International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

A Novel Steganography Technique USING Same Scale Wavelet

H S Jayaramu[1], Dr K B Shivakumar[2], Srinidhi G A[3], Dr A K Goutam[4],

[1]Research Scholar, Mewar University, India
[2&3]Department of TCE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India
[4]Principal, S D College of Engineering, Muzzaffarnagar, India

Abstract

Steganography has evolved as one of the standards for digital data security along with digital watermarking. Steganography is the technique for storing any digital object called payload behind another digital object called cover. One of the most important requirement for steganography is that the length of the cover must be very high in comparison to payload such that the effect of noise is minimized after the steganography process. But this becomes a difficult constraint for transmission of embedded or stego data over internet or any network.

Therefore this work presents a unique solution for hiding an image behind another image of the same scale and size. The idea can be perceived at achieving image steganography of 1BPP. The technique relies on spectral decomposition of the image using wavelet transform followed by a normalization process of the payload. These normalized values of downsampled payloads are embedded into non normalized cover. The resultant image does not present any visual dissimilarity and is proven through high PSNR and low MSE. As there are no other techniques proposed in this direction for same scale steganography, we believe that our work lay strong foundation in this direction.

Keywords: Digital Steganography, Wavelet, Hiding Image Behind Image, Same Scale Steganography

1. INTRODUCTION

An image Steganography system consists of two modules: the embedding module and the retrieval module. The embedding module is used at the sender's end where the payload is embedded into the cover image to derive stego-image using any one of the Steganographic techniques, whereas the retrieval module is used at the receiver end to extract the payload from the stego-image by using inverse Steganographic technique as shown in the Figure 1.1.

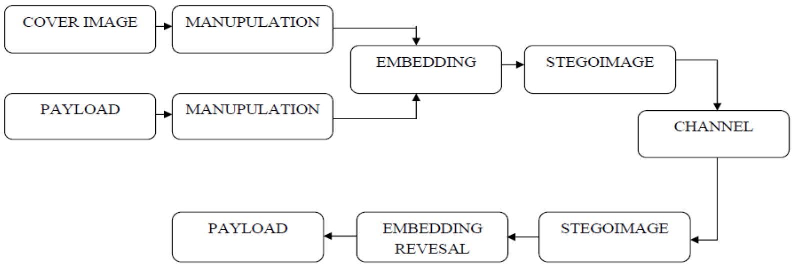


FIGURE 1: Block diagram of Steganography Model

At the transmitter end, cover image and the payload are applied to the stego-system encoder to generate stego image using certain steganographic techniques. At the receiver end stego system decoder extracts the payload by identifying the key which may be used between the transmitter and the receiver to provide security against intelligent attackers.

1. Cover image: It is an object consisting of the signal stream or data file as a carrier of the embedded object. The most important property of a cover image is the amount of data that can be embedded into it, without changing the noticeable statistical properties of the cover image. Good cover images are (i) grayscale images (ii) uncompressed images containing large number of colors (iii) landscapes and portraits. JPEG format images are very poor choice for cover images because small modifications in cover image can be detected easily.
2. Payload: It is the size of the data i.e., (signal, stream or file) embedded in the cover image.
3. Stego-object: It is a unified object /image obtained from the combination of the cover object and payload.
4. Capacity: It is the amount of data that can be hidden in the cover image without destroying the statistical properties of the cover image. The capacity depends on the type of cover image used. The capacity is given by bits per pixel (bpp) by the Equation 1.1.

$$\text{bpp} = \frac{\textit{nuber of bits embedded in cover image}}{\textit{total number of pixel in cover image}} \qquad (1.1)$$

5. Robustness: The amount of modification that can be withstood by the cover medium without being destroyed completely is defined as robustness. It is the extent of modification that can be tolerated by the stego-object without destroying the hidden image under attacks.
6. Security: It can be considered as safeguarding or protecting information of the payload in the cover image. It is the extent of inability of adversary to detect hidden images accessible only to the authorized user. The quality factor can enhance the security of the image. A steganographic image is perfectly secure when the statistical data of the cover and stego images are identical.
7. Imperceptibility: It is the extent of in distinguishability of the original cover image and stego image. The measure of this can be obtained by the PSNR equation. Though it is not an accurate measure, it can give satisfactory results.
8. Wavelet: Wavelet is a small wave and its analysis is about analyzing a signal with short duration finite energy functions.
9. Wavelet Transform: Wavelet transform provides the time-frequency representation. The wavelet transform of an image is created by repeatedly filtering the image coefficients on a row-by-row and column-by-column basis.
10. Approximation Band: It is the band of an image having the low frequency coefficients in the wavelet domain.
11. Detail Band: It is the band of an image having the high frequency coefficients in the wavelet domain.
12. Mother Wavelet: A mother wavelet, (x) is a prototype that can be scaled and translated. A mother wavelet has to satisfy the condition given below.

$$c_{i,j} = \int_{-\infty}^{\infty} f(x)\psi_{i,j}(x)\,dx \qquad (1.3)$$

$$f(x) = \sum_{j,k} c_{j,k}\psi_{j,k}(x) \qquad (1.4)$$

The wavelet function of a signal, f(x) can be computed using the following analysis and synthesis formulae:

$$\psi(t) = \begin{cases} 1 & \text{if } 0 \le t \le 1/2 \\ -1 & \text{if } 1/2 \le t \le 1 \\ 0 & \text{otherwise} \end{cases} \qquad (1.5)$$

13. Haar Wavelet: It is a function which consists of a short positive pulse followed by a short negative pulse, which provides orthogonality decomposition of an image signal.
14. Detectability: Identification of the Steganographic image visually or by computer analysis is called detectability. The challenge of steganography is to hide the information which cannot be identified by any means.
15. Histogram: It shows the distribution of intensities of an image. It is the plot of Number of pixels and intensity of the pixel values.
16. Distortion: The distortion of the cover image depends on the size of the pay- load. Larger the payload higher is distortion of the stego image.
17. *Mean Square Error (MSE):* It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE and is calculated using Equation 1.6.

$$\left.\begin{array}{l} mse1= abs\ (uint8\ (stego\ image)-uint8\ (hidden\ image)) \\ MSE=mean\ (mean\ (mse1.*mse1)) \end{array}\right\} \qquad (1.6)$$

18. Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage, is calculated using Equation 1.7

$$PSNR - 10log_{10}\frac{255^2}{MSE}db \qquad (1.7)$$

19. Pixel: It is an element of the image which is not further divisible from the image analysis point of view. A pair of adjacent pixel values is called Pixel Pair.
Some of the Steganographic techniques are: Least Significant Bit (LSB) embedding, Masking and filtering, Mapping method, Frequency Domain Embedding, Spread spectrum, Color Palette Technique, Genetic Algorithm based Steganography and Multi Transform based Steganography.
1. LSB embedding: In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Most Significant Bits (MSB) of the image to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover-object are replaced.
2. Masking and Filtering: In masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the human eye. This is mainly used in watermarking techniques.
3. Mapping method: In this method the pixels of the cover image is altered based on some mathematical function selected at the transmitter which has to be known by the receiver to retrieve the hidden data in the image pixels. This method has small capacity compared to other technique.

4. Frequency Domain Embedding: In this technique the image is transformed into frequency domain using, Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Wavelet Transforms and the payload is embedded in the least significant frequency coefficients and it is again transformed into spatial domain and transmitted to the destination. The reverse process is followed at the destination to retrieve the payload.
(a) Fast Fourier Transform (FFT): In FFT, the message is hidden in the most significant coefficients of the data stream. This is better than hiding data in the least significant coefficients, since it is the most likely to be modified by compression .
(b) Discrete Cosine Transform (DCT): In DCT method, the image is first transformed to frequency domain and then separated into spectral sub-bands. The spectral sub-bands are classified as High and Low frequency components. The discrete cosine coefficients of hidden image are embedded into the cover image such that the distortion is minimum and no significant changes in the statistical features of the stego image with respect to cover image occur . DCT is used in the JPEG images to transform successive pixel blocks of the image from spatial domain to frequency domain.
(c) Discrete Wavelet Transformation (DWT): In DWT method, the image is decomposed based on frequency components into detailed and approximation bands, also called the sub-bands. Detailed band contains vertical, horizontal and diagonal bands. The total Information of the image is present in the approximation band. The payload is normally embedded in the detailed band and sometime in the approximation band . Wavelet transforms often have floating point coefficients. Thus, when the input data consists of sequence of integers (as in case of image), the resulting filtered output no longer consists of integers, which does not allow perfect reconstruction of the original image. As a result, the inverse wavelet transform becomes lossy. However, with the introduction of Wavelet Transforms that map Integers to Integers (IWT), the output can be completely characterized by integers and exact decompression of the original data is achieved [13].
5. Spread Spectrum Embedding: In this technique the pay load is spread over a wide frequency bandwidth using pseudorandom noise sequence .
6. Color Palette Embedding: The color intensity levels are quantized into a number of centroids known as initial centroids. The cover image pixels are clustered around the corresponding initial centroids to derive new centroids. The set of new centroids constitute the color palette which is used at the receiver to extract the payload. The payload is embedded into the color palette as the index of the pixel position around the centroids.
7. Genetic Algorithm based Steganography: Genetic Algorithm (GA) is used to generate many stego-images. One of these which give least statistical evidence of hidden data is chosen as the optimal stego-image.

2. LITRATURE REVIEW

Nan-I Wu and Min-Shiang Hwang [1] have done a survey of the existing Steganographic techniques and discussed the requirements of stego systems, in various image formats like gray scale, JPEG, binary and Pallet images. They have summarized various spatial-domain hiding techniques like LSB, PVD and MBNS and made a comparison of the systems. Some suggestions regarding future research and development are made.
Cachin [2] has proposed a model of steganography based on information theory by interpreting the adversary's task of differentiating between cover text and stego text as
hypothesis testing problem. Relative entropy is used as a quantitative measure of a stego systems security. The universal stego system that needs no knowledge of cover text distribution, except that it is generated from independently repeated experiments is discussed.
Neil F. Johnson and SushilJajodia [3] have discussed an overview of steganalysis technique. Some properties of information hiding techniques can help the steganalyst to infer the presence of hidden message and where to look for such hidden messages in the medium.
İsmail Avcıbaş, et al., [4] have presented a steganalysis technique for images that have been subjected to embedding by Steganographic algorithms. They have used the seventh and eighth bit planes of an image for the computation of several binary similarity measures. The correlation between the bit planes as well as the binary texture characteristics within the bit planes is used to construct a classifier that can distinguish between stego and cover images. The scheme is found to have complementary performance with other steganalysis schemes.
Young WANG et al., [5] discussed a Steganographic method based on keyword shift by borrowing the ideas from cryptographic algorithm of low key authentic degree. Shifting of sensitive keywords in the text is the master key of the method.
Bhattacharyya et al., [6] proposed a specific image based steganography technique for communicating information more securely between two locations by incorporating the idea of secret key for authentication at both ends in order to achieve high level of security.
Sarreshtedari and Ghaemmaghami.,[7] proposed a high capacity method for transform domain image steganography is and algorithm works on the wavelet transform coefficients of the original image to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding.

Elham Ghasemi et al., [8] presented the application of Wavelet Transform and Genetic Algorithm in a steganography scheme by employing a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message and the frequency domain is utilized to improve the robustness of steganography.
Safy et al., [9] proposed an adaptive steganographic technique in which the bits of the payload are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm.
Jskolka et al., [10] proposed a model to provide a perception of covert channel communication to yield a better understanding of covert channels by explore the relationship between covert channels, steganography and watermarking.
Sanjeev Manchanda et al., [11] proposed a model that present random numbers logic based steganographic methods and layout management schemes for hiding data/image into image(s). These methods and schemes can be customized according to the requirements of the users and the characteristics of data/images.
ShivaKumar et al.,[12] proposed Steganography based on Payload Transformation (SPT) which is non LSB and non transform domain technique where the cover image is segmented into 2*2 matrices and the matrix for payload embedding is considered based on the threshold value fixed by computing adjacent pixel intensity differences. The transformation matrix is obtained based on identity matrix and the payload bit pair
ShivaKumar et al.,[13] proposed a hybrid steganography (HDLS) which is an integration of both spatial and transform domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial to transform domain using DCT/DWT/FFT and embedded in a special manner, the components of cell II retained in spatial domain itself.

3. PROPOSED STEGANOGRAPHIC MODEL

3.1 ENCODING MODEL:

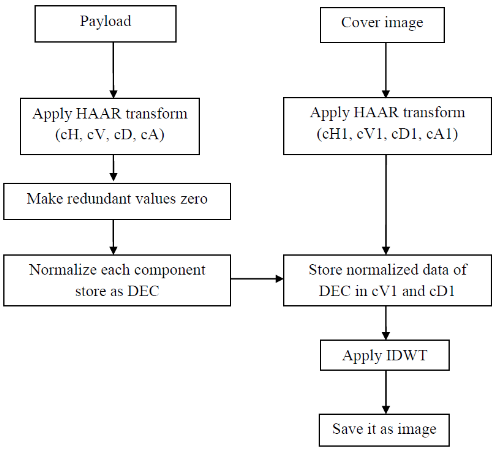

Payload
Cover image
Apply HAAR transform (cH, cV, cD, cA)
Apply HAAR transform (cH1, cV1, cD1, cA1)
Make redundant values zero
Normalize each component store as DEC
Store normalized data of DEC in cV1 and cD1
Apply IDWT
Save it as image

Figure 2 : Proposed encoding model

3.2 DECODING MODEL:

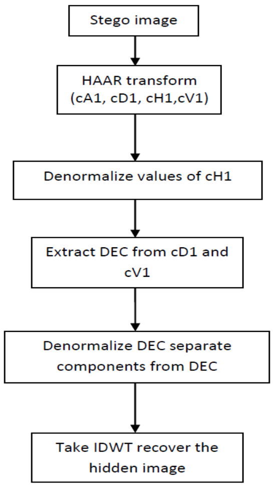

Stego image
HAAR transform (cA1, cD1, cH1,cV1)
Denormalize values of cH1
Extract DEC from cD1 and cV1
Denormalize DEC separate components from DEC
Take IDWT recover the hidden image

Figure 3 Proposed Decoding model

4. ALGORITHM

Encoding process:

1. Input the image to be hidden (img_hide)
2. Take wavelet transform with HAAR wavelet for img_hide and call the components: cA, cH, cV, cD respectively.
3. Make redundant values in the img_hide as 0.
4. Find the maximum of all the components and normalize each sub image by dividing it with the maximum values.
5. DEC is the data that contains normalized wavelet decomposed values of img_hide
6. Decompose the cover image im, into cA1,cV1,cH1,cD1 components using HAAR wavelet
7. Store the cA size,M1,M2,M3,M4 I first four values of cH1.
8. Store normalized img_hide data dec in cV1 and cD1.
9. Take IDWT of DEC1 which is nothing but idwt(cA1,cH1,cV1,cD1) and call it as S.
10. While saving the image S directly there may be loss during conversion so we normalize S.
11. Convert S to 16 bit format with the value M stored as the first pixel value. Where M=maximum (absolute(S)).
12. Calculate mean square error and calculate PSNR using PSNR=10LOG$_{10}$(255^2/MSE).

Decoding process:

1. Read the stego image to S1.
2. Extract the normalization size m from first pixel.
3. Set the first pixel value as second pixel for compensating for the losses that will incur otherwise.
4. Convert S1from unit16 scale to original scale.
5. Apply wavelet transform of variable S1and call the sub image or the components as cA1,cV1,cH1,cD1respectively.
6. Extract the data from cH1.
7. Denormalize the values.
8. Extract dec from combined data of cD1 and cH1.
9. Denormalize the dec .
10. Take IDWT of set {cA,cD,cV,cH} and call it as rec.
11. It is the recovered image

5. RESULTS:

The experiment is conducted using different formats of images, “coin”, “cameraman”, “eight”, “circuits” etc., as shown in figure below.

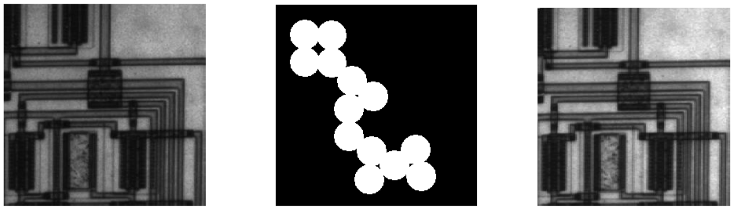
The Peak Signal To Noise Ratio is used for image quality evaluation. The PSNR for 8 bit gray level image is defined as below

$$PSNR=10LOG_{10}\,(255^2/MSE)$$

Where

mse1= abs (uint8 (stego image)-uint8 (hidden image))

MSE=mean (mean (mse1.*mse1))

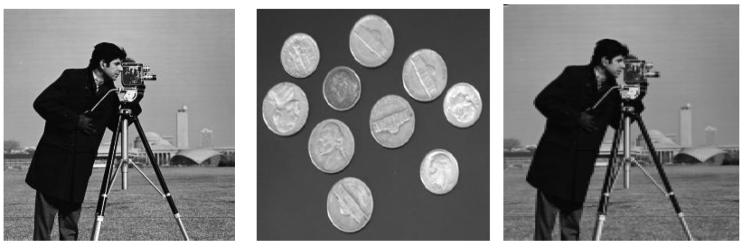


Cover image
Circuit.tif

Payload image
Circles.png

Stego image
Embedded image

Figure 4 Experimental Results (Cameraman, Coins)



Cover image
Cameraman.tif

Payload image
Coins.png

Stego image
Embedded image

Figure 4 Experimental Results (Circuit, Circles)

Table below shows the PSNR for different cover image and the payload.

Table 1: PSNR for different cover image and the payload.

Sl. no	Cover image	Payload image	size of the cover image	Size of payload image	MSE	PSNR
1	Cameraman.tif	Coins.png	256*256	300*246	2.317	44.48
2	Circuit .tif	Circles.png	272*280	256*256	0.68	49.78
3	Forest.tif	Football.jpg	447*301	320*256	1.32	45.39

6. CONCLUSION

Steganography is data hiding technique to prevent the detection of hidden messages. The message such as images, videos, audio, files, text and other computer files can be hidden inside images or other digital objects. The purpose of Steganography is not to keep others from knowing the information – it is to keep others away from thinking that the information even exists.

In our paper, we propose a unique technique for hiding payload images having same size as that of the cover image by employing Harr Transform where both the cover image and the payload are transformed using DWT and the normalized components of payload are embedded into the vertical and diagonal bands of cover image. The proposed system has got excellent PSNR with high capacity.

It is observed that the PSNR varies with the not only with the embedding technique but also on the type of images. The highest PSNR obtained is 49.78 which is considered to be best one compared to the existing techniques.

REFERENCE:

[1] Nan-I Wu and Min-Shiang Hwang, “Data Hiding: Current Status and Key Issues,” International Journal of Network Security, vol.4, no.1, pp. 1-9, January 2007

[2] C Cachin, “An Information-Theoretic Model for Steganography,” Journal Information and Computation, vol.192, no.1, pp.41-56, 2004

[3] Neil F Johnson and SushilJajodia, “Steganalysis: The Investigation of Hidden Information,” *Proceedings of IEEE International Conference on Information Technology*, pp. 113-116, September 1998.

[4] İsmail Avcıbaş, Mehdi Kharrazi, NasirMemon and BülentSankur, “Image Steganalysis with Binary Similarity Measures,” EURASIP Journal on Applied Signal Processing, pp. 2794-2757, 2005

[5] Yong WANG, Qichang HE, Huadeng WANG, Bo YIN and Shaoling DING, “Steganographic Method Based on Keyword Shift,” Information Management and Engineering (ICIME), pp. 454-456, 2010

[6] Bhattacharyya S Kshitij and A P Sanyal G, “A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform,” *International Conference on Recent Trends in Information, Telecommunication and Computing*, pp.173-178, 2010.

[7] Sarreshtedari S and Ghaemmaghami S, “High Capacity Image Steganography in Wavelet Domain,” *International Conference on Consumer Communications and Networking*, pp.1-6, 2010.

[8] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi, “High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm,” *International Multi Conference of Engineers and Computer Scientists*, vol. 1, 2011

[9] R O El Safy, H H Zayed and A El Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform,” *International Conference on Networking and Media Convergence*, pp.111-117, March 2009.

[10] Jaskolka, Jason Khedri and Ridha, “Exploring Covert Channels,” *Hawaii International Conference on System Sciences*, pp.1-7, 2011

[11] Sanjeev Manchanda, Mayank Dave and S. B. Singh, “Customized and Secure Image Steganography through Random Numbers Logic” in Signal Processing: *An International Journal, Volume 1: Issue (1)*, 2008

[12] K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattnaik, “Steganography Based on Payload Transformation”, *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2*, March 2011

[13] K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, “Hybrid Domain in LSB Steganography”, *International Journal of Computer Applications (0975 – 8887)Volume 19– No.7*, April 2011

AUTHOR

H S Jayaramu received the BE degree from Malnad College of Engineering, Hassan. MTech MTech degree from SJCE Mysore, MS degree from Birla Institute of Technology and Science BITS, Pilani, Rajasthan. He has got more than 33 years of teaching experience in various institutions and he has over 13 research publications in National and international conferences and Journals. Currently he is working as Professor and HOD in the Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Logic design, and Steganography.

Dr K B ShivaKumar received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA Degree from Bangalore University, Bangalore and M Phil Degree from Dravidian University Kuppam. He obtained Ph.D. in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 30 years of teaching experience and has over 60 research publications in National and International conferences and journals. Currently he is working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Multi rate systems and filter banks, and Steganography.

Srinidhi G A received the BE degree in Telecommunication Engineering, from Visveswaraya Technological University, Belgaum, Karnataka, MTech degree in Sensor Systems Technology from VIT University Vellore, Tamilnadu. He has over 10 research publications in National and International conferences and journals. Currently he is working as Asst Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, image processing, Automotive Sensor systems, MEMS and Steganography.

sDr Arvind K Goutam received his M Tech degree in Electronics & Communication Engineering from Rajastan VidhyaPeet & another M Tech degree in Instrumentation Engineering from R E C Kulakshetra and PhD from Meerut University. He has got 18 years of teaching experience and has 40 research publications in National and International conferences. Currently he is working as Principal, S D College of Engineering, Muzzaffarnagar, Uttar Pradesh. His research interests include image processing.