher or unreadable format using a secret key.Cryptography techniques may provoke the middle person or attacker to decipher the unreadable format as it gives a hint that a secret information is being transferred or being stored.Combining both steganography and cryptography methods helps to improve the level of security as in case the hidden information from the stegofile is extracted from the attacker still the used cryptography technique provides an additional layer of security.

The strength of the steganography techniques mainly depends on the ability of the stegofile to provide security so that the attacker finds it a challenging and difficult to extract secret information from the cover media in case the attacker has found that the image consists of some secret information. Secondly the hiding capacity of the cover media is important as the main goal is to hide maximum secret information without much distorting the cover image.Thirdly the stegofile should have less distortion as increase in distortion gives an hint that secret information is hidden in the cover image.

## II. Haar DWT

Discrete Wavelet Transform(DWT) techniques can be used to hide the secret information in the cover image. There are many wavelet transforms like haar wavelet transform, integer wavelet transform, daubechies wavelet transform, Morlet wavelet transform and so on. Haar wavelet transform can be used to decompose the discrete signal into the approximation component and detail component. When we apply Haar wavelet transform the image can be divided into the four sub bands LL, LH, HL, HH and the most of the image information is present in LL sub band [1].

Each of these sub bands have one fourth of the size of the original image. As LH, HL, HH sub bands consist of lesser information hence these sub bands can be used to hide the secret information. Applying Haar wavelet transform on the sub bands is equivalent to the second level haar wavelet transform on the original image and can help to hide more secret information without much distortion of the cover image. Fig.1 shows Haar DWT applied on the image to obtain one approximate and three detailed sub bands.

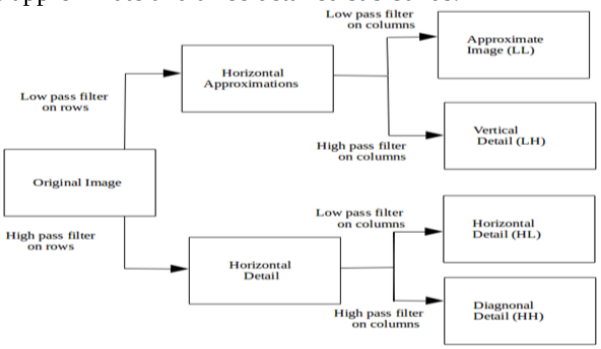


**Fig 1. Two-D Haar Discrete Wavelet Transform.**

## III. Data Compression and Encryption

Before embedding the secret information it would be helpful to compress the secret information and encrypt using

the known key.There are many techniques available for compressing the data. Data compression can be classified as lossy or lossless techniques. In the lossy data compression techniques the compressed data would not be extracted completely after decompressing the data.JPEG image compression is lossy compression technique where non essential information is rounded off.Lossless image compression techniques can be used to extract the complete data after decompression. Run length encoding, Huffman coding and arithmetic coding are some of the examples of lossless data compression techniques aditional geometric and appearance based methods with high accuracy.

Encryption techniques can be used to convert the readable information into unreadable or cipher format. Encryption methods can be classified as private or symmetric key and public key encryption methods. In private key method the same key is used for encrypting and decrypting. In public key method the encryption of the message can be done by using the public key and only the receiving party can decrypt the information using the private key.

**IV. Related Work**

Nikhil Simha H.N. et al. [1] proposed the method to hide the secret image in the cover image by using haar wavelet transform and modified LSB technique.Secret image and cover image of same size were taken and gaussian filter was applied to remove the noise.If the cover image and secret image were of different size then resizing of the cover image can be done. Two level haar wavelet transform was applied on both cover image and secret image to obtain the LL, LH, HL, HH bands. As LL band consists of maximum information of the image hence neglecting the remaining three bands(LH,HL,HH)only LL band was used for stegnography purpose. The four least significant bits of LL band of cover image is replaced by the four most significant bits of the LL band of secret image.As the LL band is one fourth of the original image size hence the stgoimage is reduced by one fourth of the size which helps in faster transmission. At the receiver side the four LSB bits of each pixel of the stego file are extracted and appended with four zeros at the right end to form the pixel value of the secret information. To enhance the security pre shared key which is known by both sender and receiver is used to determine the pixel values of the secret image.

Janki Jasani et al. [2] proposed the stegnographic technique based on coefficient details of the haar wavelet transform. Decimal part of the $1^{st}$ level haar transformation can consist of two values 0.0 or 0.5, so at the first level one bit can be hidden. Similarly at the $2^{nd}$ level four possible decimal values are 0.0, 0.25, 0.5 and 0.75 so two bits can be hidden. In third level there are eight possible decimal values so three bits can be hidden.Using odd and even type of integer part one additional bit can be hidden. Arithmetic coding is used for compressing the secret image which helps to improve the hiding capacity and the security level. This technique is based on the fact that the coefficients at the same position of the four sub bands are related and if changes are made in the coefficient values at one of the sub band then change in coefficient values has to be done in the remaining three sub bands so as to obtain integer value after applying inverse discrete wavelet transform.

M.Gomathymeenakshi et al.[3]proposed the method which involves compression of plain text using arithmetic coding and hiding of the compressed data in the cover image. With the help arithmetic coding method the floating point number is found which lies in the range from 0.0 to 1.0. The floating point number is converted to the binary number. If the floating point number is 0.2801 then the corresponding binary code would be 0010 1000 0000 0001.The binary code is divided into two bits chunks and hidden in the cover image by replacing the two LSB bits of the pixels in the cover image. At the receiver side two LSB bits of the stegoimage are extracted and converted into floating point number by considering every time four bits. By using the floating point number the plain text can be extracted.

Saeid Fazli et. al. [4] proposed the method to hide the LL band of secret image into the RGB components of the color image. Using one level haar wavelet transform LL band of the secret image was found. Here the colored cover image of dimension 512 X 512 and gray secret image of dimension 180 X 180 was considered for steganography purpose. After applying haar transform LL band of dimension 90 X 90 is obtained which is embedded in selected area of the cover image. Six most significant bits of LL band are considered for embedding purpose.Two pixels of color image are required to hide one pixel of gray image. In one pixel of color image 3 bits are hidden corresponding to one bit for each RGB component. For extracting the secret information, from the selected area each pixel is taken and three bits for each pixel is extracted (one bit for each RGB component). From two consecutive pixels six bits can be extracted and two zero bits can be appended at LSB position to form the 8 bit pixel value for the gray secret image. This procedure is continued till all the pixel values are extracted. The security level is improved by using the random matrix which has to be known by both sender and receiver.

Punam Bedi et. al. [5] presented a method to hide secret information using 2 level haar wavelet transform. Initially using 1 level haar DWT four subbands CA, CH, CV, CD are obtained. Further haar wavelet transform is applied to CH, CV, CD components to obtain the 12 bands CHA, CHH, CHV,CHD from CH component, CVA, CVH, CVV,CVD from CV component and CDA, CDH, CDV, CDD from CD component. Based on the secret message size number of LSBs to be used for embedding is determined.The order of the blocks used for hiding in case the large secret message is CDD,CDH, CDV, CHD,CVD, CHH, CHV, CVH,CVD. After embedding the complete secret information meta data which has information about total number of components used and number of bits used in the last component is stored in CDAD component which can be obtained by applying haar transform on CDA band. Security is enhanced by embedding secret information in zig zog order of the component rather than in linear order.

Ajaya Shrestha et al. [6] proposed the method to hide secret information in LH and HL bands using 4 LSB Technique.Initially the cover image is converted into four sub bands using wavelet transform. The four lower significant bits of secret image was hidden in the four LSBs of one of the band selected from LH and HL.The four most significant bits of secret information was hidden in the four LSBs of the other band.The comparison was done between the Daubechius and Haar wavelet transform.The reverse steps of embedding can be used to extract the secret image.

Martin Broda et al.[7] proposed the method to hide secret information by using YCbCr color model.As chrominance component is less sensitive to human eye, chrominance red component is used for hiding the secret information.The secret information is encrypted using advanced encrypted

**Table 1. Comparison between the methods.**

| Paper | Secret message | Cover image | HDWT Level | PSNR (range) | Data compression technique | Encryption Technique |
|---|---|---|---|---|---|---|
| [1] | 256x256 (gray) | 256x256(gray) | 1 | 69.68-75.25 | | Pre shared key to determine pixel value |
| [2] | 384x384 (gray) | 384x384(gray) | 1,2,3 | 41.597-41.730 | Arithmetic encoding | |
| [3] | | | | | Arithmetic encoding | |
| [4] | 180x180 (gray) | 512x512(RGB) | 1 | 63.2214-63.2613 | | Random matrix |
| [5] | Text messages( 1% to 21.46% of cover image) | 512x512(gray) | 2 | 25.723-52.646 | | Zig Zog order of subcomponent |
| [6] | 128x128 (gray) | 512x512(gray) | 1 | 12.12-26.92 | | Xor operation with secret key |
| [7] | 4096-49004 bits | 256x256 or 512x512 (YCbCr) | 1 | 47.31-52.02 | | AES |

standard (AES) cryptography method.After encryption message is converted into binary form and hidden in the LSBs of LL,LH,HL bands of Cb component.After embedding the message using IDWT Cb' component is obtained. Image is converted back to RGB model and thus stegoimage is formed. The secret information can be obtained by applying the reverse steps.

## V. Comparison

The following table gives the comparison between the different methods based on the type of the secret message and cover image. Level of haar discrete wavelet transform applied and the possible PSNR range in different methods is compared. Data compression and encryption techniques used in various methods is also compared.

## VI. Conclusion

Combining the techniques of steganography, data compression and encryption can yield the better security for communicating the secret information. In this paper, related work on image steganography using haar wavelet transform, data compression and encryption is reviewed. Comparison between various proposed methods is done based on type of secrert message and cover image used, HDWT level, PSNR, data compression and encryption techniques used.

## Acknowledgment

The Authors would like to thank Sardar Vallabhbhai National Institute of Technology for supporting this study.

## References

[1]. Nikhil Simha H.N, Pradeep M. Prakash, Suraj S. Kashyap, Sayantam Sarkar. "FPGA Implementation of Image Steganography using Haar DWT and Modified LSB Techniques". 2016 IEEE International Conference on Advances in Computer Applications (ICACA).

[2]. Janki Jasani, Sarita Visavalia. "A secure and high capacity image hiding scheme using DWT and arithmetic coding". 978-9-3805-4421-2/16/ 2016 IEEE .

[3]. M. Gomathymeenakshi, S. Sruti, B. Karthikeyan, Meka Nayana. "An Efficient Arithmetic Coding Data Compression With Steganography". 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013).

[4]. Saeid Fazli, Sajad Gholamrezaei, and Amir Bazrafshan. "Advanced Wavelet Based Steganography for Colored Images".2010 International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 IEEE.

[5]. Punam Bedi, Veenu Bhasin, Tarun Yadav. "2L-DWTS – Steganography technique based on second level DWT". 2016 Intl. Conference on Advances in Computing,Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India. 2016 IEEE.

[6]. Ajaya ShresthaDr. Arun Timalsina."Color Image Steganography Technique Using Daubechies Discrete Wavelet Transform".2015 9th International Conference on Software,Knowledge,Information Management and Applications(SKIMA).

[7]. Martin Broda, Valdimir Hajduk, Dusan Levicky. "Image Steganography Based on Combination of YCbCr color model ".57th international symposium ELMAR-2015,Zadar, Croatia.

[8]. Neha Sikka."Lossless Image Compression Technique using Haar Wavelet and Vector Transform".RAINS-2016 IEEE.

[9]. Mohammad Reza Dastjani, Farahani Ali Pourmohammad "A DWT Based Perfect Secure and High Capacity Image Steganography Method".2013 International Conference on Parallel and Distributed Computing,Applications and Technologies.

[10]. Gabriel Bugár, Vladimír Bánoci, Martin Broda, Dušan Levický,Ervin Mikó."Blind Steganography based on 2D Haar Transform".55 International Symposium ELMAR-2013, 25-27 September 2013, Zadar, Croatia.