International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-11 September-2013

Image Steganography using DCT-DST, Haar-DST, Walsh-DST, Hartley-DST Hybrid Wavelet Transforms

H. B. Kekre[1], Sudeep D. Thepade[2], Ratnesh N. Chaturvedi[3]

Abstract

Steganography is the process of hiding a secret message within a larger cover image in such a way that no one can know the presence of the hidden message in it. The purpose of Steganography is to maintain secret communication between two parties. Steganography is a science for invisible communication and play vital role on the network security. To improve the embedding capacity as well as to have minimum distortion to carrier media, the paper proposed a method of hiding secret data into the transformed cover image. In the proposed system a block based information hiding scheme is developed using DCT-DST, Haar-DST, Walsh-DST, Hartley-DST Hybrid Wavelet Transforms for providing 62.5% of the embedding capacity. The Experimental results show that, the stego-image is visually indistinguishable from the original cover-image obtained in the proposed method. The paper compares block based information hiding schemes that hide secret information into DCT-DST, Haar-DST, Walsh-DST, Hartley-DST Hybrid Wavelet Transforms. Our experimental results show that use of DCT-DST hybrid wavelet transform (HWT) for image steganography achieves much better results as compared to Haar-DST, Walsh-DST, Hartley-DST Hybrid Wavelet Transforms.

Keywords

Steganography, Information hiding, Transforms, Hybrid Wavelet Transform.

1. Introduction

With the rapid development of information technology, security for the confidential information has become challenging issue today. Steganography techniques have been developed in order to achieve the security. Steganography is an art and science of hiding secret information into multimedia such as images, audios or text. The stego media is similar to the cover media hence it is difficult for the hackers to detect the existence of secret message on the cover media. The hidden secret information can be extracted by using retrieving algorithm. Image steganography has become an essential and potential field in information hiding for protecting the confidential information.

The three important requirements need to be considered for steganographic model are [1] :

- Imperceptibility: means to preserve the details of the cover image when the secret information is being embedded.
- Payload capacity: means the maximum number of bits that can be hidden with an acceptable resultant stego image quality.
- Robustness: is the ability of stego image to retain its contents from attacks.

The paper is organized as follows. Section 2 represents the related work, Section 3 describes hybrid wavelet transform generation. Section 4 presents method to embed and extract the secret message image . Section 5 describes experimental results and finally the concluding remarks and future work are given in section 6.

2. Related Work

The steganography techniques are broadly classified into two categories viz., (i) spatial domain and (ii) frequency domain. In spatial domain the secret information is directly embedded into the pixels of the cover image by using 1bit-LSB, 2bit-LSB, Variable bit LSB etc replacement. Hiding images using LSB substitution techniques can be found in [1]-[7]. But this method has very low robustness to modifications made to the stego-image such as a low pass filtering and compression.[8] In frequency domain [9][10]the cover image is transformed into coefficients such as DCT [11], DST [12], Hartley[13], Walsh [14], Haar[15], Wavelet Transforms[9] [16], Hybrid Wavelet Transforms [17] etc., and the secret data to be embedded is embedded

H. B. Kekre, Sr. Prof. Computer Engineering Dept., Mukesh Patel School of Technology, Management & Engineering, NMIMS University, Mumbai, India.

Sudeep D. Thepade, Prof. & Dean (R&D), PimpriChinchwad College of Engg., University of Pune, Pune, India.

Ratnesh N. Chaturvedi, Asst. Prof. Computer Engineering Dept., Mukesh Patel School of Technology, Management & Engineering, NMIMS University, Mumbai, India.

in high frequency region. The frequency domain embedding process is more secure [9] than the spatial domain [8]. Steganography is employed in various applications like copy right control of materials, enhancing robustness of image search engines and smart identity cards, video-audio synchronization, protection of intellectual property, exchange of highly confidential data in a covert manner and bank transactions.

The steganography techniques are broadly classified into two categories viz., (i) spatial domain and (ii) frequency domain. In spatial domain the secret information is directly embedded into the pixels of the cover image by using 1bit-LSB, 2bit-LSB, Variable bit LSB etc replacement. Hiding images using LSB substitution techniques can be found in [1]-[7]. But this method has very low robustness to modifications made to the stego-image such as a low pass filtering and compression.[8] In frequency domain [9][10]the cover image is transformed into coefficients such as DCT [11], DST [12], Hartley[13], Walsh [14], Haar[15], Wavelet Transforms[9][16], Hybrid Wavelet Transforms [17] etc., and the secret data to be embedded is embedded in high frequency region. The frequency domain embedding process is more secure [9] than the spatial domain [8]. Steganography is employed in various applications like copy right control of materials, enhancing robustness of image search engines and smart identity cards, video-audio synchronization, protection of intellectual property, exchange of highly confidential data in a covert manner and bank transactions.

3. Hybrid Wavelet Transform

Kronecker product is also known as tensor product. Kronecker product is represented by a sign $\otimes$. The Kronecker product of 2 matrices (say A and B) is computed by multiplying each element of the 1st matrix(A) by the entire 2nd matrix(B) as in equation 1:

$$\begin{bmatrix} a1 & a2 \\ a3 & a4 \end{bmatrix} \otimes \begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix} = \begin{bmatrix} a1\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix} & a2\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix} \\ a3\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix} & a4\begin{bmatrix} b1 & b2 \\ b3 & b4 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a1b1 & a1b2 & a2b1 & a2b2 \\ a1b3 & a1b4 & a2b3 & a2b4 \\ a3b1 & a3b2 & a4b1 & a4b2 \\ a3b3 & a3b4 & a4b3 & a4b4 \end{bmatrix} \quad \text{----(1)}$$

The hybrid wavelet [17] transform matrix of size NxN (say 'T_{CD}') can be generated from two orthogonal transform matrices (say C and D respectively with sizes pxp and qxq, where N=p*q=pq) as given by equations 2.

$$C=\begin{bmatrix} c11 & c12 & \dots & c1p \\ c21 & c22 & \dots & c2p \\ \vdots & \vdots & \vdots & \vdots \\ cp1 & cp2 & \dots & cpp \end{bmatrix} \begin{matrix} C1 \\ C2 \\ C3 \\ CP \end{matrix}$$

$$D=\begin{bmatrix} d11 & d12 & \dots & d1q \\ d21 & d22 & \dots & d2q \\ \vdots & \vdots & \vdots & \vdots \\ dq1 & dq2 & \dots & dqq \end{bmatrix}$$

----(2)

Here first 'q' rows of the hybrid wavelet transform matrix are calculated as Kronecker product of D and C1 which is given as:

$D \otimes C1=$

$$\begin{bmatrix} d11c11 & d11c12 & \dots & d11c1p & d12c11 & d12c12 & \dots & d12c1p & \dots & d1qc11 & d1qc12 & \dots & d1qc1p \\ d21c11 & d21c12 & \dots & d21c1p & d22c11 & d22c12 & \dots & d22c1p & \dots & d2qc11 & d2qc12 & \dots & d2qc1p \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ dq1c11 & dq1c12 & \dots & dq1c1p & dq2c11 & dq2c12 & \dots & dq2c1p & \dots & dqqc11 & dqqc12 & \dots & dqqc1p \end{bmatrix}$$

----(3)

For next 'q' rows of hybrid wavelet transform matrix Kronecker product of identity matrix I_q and C2 is taken which is given by equation 4:

$I_q \otimes C2 =$

$$\begin{bmatrix} c21 & c22 & \dots & c2p & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & c21 & c22 & \dots & c2p & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & c21 & c22 & \dots & c2p \end{bmatrix}$$

----(4)

Similarly the other rows of hybrid wavelet transform matrix are generated as $I_q \otimes C3$, $I_q \otimes C4$, $I_q \otimes C3$ ….. and the last 'q' row are generated as equation 5:

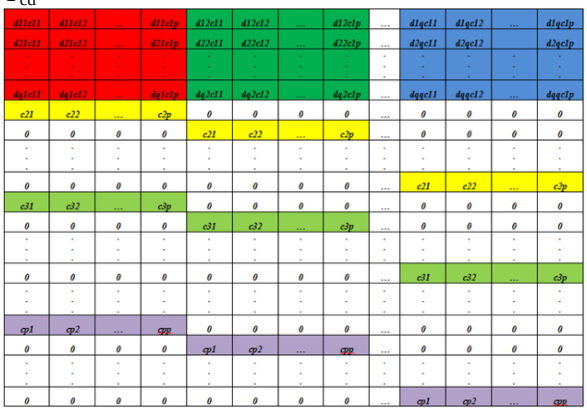
$I_q \otimes CP =$

$$\begin{bmatrix} cp1 & cp2 & \dots & cpp & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & cp1 & cp2 & \dots & cpp & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & cp1 & cp2 & \dots & cpp \end{bmatrix}$$

----(5)

and the final hybrid wavelet transform matrix is given by equation 6:

$T_{cd}=$



----(6)

4. Proposed Steganography System

Hybrid wavelet transforms like DCT-DST HWT, Haar-DST HWT, Walsh-DST HWT, Hartley-DST HWT are applied on the full cover image. The entire transformed cover image is then divided in 16 non-overlapping blocks [8]. The energy of each block is computed and ten blocks of lower energy [9] are selected to embed the normalized secret message into these blocks to achieve 62.5% embedding capacity. A conceal plan is generated of the size 4x4 which has information about where the secret message is hidden, the block containing the hidden message is marked by '1' and rest of the blocks are marked by 0 as shown in Figure 1 . The conceal plan size is minimized to 4x1 by converting each row of conceal plan into its decimal equivalent and then normalizing it. Then a lower energy block is selected in which this minimized normalized conceal plan is embedded which is known only by the sender and the receiver. The inverse transform is applied to get the Stego image and the reverse is applied to obtain the hidden secret message.

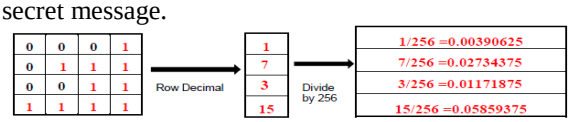


Figure 1: Conceal Plan Generation

Embedding Algorithm

1) Cover Image Transformation.
   Apply hybrid wavelet on the color image of size 256x256.
2) Block division and Energy calculation of transformed Cover Image.
   Divide the transformed cover image into block size of 64x64 and calculate the energy of each block.
3) Message Images Normalization.
   In all secret message each pixel value is divide by 256 to minimize the embedding error.
4) Generation of Conceal Plan.
   For embedding 62.5% of the cover image capacity 10 blocks with minimum energy are marked with 1 and rest by 0 as in Figure 1.
5) Minimizing the size of Conceal Plan and Normalizing it.
   Each row of a conceal plan is converted to its decimal equivalent and divided by 256 to normalize it.
6) Embedding secret normalized message as per Conceal Plan.
7) Embedding Conceal Plan.
8) Obtaining Stego image by taking inverse hybrid wavelet on modified Cover image.

Extraction Algorithm

1) Transformation of Stego Image.
   Apply hybrid wavelet on stego image
2) Retrieving and regeneration of Conceal plan.
   Obtain the minimized conceal plan and convert each digit into its binary equivalent to obtain the original conceal plan.
3) Retrieving Secret message blocks as per Conceal plan.
4) De-normalization of Retrieved Secret message.
   Multiply each pixel of the obtained message by 256 to de-normalize and obtain the original secret message.

5. Result and Discussion

These are the experimental results of the images shown in Figure 2 used as secret message and Figure 3 used as cover image. Our experimental results shows that by embedding 62.5% of the Cover image information as in Figure 3 with Secret Message image as in Figure 2 in various hybrid wavelet transforms like DCT-DST HWT, Haar-DST HWT, Walsh-DST HWT, Hartley-DST HWT. DCT-DST HWT gives the least MSE (Mean Squared Error) between the Cover Image and the Modified Cover Image i.e. Stego Image as in Figure 4 and Table 1. Total four Secret Message Image (Left to Right and Top to Bottom, Image1 128x128, Image2 64x128, Image3 128x64 and Image4 64x128) were embedded into the Cover image (Left to Right and Top to Bottom, Image1, Image2, …..,Image6) of size 256 x 256.

Figure 2: Test Bed of Secret Message

As shown in Table 1 and in Figure 4, Image1 has more granularity as compared to all other images and Image 5 has less granularity as compared to all other images, so more the granularity of the image greater is the MSE value between the cover image and the stego image and viz.

Table 1: MSE of Cover Image w.r.t Stego Image

Cover Image	DCT-DST HWT MSE	Haar-DST HWT MSE	Walsh-DST HWT MSE	Hartley-DST HWT MSE
Image 1	158.671	379.307	357.797	247.774
Image 2	19.294	83.416	79.028	55.101
Image 3	87.263	215.288	193.526	149.630
Image 4	27.250	78.362	75.288	64.942
Image 5	7.911	39.469	33.288	23.674
Image 6	34.673	73.545	72.970	51.025
Average	55.843	144.898	135.316	98.691

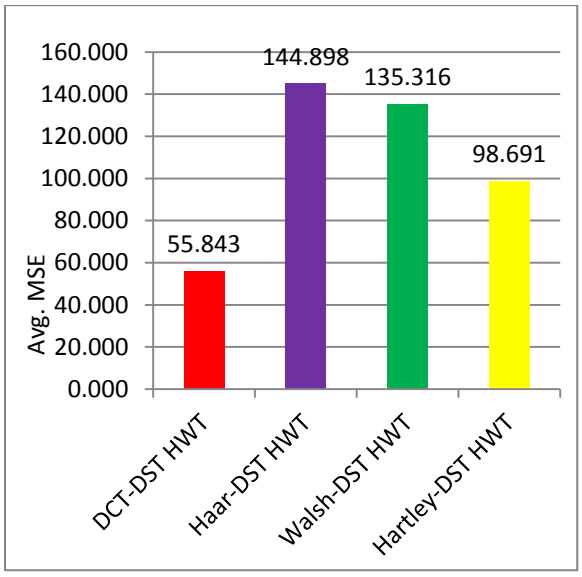


Figure 4: Average MSE of Cover Image w.r.t Stego Image

Figure 3: Test Bed of Cover Image
Observation : Cover image (Left to Right and Top to Bottom, Image1, Image2, …..,Image6)

6. Conclusion and Future Work

This paper proposes a novel image steganography technique using hybrid wavelet transforms (HWT). Image Steganography using DCT-DST HWT, Haar-DST HWT, Walsh-DST HWT, Hartley-DST HWT have been implemented. The paper compares the result of DCT-DST HWT, Haar-DST HWT, Walsh-DST HWT, Hartley-DST HWT respectively. Our experimental results prove that steganography among DCT-DST HWT, Haar-DST HWT, Walsh-DST HWT, Hartley-DST HWT and for 62.5% embedding, DCT-DST wavelet gives the least MSE. If the image used as cover image is having lower granularity then the MSE will be minimum. Our next research step could be to test other hybrid wavelets for information hiding and to test them against various attacks like Histogram Equalization, Brightness, Salt and Pepper noise, Cropping etc.

References

[1] Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S ," Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Vision, Image and Signal Processing, IEE Proceedings - Volume 152, Issue 5, 7 Oct. 2005.

[2] C.K Chan and L.M Cheng," Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[3] Wu, H.-C.; Wu, N.-I.; Tsai, C.-S.; Hwang, M.-S ," Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Vision, Image and Signal Processing, IEE Proceedings - Volume 152, Issue 5, 7 Oct. 2005.

[4] C.K Chan and L.M Cheng ," Hiding data in images by simple LSB substitution ," Pattern Recognition , pp. 469-474, Mar. 2004.

[5] Dr. H. B. Kekre, Ms. ArchanaAthawale and Ms. Pallavi N. Halarnkar, "Increased Capacity of Information Hiding in LSBs Method for Text and Image", International Journal of Electrical, Computer and Systems Engineering, Volume 2 Number 4. http://www.waset.org/ijecse/v2.html.

[6] Dr. H. B. Kekre, Ms. ArchanaAthawale, "Information Hiding using LSB Technique with Increased Capacity" International Journal of Cryptography and Security, Vol-I, No.2, Oct-2008.

[7] Dr. H. B. Kekre, Ms. ArchanaAthawale and Ms. Pallavi N. Halarnkar, "Polynomial Transformation To Improve Capacity Of Cover Image For Information Hiding In Multiple LSB's ",International Journal of Engineering Research

and Industrial Applications (IJERIA), Ascent Publications, Volume II, March 2009, Pune.

[8] Dr. H.B. Kekre, Archana B. Patankar and Dipali Koshti, "Performance Comparison of Simple Orthogonal Transforms and Wavelet Transforms for Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 44– No.6, April 2012.

[9] Sherin Youssef, Ahmed Abu Elfarag, RetaRaouf, "A ROBUST STEGANOGRAPHY MODEL USING WAVELET-BASED BLOCK-PARTITION MODIFICATION", International Journal of Computer Science & Information Technology (IJCSIT) pp. 15-28 Vol 3, No 4, August 2011.

[10] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, pp. 358-364 Vol. 7, No. 4, October 2010

[11] Ahmed N., Natarajan T., Rao K.R. "Discrete Cosine Transform", IEEE TRANSACTIONS ON COMPUTERS, Volume: C-23 , Issue: 1, Page(s): 90 – 93, Jan. 1974.

[12] Dr. H.B. Kekre, Ms. ArchanaAthawale and DipaliSadavarti,"A Novel Steganographic Scheme Using Discrete Sine Transform based upon energy distribution", International conference on contours of computing technology, Thinkquest-2010, held on 13th,14th March , 2010, Mumbai.

[13] R. N. Bracewell, "Discrete Hartley transform," Journal of the Optical Society of America, Volume 73, Issue 12, pp 1832-1835, Dec. 1, 1983.

[14] J Walsh, "A closed set of normal orthogonal functions", American Journal of Mathematics, Volume 45, No 1, pp 5 – 24, 1923.

[15] Alfred Haar, "ZurTheorie der orthogonalenFunktionensysteme" (German), MathematischeAnnalen, Volume 69, No 3, pp 331 – 371, 1910.

[16] Dr. H. B. Kekre, Dr. Tanuja K. Sarode, Sudeep D. Thepade, Ms.SonalShroff, "Instigation of Orthogonal Wavelet Transforms using Walsh, Cosine, Hartley, Kekre Transforms and their use in Image Compression", International Journal of Computer Science and Information Security, Volume 9, No 6,pp 125-133, 2011.

[17] Dr. H. B. Kekre, DrTanuja K. Sarode, Sudeep D. Thepade, "Inception of Hybrid Wavelet Transform using TwoOrthogonal Transforms and It's use for Image Compression", International Journal of Computer Science and Information Security,Vol. 9, No. 6, pp. 80-87, 2011

H. B. Kekre has received Ph.D. (System Identification) from IIT Bombay in 1970. He has worked as Faculty of Electrical Engg. and then HOD Computer Science and Engg. at IIT Bombay. For 13 years he was working as a professor and head in the Department of Computer Engg. at Thadomal Shahani Engineering College, Mumbai. Now he is Senior Professor at MPSTME, SVKM's NMIMS University. He has guided 17 Ph.Ds more than 100 M.E./M.Tech and several B.E./B.Tech projects.. He has more than 450 papers in National / International Conferences and Journals to his credit. He was Senior Member of IEEE. Presently He is Fellow of IETE and Life Member of ISTE. Recently fifteen students working under his guidance have received best paper awards. Eight students under his guidance received Ph. D. from NMIMS University. Currently five students are working for Ph. D. Under his guidance

Sudeep D. Thepade has Received Ph.D. Computer Engineering from SVKM's NMIMS in 2011. He has about 10 years of experience in teaching and industry. Currently he is Professor and Dean (R&D), at Pimpri Chinchwad College of Engineering, Pune. He more than 185 papers inInternational Conferences/Journals to his credit. He is member of International Advisory Committee for many International Conferences, acting as reviewer for many referred international journals/transactions including IEEE and IET. His areas of interest are Image Processing and Biometric Identification. He has guided five M.Tech. Projects and several B.Tech projects.

Ratnesh N. Chaturvedi has Received M.Tech Comp. Engg. from SVKM's NMIMS in 2013. He is Asst. Professor at SVKM's NMIMS, Mumbai. He has about 04 years of experience in teaching.He has 9 papers in International Conferences /Journals to his credit in last one year. His area of interest is Image Colorization & Information Security.