Journal of Computer Science, 9 (3): 277-284, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.277.284 Published Online 9 (3) 2013 (http://www.thescipub.com/jcs.toc)

A High Secure and Robust Image Steganography Using Dual Wavelet and Blending Model

Prabakaran Ganesan and R. Bhavani

Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India

Received 2013-03-01, Revised 2013-04-07; Accepted 2013-04-12

ABSTRACT

Steganography is an ability of concealing information inside the cover in such a way it looks like simple cover though it has concealed information. There are many techniques to carry out steganography on electronic media, most especially audio and image files. In this method, we proposed a high secure steganography scheme hiding a 256×256 size gray secret image into a 512×512 size gray cover image with different combination of Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). Pixel Value Adjustment (PVA) is first performed on cover image. The secret image values are scrambled by using Arnold transform. The DWT /IWT is applied on both cover and scrambled secret image. Blending process is applied to both images and compute Inverse DWT/IWT on the same to get the stego image. The extraction model is actually the reverse process of the embedding model. Different combination of DWT/IWT transform is performed on the scrambled secret image and cover image to achieved high security and robustness. Hybrid transform combination approach and case analysis provided the various hiding environment. Experimental results and case study provided the stego-image with perceptual invisibility, high security and certain robustness.

Keywords: Image Quality Metrics, Blending Process, Wavelet Transform, Arnold Transform, Steganography

1. INTRODUCTION

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography is a method of hiding data in a cover file. The steganography technique has to satisfy three requirements viz., (i) Capability measurement is the amount of payload embedded into the cover image. (ii) Imperceptibility is the stego image must be similar to the cover image. (iii) Security is the hidden payload in the cover image should not be disturbed by the noise in the communication channel and also not to reveal to hackers. There must be tradeoffs between the three parameters to have better steganographic technique.

Choosing the hiding medium as the criteria, the steganographic techniques are classified as (i) Text- or linguistic based Steganography uses written natural language to conceal secret information. (ii) Audio Steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range by LSB manipulation, phase coding and echo hiding. (iii) Image Steganography hide the secret message in the images which is nearly impossible to differentiate by human eyes. Spatial domain technique approaches embeds the message in intensity of image pixel directly. In transform domain technique the images are transformed into frequency coefficients and messages are embedded in transformed coefficients. Today steganography techniques are mostly used for computers with digital data being the carriers and networks being the high-speed delivery channels.

1.1. Related Study

Review of related study has been conducted on various hiding methods like as Least Significant Bit (LSB), Discret

Corresponding Author: Prabakaran Ganesan, Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India

Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). Ahuja and Kaur (2009) proposed an image based steganography algorithm that combines LSB with high data hiding capacity, high confidentiality as distortions which can cause suspiscions for the intruders, are removed through filtering techniques and two level high security is applied in the model. Mamta and Sandhu (2009) proposed a robust image steganography technique based LSB insertion and encryption. Luo *et al*. (2010) proposed LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image.

Shivakumar *et al*. (2011) proposed a performance comparison of multiple transformation technique with error detection and correction coding technique was employed to ensure more reliable communication system. Reddy and Raja (2011) proposed a performance analysis of IWT and DWT on Non LSB with better PSNR value in the case of IWT compare to DWT. Battacharya *et al*. (2012) proposed a steganographic technique for hiding multiple images in a color image based on DWT and DCT.

Ghasemi *et al*. (2011) proposed to embeds data in IWT coefficients by using a mapping function based on Genetic Algorithm and increase the hiding capacity with low distortions. Peng *et al*. (2012) proposed a method that allows embedding more data bits into smooth blocks while avoiding large distortion generated by noisy ones and thus enables very high capacity with good image quality.

Yang *et al*. (2012) proposed a simple reversible data hiding scheme based on IWT. This model shows that both the host media and secret message can be completely recovered, without distortion, if the stego-images remain intact. Dinesh and Ramesh (2012) proposed a method in DWT transforms that allows to perfect embedding of the hidden message and reconstruction provide an efficient capacity for data hiding without sacrificing the original image quality.

Huang and Chang (2013) presented a hierarchy based reversible data hiding. In this study, there are many parameters for accessing the performances of reversible data hiding algorithms, including the output image quality, the hiding capacity and the overhead for decoding. Chang *et al*. (2013) presented a new index compression and reversible data hiding scheme based on Side-Match Vector Quantization (SMVQ) and Search Order Coding (SOC). In this proposed scheme, the confidential data are embedded into the transformed index table of a cover image and achieved more robustness.

The remaining chapter of the study will be organized as follows. Chapter two discusses about the materials and methods used in proposed steganography model. Chapter three describes the experimental results. Chapter four explained the discussion of our work. Conclusion and future improvements of the system are given in chapter five. Finally references are given in chapter six.

2. MATERIALS AND METHODS

2.1. Pixel Value Adjustment (PVA)

The gray scale cover image and payload pixel intensity values vary from zero to 255. During the payload embedding process the intensity values of cover image may exceed lower and higher levels which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255.

2.2. Haar-DWT

Haar wavelet operates on data by calculating the sums and differences of adjacent elements. A 2-D Haar-DWT operates first on adjacent horizontal operation and the other is the vertical one. One nice feature of Haar wavelet transform is that the transform is equal to its inverse.

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed.The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

Step 2: Next, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in **Fig. 1a and b**. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The procedure described above is called the first-order 2-D Haar-DWT that is shown in **Fig. 2**.

2.3. Arnold Transform

The first mathematical Arnold transform is proposed by Arnold and Avez (1968). It's improved chaotic map introduced by Mishra *et al*. (2012) which is applied to a digital image that randomizes the original organization of its pixels and the image becomes imperceptible or noisy. However, it has a period p and if iterated p number of times, the original image reappears.

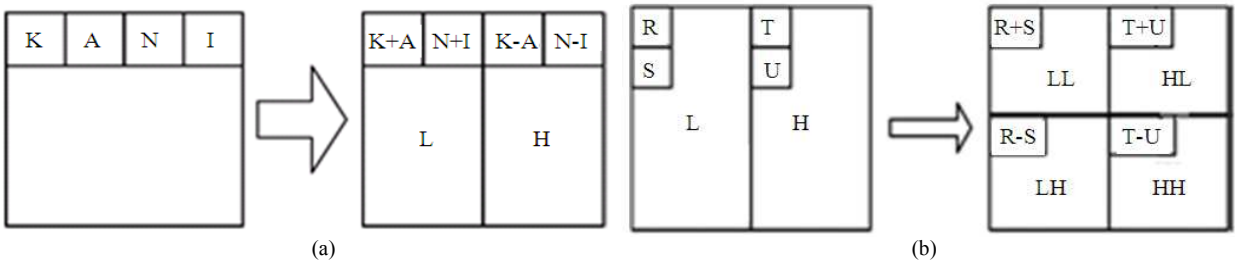


Fig. 1. (a) Shows the horizontal operation on the first row and (b) Shows the vertical operation

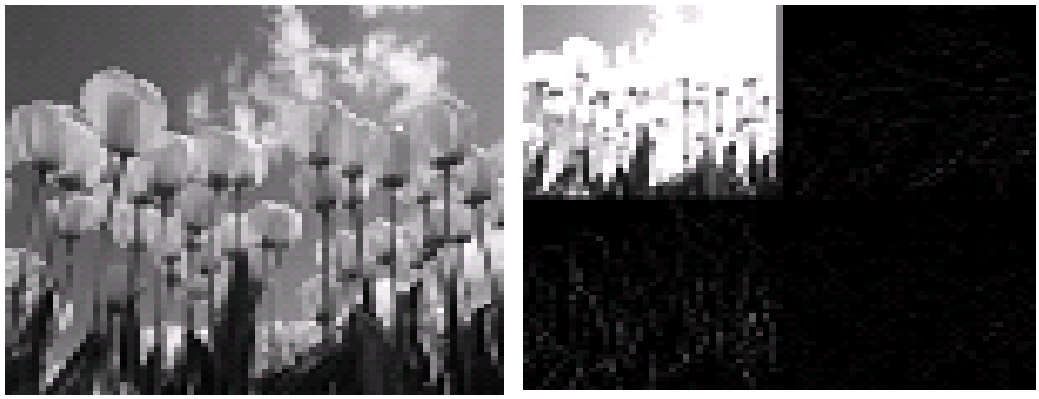


Fig. 2. Represents original image and result after the first order 2-D Haar-DWT

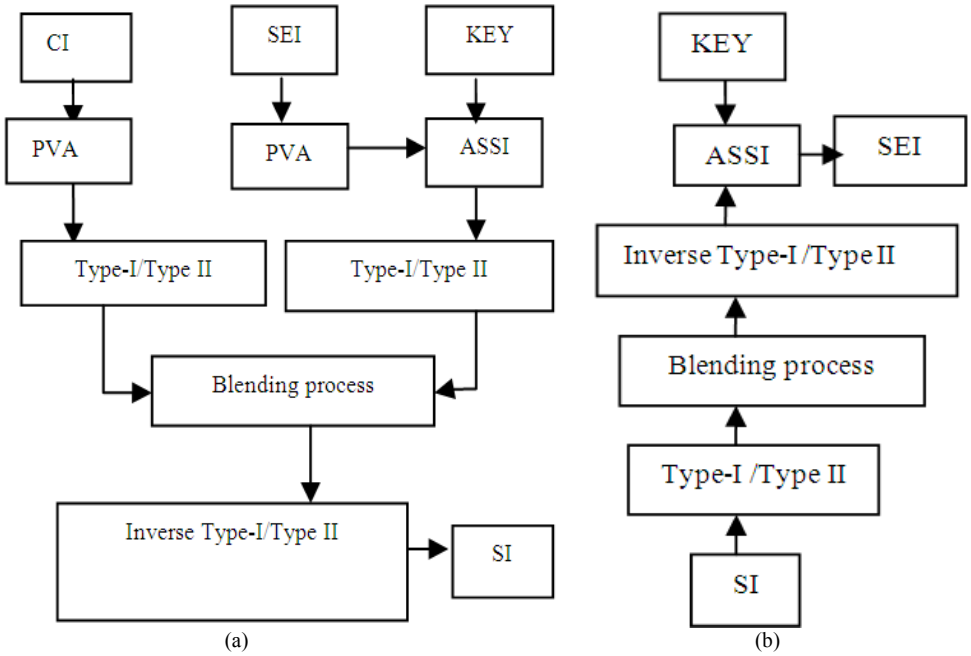


Fig. 3. The proposed (a) Encoding model (b) Decoding model (Cover Image-CI, Secret Image-SEI, Type-I: DWT, Type-II: IWT, Stego-image-SI, Arnold Scrambled Secret Image-ASSI)

We put the digital image as a matrix, which will become "chaotic" after Arnold transform. The discrete digital image is equivalent to a class of special matrices in which there is a correlation between elements. The Arnold transform of this matrix and then a new matrix can be obtained in order to achieve image scrambling processing.

Set the image pixel coordinates. N is the order of the image matrix, I, j € (0, 1, 2, N−1) and the Arnold transform is defined as Equation 1:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} (\text{Mod } N) \quad (1)$$

The above transform is one-to-one correspondence; the image can do iteration, iteration number can be used as a secret key for extracting the secret image. This transformation gives more security and robustness to our algorithm.

2.4. Integer Wavelet Transform

Integer Wavelet Transform is a Nonlinear transform having a structure of lifting scheme and as its rate distortion. Performance similar to DWT, Wavelet transforms that map integers to integers allow faultless reconstruction of the original image. The proposed algorithm employs the wavelet transform coefficients to insert messages into four subbands of two dimensional wavelet transform. To avoid problems with floating point precision of the wavelet filters, we used Integer Wavelet Transform. The LL subband in the case of IWT appears to be a close copy with the smaller scale of the original image while in the case of DWT the resulting LL subband is distorted.

2.5. Proposed Model

The following session describes the implementation of the encoding and decoding process in a sequential manner. The schematic representation of encoding and decoding process was given in **Fig. 3a and b**.

2.6. Encoding Process for Proposed Model

During the encoding process that the cover image and scrambled secret image was relocated by DWT/IWT transform domain and then by blending process. Next, IDWT/IIWT was performed to reform the stego image.

2.7. Algorithm for Encoding Process

Step1: Read the Cover Image (CI) and Secret Image (SEI) file into 2-D array.
Step2: Apply PVA on CI.
Step3: Perform a 2-D DWT/IWT at level 1 of the image CI.
Step4: Extract the approximation co-efficient of matrix (LA) and detail coefficient matrices LH, LV & LD of level 1of the image CI.
Step5: Apply Arnold transformation of SEI using key to get Arnold scrambled secret image ASSI.
Step6: Next extract the approximation coefficient of the matrix LA1 and detail coefficient matrices LH1, LV1 and LD1 of level-1 of the image ASSI.
Step7: Compute the hiding place by applying the following condition.
If (th < thset) (threshold value (th) less than threshold setted (thset) value of all coefficients then Alpha blending process for on CI and SSI to form Blending Image (BI)).
else (no change in pixels).
Step8: Finally, perform 2-D IDWT/IIWT on BI and form the Stego Image (SI).

2.8. Decoding Process for Proposed Model

The recover stego image was reconstructed with DWT/IWT transform domain and followed by blending process. Next, IDWT/IIWT was performed to rebuild the secret image.

2.9. Algorithm for Decoding Process

Step1: Received the image SI.
Step2: Perform a 2-D DWT/IWT at level 1 of the SI.
Step3: Calculate the threshold value less than threshold set and extract the ASSI coefficients.
Step4: Take the inverse transform and obtain ASSI.
Step5: Give the secret key and extract the recovered secret image SEI.

2.10. Case Study

In our case study, the various wavelets like DWT and IWT combinations are taken and worked out in our experiment. The following case study gives an idea of implementation of our security model. The Case-1 model is applied DWT for both cover and secret image. Next, Case-2 model was applied DWT for cover and iwt for secret image. Then Case-3 model applied IWT for cover and DWT for secret image. Finally, Case-4 model was applied the IWT for both cover and secret image.

3. RESULTS

To evaluate the performance of the proposed method by using Matlab R2012a. Images are collected from a database such as SIPI and University of Washington. We performed the blending process in our experiments with 200 general sample images.

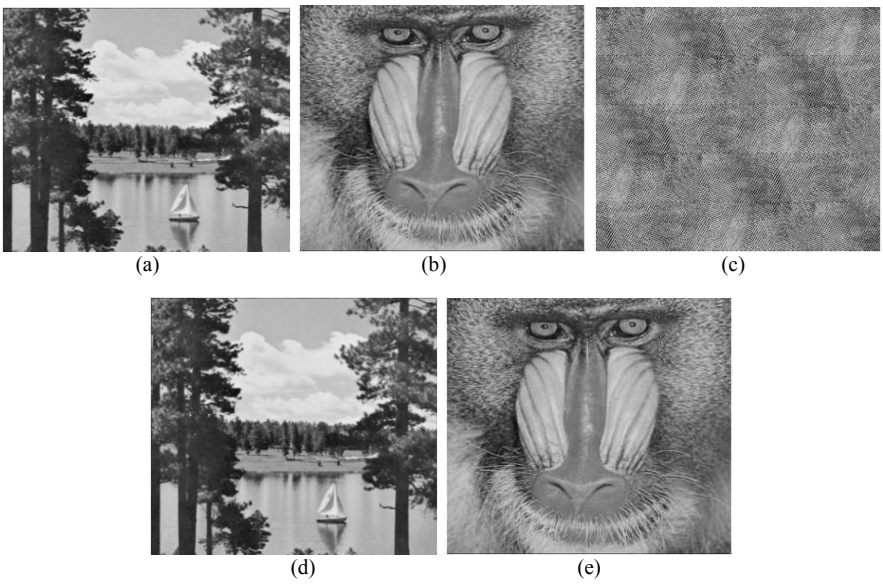
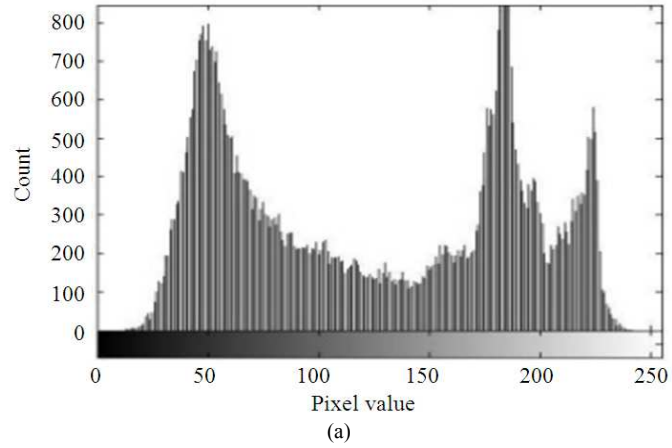
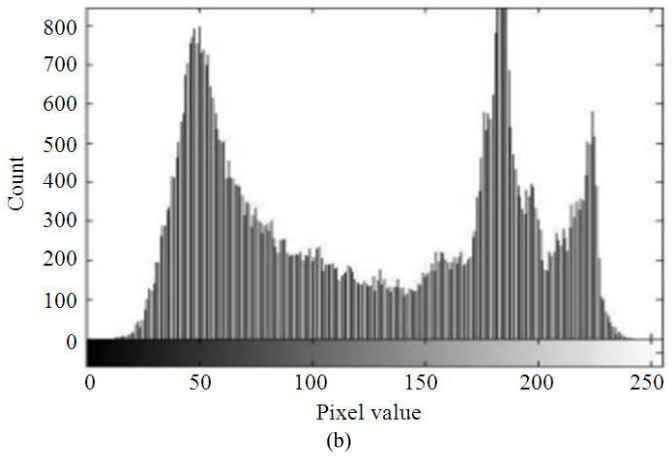


Fig. 4. The experimental (a) cover image, (b) secret image, (c) Scrambled secret image, (d) stego image, (e) Extracted secret image



(a)



(b)

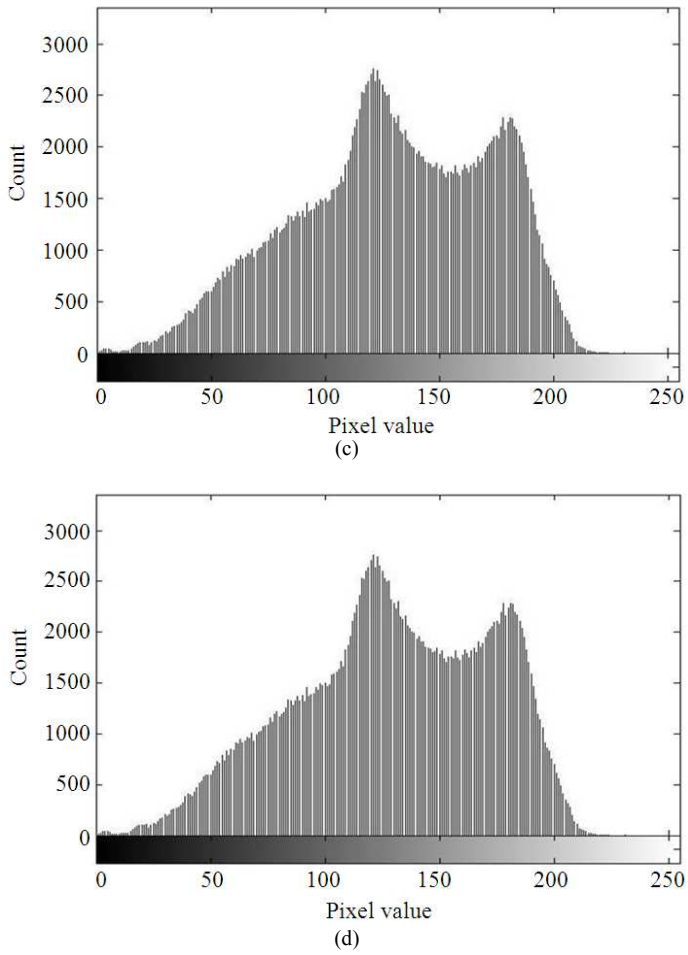


Fig. 5. Histogram plot of (a) cover image (b) stego image (c) secret image (d) recovered secret image

Table 1. Image quality metrics with their formulas

Quality metrics	Formulas
1. Mean Square Error (MSE)	$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)^2$
2. Peak Signal to Noise Ratio (PSNR)	$PSNR = 10\frac{\log_{10}(255)^2}{MSE}dB$
3. Normalized Cross Correlation (NCC)	$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)\frac{1}{\sum_{j=2}^{M}\sum_{k=2}^{N}\left(x_{j,k}\right)^2}$
4. Average Difference (AD)	$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)/MN$
5. Structural Content (SC)	$SC = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k}\right)^2 / \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x'_{j,k}\right)^2$
6. Maximum Difference (MD)	$MD = Max\left(\left\|X_{j,k} - X_{j,k}\right\|\right)$
7. Normalized Absolute Error (NAE)	$NAE = \sum_{j=2}^{M}\sum_{k=2}^{N}\left\|x_{j,k} - x_{j,k}\right\| / \sum_{j=2}^{M}\sum_{k=2}^{N}\left\|x_{j,k}\right\|$

For representation purpose we have given tree.tiff (512×512) as cover image, where as baboon.tiff (256x256) is considered as secret image. Cover image and secret image are shown in **Fig. 4a and b**. An Arnold trasform performed scrambled secret image is shown in **Fig. 4c**. The corresponding stego image is shown in **Fig. 4d** and extracted secret image are shown in **Fig. 4e**. The **Fig. 5** shows the histogram of original cover image versus stego image and secret image versus recovered secret image.

3.1. Image Quality Metrics

To retain the image quality,provide a stronger robustness and imperceptibility by using the wavelet transform technique. The good visual quality of stego images(i.e. images with a secret image) is the very important property of steganographic system because it is difficult to detected by detectors. We used different image quality metrics in our experiment as shown in the **Table 1**.

In first formula, the Mean Square Error (MSE) is defined as error between cover image and stego image. Second formula is Peak to Signal Noise ration (PSNR), which is findout peak signal to noise ration between cover and stego image. Third one calculated the Normalized cross correlation (NCC), which is findout the correlation between cover image and stego image. Fourth one calculated theAverage Different (AD), which is calculated the average different between the cover image and stego image. The stuctural content differences should be findout by using the formula Stuctural Content (SC). Similarly we findout Maximum difference (MD) and Normalized Absolute Error (NAE) was calculated absolute errror between cover image and stego image. All image quality metrics are useful to finout the difference between cover image and stego image.

4. DISCUSSION

We had tried a different combination of wavelet transform in our secure steganography system. This study includes analysis of proposed algorithm and four cases in our proposed model. Our proposed method in terms of pixel value adjustment and depth values. Pixel Value Adjustment (PVA) is applied to cover image. It is used to prevent the overflow /underflow that occurs when the change values in wavelet co-efficients.

In our case study,we had findout the compression ratio for hiding enviroment and image quality for imperceptibility. First case DWT decomposition gives the high compression ratio with less image quality . Second case DWT and IWT hybrid decomposition gives the acceptable image quality. Third case IWT and DWT decomposition gives less compression ratio with reasonable image quality. Fourth case IWT decomposition gives less compression ratio with high image quality.The combined approach case 2 gives the better performance than case3. In case of single transform approach case1 gives better performance than case 4. This hybrid environment is offer more security and imperceptibility.

Table 2. Image quality metrics values comparison of cover and stego image

Case	MSE	PSNR	NCC	AD	SC	MD	NAE
1	0.5498	50.7286	0.9986	-0.0376	1.0027	1.8700	0.0051
2	0.7841	49.1872	0.9938	0.6466	1.0125	2.1835	0.0060
3	2.9633	43.4131	1.0049	-0.9244	0.9902	4.9835	0.0113
4	1.6003	46.0880	0.9952	0.4395	1.0097	4.9780	0.0082

(MSE = Mean Square Error), (PSNR = Peak Signal to Noise Ratio), (NCC = Normalized Cross Correlation), (AD = Average Difference), (SC = Structural Content), (MD = Maximum Difference), (NAE = Normalized Absolute Error)

Table 3. Different image manipulation attacks on stego images with respect to their sample images for robustness checking

Manipulation attacks variance value		Case 1	Case 2	Case 3	Case 4
Image contrast	0.04	50.0999	48.5585	42.7844	45.4593
	0.06	50.0632	48.5218	42.7477	45.4226
	0.08	49.9433	48.4019	42.6278	45.3027
	0.10	49.6925	48.1511	42.3770	45.0519
Image suppression	0.04	50.1334	48.5920	42.8179	45.4928
	0.06	49.4777	47.9363	42.1622	44.8371
	0.08	48.6973	47.1559	41.3818	44.0749
	0.10	47.8627	46.3213	40.5472	43.2221
Image rotate	0.50	50.7286	49.1872	43.4131	46.0880

The image qualtiy metrics values comparison of cover and stego images were reported in **Table 2** . In this table the MSE value is observed 0.5 to 2.96. The best MSE value get from case 1 and case 2. The PSNR value observed nearly 43 to 50 dB. It shows that our system is high imperceptibility and secure. Normalized Cross Correlation between the cover and stego image are observed by nearly one. Structural Content value close to one that shows the highest correspondence structure of cover image. AD and MD values are observed in the range of 0 to 5. So it is also indicate less difference between cover and stego image. NAE is detected less than 0.01 value, which shows the minimum absolute error and shows good quality of stego image.

For our hiding methods, the various image processing and image manipulation attacks are given to stego images are also reported in **Table 3**. The measurements of image quality metrics not only reduces the image perceptibility but also enhances the robustness to resist attacks. Such attempts include image manipulations like image contrast, image suppression and image rotation. The various variance values are applied to stego image with our four case study. The PSNR value calculated between the cover image and image manipulation attacked image. The PSNR values shows that very less difference as early calculated cover image vs stego image. The PSNR differences are observed for the ranges from o.6 to 1 dB for our attacks.

5. CONCLUSION

In this study, we make use of DWT and IWT schemes in spatial domain for digital images by using blending embedded strategy. The PVA also carried out in the study it can also gain up to 2 dB in PSNR value. We achieved additional security using Arnold transform to scramble the secret image. This blending combination approach is capable of achieving more security, imperceptibility and certain robustness. According to our study of alpha and beta multiplier provided a deep depth value to hide the secret image. It is observed that the robustness and capacity are improved with very little tradeoffs in PSNR. In future, this model should be extended to apply in to medical image and medical report transaction process.

6. REFERENCES

Ahuja, B. and M. Kaur, 2009. High capacity filter based steganography. Int. J. Recent Trends Eng., 1: 672-674.

Arnold, V.I. and A. Avez, 1968. Ergodic Prblems in Classical Mechanics. 1st Edn., New York, Benjamin, pp: 286.

Battacharya, T. N. Dey and S.R.B. Chauduri, 2012. A session based multiple image hiding technique using DWT and DCT. Int. J. Comput. Applic., 38: 18-21.

Chang, C.C. T.S. Nguyen and C.C. Lin, 2013. A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies. J. Syst. Software, 86: 389-402. DOI: 10.1016/j.jss.2012.09.001

Dinesh, Y. and A.P. Ramesh, 2012. Efficient capacity image steganography by using wavelets. Int. J. Eng. Res. Applic., 2: 251-259.

Ghasemi, E. J. Shanbehzadeh and B.Z. Azami, 2011. A steganographic method based on integer wavelet transform and genetic algorithm. Proceedings of the International Conference on Communications and Signal Processing, Feb. 10-12, IEEE Xplore Press, Calicut, pp: 42-45. DOI: 10.1109/ICCSP.2011.5739395

Huang, H.C. and F.C. Chang, 2013. Hierarchy-based reversible data hiding. Expert Syst. Applic., 40: 34-43. DOI: 10.1016/j.eswa.2012.07.010

Luo, W. F. Huang and J. Huang, 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inform. Forensics Securty, 5: 201-214. DOI: 10.1109/TIFS.2010.2041812

Mamta, J. and P.S. Sandhu, 2009. Designing of robust image steganography technique based on LSB insertion and encryption. Proceedigs of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 27-28, IEEE Xplore Press, Kottayam, Kerala, pp: 302-305. DOI: 10.1109/ARTCom.2009.228

Mishra, M. A.R. Routray and S. Kumar, 2012. High security image steganography with modified arnold's cat map. Int. J. Comput. Applic., 37: 16-20. DOI: 10.5120/4636-6685

Peng, F., X. Li and B. Yang, 2012. Adaptive reversible data hiding scheme based on integer transform. Signal Process., 92: 54-62. DOI: 10.1016/j.sigpro.2011.06.006

Reddy, H.S.M. and K.B. Raja, 2011. Wavelet based non LSB steganography. Int. J. Adv. Network. Applic., 3: 1203-1209.

Shivakumar, H.B., K. Raja, R.K. Chhotaray and S. Pattnaik, 2011. Performance comparison of robust steganography based on multiple transformation techniques. Int. J. Comp. Tech. Appl., 2: 1035-1047.

Yang, C.Y., C.H. Lin and W.C. Hu, 2012. Reversible data hiding for high-quality images based on integer wavelet transform. J. Inform. Hiding Multimedia Signal Proces., 3: 142-150.