A TQWT BASED APPROACH FOR IMAGE STEGANOGRAPHY

DR. SUSHIL KUMAR

Abstract: Image Steganography refers to the process of hiding digital data in the digital images in an imperceptible manner. There are mainly two types of Steganography: Spatial Domain and Transform Domain. This paper presents the study of Transform domain based image steganography using Tunable Q-Factor Wavelet Transform (TQWT) and a self-synchronizing variable length codes: T-codes. The proposed algorithm provides larger embedding capacity and minimizes the distortion of the stego-image. The TQWT is a flexible fully-discrete wavelet transform, has the perfect reconstruction property, is modestly overcomplete, is developed in terms of iterated two-channel filter banks, and implemented using the DFT. The transform is specified by two parameters: Q and r, the transform's Q-factor and redundancy. The transform can be tuned according to the oscillatory behavior of the signal to which it is applied. The secret message, obtained from the original message by the application of T-codes, is embedded in the first three wavelet coefficients resulted from the three stages of TQWT. Coefficients in the fourth Wavelet are preserved unaltered to improve the image quality. The basic strategy of embedding is based on the Reversible threshold technique, also known as Companding technique. The use of T-codes does not only compress the message but also provides self-synchronization at decoding stage. The Proposed algorithm is implemented on Matlab 10 and the experimental results are provided in terms of the metrics PSNR, SSIM and KLDiv.

Keywords: TWQT; PSNR; SSIM; KLDiv

Introduction: Reversible (or distortionless) Steganography has a great significance in the organizations and in our digital life where security and privacy are utmost important issues. Steganography or data hiding means covert communication. In Image steganography, we hide messages by using redundancy in the image. It resolves the issue of authenticity to a great extent and provides image integrity. There are two domains, viz. Spatial domain and Transform domain for hiding the messages. The transform domain techniques are found to be robust than the spatial domain, hence, it has attained more attention of the researchers. One of the important features of steganography is imperceptibility, i.e., the secret message hidden in image remains visually imperceptible unless it does not cause any noise or distortion to the cover image.

There are number of applications like Judiciary (i.e., law enforcement), Government HoD, medical imagery, astronomical research, and Content authentication of multimedia data and so on, where the original image is required to be restored after the hidden message is removed from it. According to X. Zhang (2013), they can be classified into following three types:

1. Lossless compression based methods, that compresses a set of selected features from a image to save space for data embedding.[Fridirch et al. (2002)]
2. Difference expansion (DE),that expands the difference between two neighboring pixels to obtain redundant space for embedding a message.[10] and
3. Histogram modification (HM) methods, that uses the histogram of the pixel values in the cover image to embed secret data into the maximum frequency pixels.[4]

In this paper, we propose a reversible (lossless) steganographic algorithm based on thresholding technique proposed by Xuan G. et al. [9]. The brief summary of this method is summarized in next subsection.

Companding technique: TheReversible Companding technique consists of two processes, viz., Compression and Expansion. Let the compression function is y = C(x), (x is the original signal) and, let the expansion function is given by x = E(y). If E[C(x)] = x, then the process known as reversible, and it could be applied into reversible data hiding. A reversible Companding method, based on a threshold value, T, for the lossless data hiding is given by Xuan et al. [9]. During the embedding process the message bit, b, is inserted into the selected coefficients of middle and high frequency subbands as follows:

$$x' = \begin{cases} 2*x + b & \text{if} \quad |x| < T \\ x + T & \text{if} \quad x \geq T \\ x - (T\text{-}1) & \text{if} \quad x \leq -T \end{cases}$$

The original image is recovered by restoring each of the high frequency coefficients by applying the following formula:

$$x = \begin{cases} \lfloor x'/2 \rfloor & \text{if} \quad -2T < | x' | < 2T \\ x' - T & \text{if} \quad x' \geq 2\,T \\ x' + T\text{-}1 & \text{if}\; x' \leq -2T + 1 \end{cases}$$

Tunable q-factor wavelet transform [4][5]: The Tunable q-factor Wavelet Transform(TQWT) is a discrete-time wavelet transform, has the perfect reconstruction property, is modestly over complete, is developed in terms of iterated two-channel filter banks, and implemented using the DFT. It is based on three parameters Q, r and J, respectively. The Q-factor, Q, is a measure of the number of oscillations the wavelet exhibits. The parameter, r, refers to redundancy of the TQWT, and J represents the stages of TQWT applied. The analysis and synthesis filter banks for the tunable-Q wavelet transform are shown in Fig.

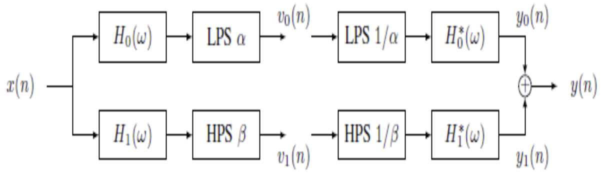


Fig.1. Analysis and synthesis filter banks for the TQWT [5].

Here, LPS and HPS represent low-pass scaling and high-pass scaling respectively. The subband signal $v_o(n)$ has a sampling rate of αfs where fs is the sampling rate of the input signal x(n). Likewise, the subband signal $v_1(n)$ has a sampling rate of βfs. A three-stage wavelet transform is illustrated in Fig. 9. The wavelet transform inherits the perfect reconstruction property from the two channel filter bank. We denote the wavelet subband signals by $w^{(j)}(n)$ for j ≥1

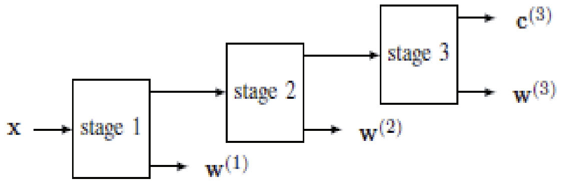


Fig. 2. Wavelet filter bank [5].

Each stage consists of the two-channelanalysis filter bank in Fig. 1.

Proposed algorithm: Each image steganography algorithm consists of an embedding process and an extraction process. At the pre-processing stage, we first obtain the secret message from the original message by applying a self-synchronizing variable length codes, viz., T-codes [7][8], and an innocuous-looking original image is selected as the cover-image to hide the secret data. Then, the secret data are embedded into the cover-image by modifying the cover image to form a stego-image based on threshold technique, using an embedding key. At the receiver end, the legal user can successfully extract the embedded data by using the corresponding extraction key in the extraction process. The embedding key and the extraction key are usually referred to as stego-keys. The details of the embedding and extraction process are given as follows:

Embedding:

Step 1: Find the secret code from the original message using T-codes.
It generates an encoding-key, k1.

Step 2: Select the cover image of size 256 x 256,and apply the histogram modification to prevent overflow/underflow.

Step 4: Apply the 3-stages of TQWT to the cover image resulting into 4- subbands w{1},w{2}, w{3} and w{4} .

Step 5: Select the appropriate threshold value, T, (usually T= 35).

Step 6: The frequency coefficients of high frequency wavelet coefficient, w{1},w{2}, w{3} are permuted using a random-key, k2 and obtain new sub-bands w'{1},w'{2}, w'{3}, respecitively

Step 8: The binary bits of secret message are embedded into the corresponding randomly chosen wavelet coefficients, using the thresholding technique discussed above.

Step 9: Apply the inverse of the random permutation to obtain stego sub-bands w"{1},w"{2}, w"{3}, respectively.

Step 10: The modified image is obtained by merging the stego wavelet coefficients with low frequency wavelet coefficient,w{4}.

Step 11: Take the inverse of TQWT to the modified image and get the stego-image.

Random selection of coefficients in Step 8 provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.

Extraction:

Step1. Apply 3-stege of TQWT to the stego image and obtain the Wavelet coefficients, w{1}, w{2}, w{3} and w{4}, respectively.

Step2. Permute the wavelet coefficients of w{1},w{2}, w{3} , using the permuted key, k2.

Step3. The secret data is extracted from the selected frequency coefficients of three high frequency wavelet coefficients, w{1},w{2}, w{3} using the stego-key and the reversible thresholding technique.

Step3. The original message is obtained by decoding the secret data using T-codes and encoding key, k1.

Step4. Finally, the original image is recovered by reverse operation of the embedding.

Experimental results: The performance of the proposed reversible steganography algorithm, we have used grayscale scale images of size 256 x 256. Simulations are done using MATLAB 10.0. The proposed algorithm based on TQWT and T-codes is compared with the correspodiong algorithm based on CDF9/7 wavelets on grayscale images. The results for some of the tested images are summarized in the Tables 1 to 3 and Fig.3 to Fig.5 , respectively.

Table 1. PSNR values of the proposed algorithm

Image	CDF(2,9)	TQWT
Lily.jpg	31.2653	41.5784
Lena.jpg	30.2151	41.6951
Baboo.bmp	23.1958	31.9281
Art.png	33.3200	44.0753
Peppers.jpg	30.5360	40.3896
Tooth1.jpg	34.6152	46.0760
Parliament.bmp	32.1990	41.2418

Table 2. SSIM values of the proposed algorithm

Image	CDF(2,9)	TQWT
Lily.jpg	0.9177	0.9996
Lena.jpg	0.9178	0.9938
Baboo.bmp	0.7200	0.9523
Art.png	0.8775	0.9882
Peppers.jpg	0.9634	0.9922
Tooth1.jpg	0.9539	0.9940
Parliament.bmp	0.9192	0.9862

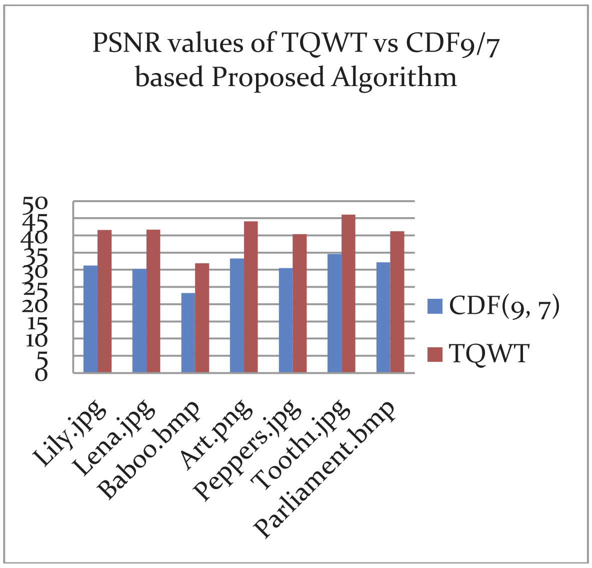


Fig.3. The comparison of Imperceptibility of proposed algorithm based on TQWT against CDF9/7 based corresponding algorithm

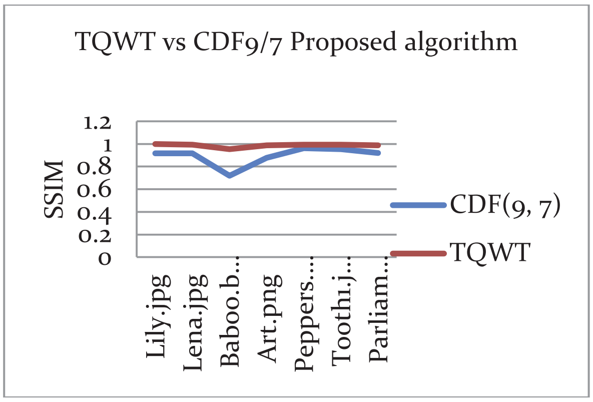


Fig.4. The comparison of Structural Similarity of proposed algorithm based on TQWT against CDF9/7 based corresponding algorithm

From Fig. 3 to Fig. 5, it can be seen that the proposed reversible steganography algorithm based on TWQT has better imperceptiblity (PSNR) , better structural similarity values (SSIM) and provable security values (KLDiv) in comparison to the Wavelet CDF9/7 based corresponding algorithm.

Table 3. KLdiv values of the proposed algorithm

Image	CDF(2,9)	TQWT
Lily.jpg	0.0101	0.0000
Lena.jpg	0.0121	0.0026
Baboo.bmp	0.0899	0.0108
Art.png	0.0032	0.0008
Peppers.jpg	0.0708	0.0000
Tooth1.jpg	0.0314	0.0000
Parliament.bmp	0.0363	0.0034

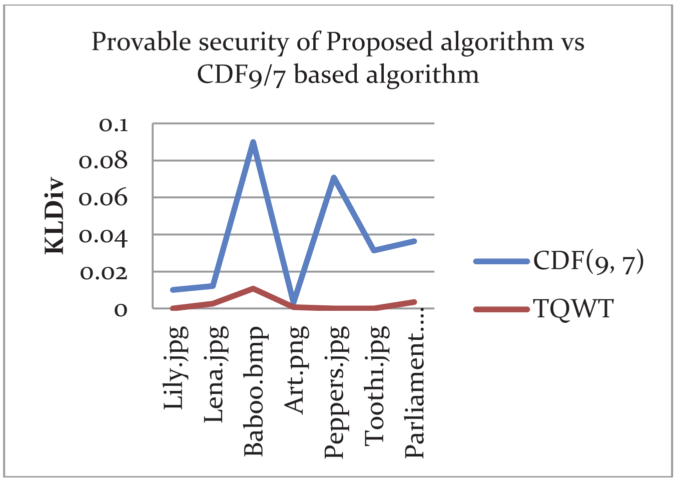
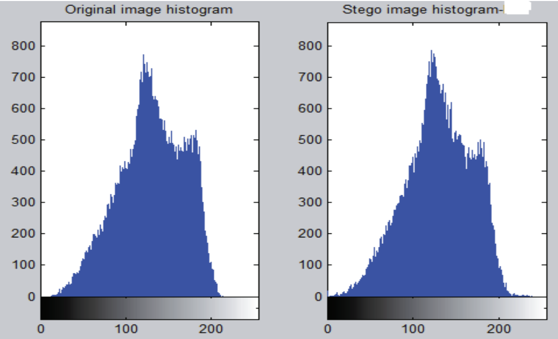


Fig.5. The comparison of provable security of proposed algorithm based on TQWT against CDF9/7 based corresponding algorithm

The results of stego-images and histogram obtained of images, baboo.bmp are shown in Fig. 6 and Fig. 7.



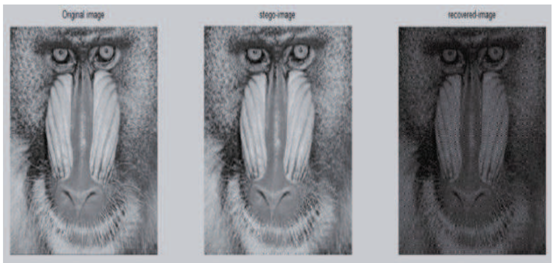
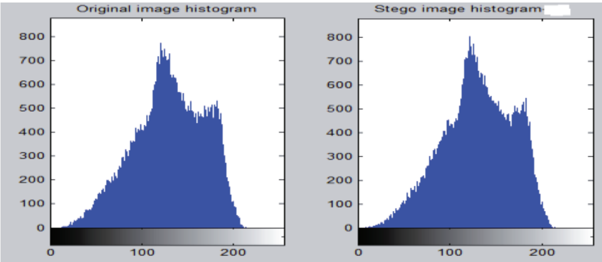


Fig.6. Results from the cdf(2/9) based proposed algorithm



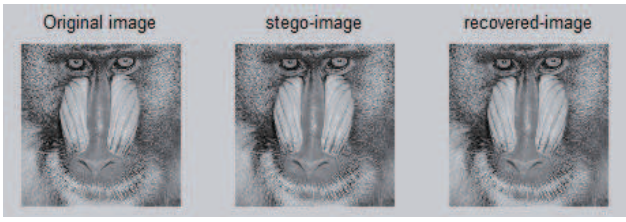


Fig.7. Results from the TQWT based proposed algorithm

It can be seen from above Fig. 6 and Fig. 7 that the proposed algorithm based on TQWT is having better recovered original image and histogram analysis results as compare to CDF9/7 Wavelet based corresponding algorithm.

Conclusions: In this paper, we present a reversible image steganography algorithm which increases the secret message capacity and improves the quality of the cover image and security. The most important achievement of this work is a high PSNR, negligible KLDIv value and SSIM value $\approx$ **1.**

Acknowledgment: The author would like to thank Ivan. W. Selesnick from Polytechnic Institute of New York University, for providing the TQWTdetails and the link to download TQWT Matlabcodes (http://eeweb.poly.edu/iselesni/WaveletSoftware/) without that it was not possible for me to precede my research in this field.

References:

1. Fridrich J., Goljan M. and Du R. (2001, Oct-Dec). Detecting LSB steganography in color and grayscale images,IEEE Multimedia (Multimedia and Security).
2. Sushil Kumar, "Data Hiding in Digital Images using Steganography". Ph.D. Thesis, University of Delhi, Delhi, (December 2013)
3. S. Manhoran, "Towards robust steganography using T-codes", Proceedings of Video/Image Processing and Multimedia Communications. (2003)
4. T. A. Raja and Fehim Jeelani, Poisson and Poisson Related Distributions With New Applications; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 4 Issue 1 (2015), Pg 14-17
5. NI Z., Shi Y.Q., Ansari N., Su Wei, Sun Q. and Lin X. (2004). Robust Lossless Image Data Hiding, IEEE International Conference on Multimedia and Expo (ICME), 2199-2202.
6. Ivan W. Selesnick, Wavelet Transform with Tunable Q-Factor, IEEE TRANSACTIONS ON SIGNAL PROCESSING (2011)
7. W. Selesnick, "Sparse signal representations using the tunable Q-factor wavelet transform," in: Proceedings of SPIE (Wavelets and Sparsity XIV), 2011, pp. 81381U:1-15.
8. M. R. Titchener, "Generalised T-codes: Extended construction algorithm for self- synchronization codes", IEE Proc. Commun., Vol. 143, No.3,122-128 (2006)
9. Gunther Ulrich, "Robust Source Coding with Generalised T-Codes", A thesis submitted in the University of Auckland. (1998)
10. Xuan G., Zhu J., Shi Y. Q., Ni Z. and Su. W. (2002, December). Distortionless data hiding based on integer wavelet transform," IEE Electronic Letters, 38(25): 1646-1648
11. Tian J. (2003). High capacity reversible data embedding and content authentication, IEEE International Conference on Acoustic, Speech and Signal Processing, April 6-10, Vol. 3, 517-520
12. Zhang X. (2013, February). Reversible Data Hiding with optimal value transfer, IEEE Transaction.

Dr. Sushil Kumar, Department of Mathematics, Rajdhani College, University of Delhi, New Delhi, India