Image Steganography Combination of Spatial and Frequency Domain

Saurabh V. Joshi
B.E. Computers

Ajinkya A. Bokil
B.E. Computers

Nikhil A. Jain
B.E. Computers

Deepali Koshti
M.E. Computers

ABSTRACT

Steganography is the art of hiding data inside a carrier file in such a way that an intruder or unwanted personnel is unable to detect the presence of data inside the carrier file. Audio, Video and Images are the different possible carrier files that can be used. This paper describes a steganographic technique which makes use of an image file as a carrier to hold the secret message and transfer it over the communication medium. There are two popular schemes used for image steganography: spatial domain embedding and transform domain embedding. Most of the steganographic techniques discussed in literature either use spatial domain or transform domain to embed the secret message. Here we have proposed a novel steganographic technique that combines both the spatial domain as well as the transform domain approach to achieve greater security. We have chosen LSB substitution technique for spatial domain embedding and Discrete Wavelet Transform (DWT) for transform domain embedding. The paper also proposes technique to combine cryptography with the proposed image steganography technique. Here we make use of the S-DES also known as the simplified DES algorithm for encryption. Our experimental results show that the proposed steganographic technique achieves moderate embedding capacity with high level of security.

KEYWORDS

Steganography, S-DES, DWT , Discrete Wavelet Transform, Carrier Image, Stego File, Stego Image, Brightness attack, Cropping attack.

1. INTRODUCTION

Steganography is a two-step process: Step 1) Creating a stego image which is a combination of message and carrier and Step 2) Extracting the message image from the stego image. Variations are in the techniques that are used to generate the stego image using the carrier and the message image. There are two popular schemes used for image steganography: spatial domain embedding and transform domain embedding.

The Least Significant Bit (LSB) substitution is the most commonly used spatial domain technique. In LSB substitution technique the least significant bit of each pixel of the cover is replaced by the secret message bits. Hiding images using LSB substitution techniques can be found in [1-4]. In transform domain technique, the transform is applied on cover image and the secrete message bits are hidden inside the coefficients of the transformed cover image. This method has been proved to be more robust than spatial domain techniques but is complex as compared to LSB techniques. Most commonly used transforms are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). Steganographic techniques using wavelet transform can be found in [5-9]. In all proposed techniques [1-9] whether spatial domain or transform domain, the major challenge is to increase the hiding capacity while maintaining the good visual quality of the cover image. Most of the steganographic techniques either use spatial domain or transform domain to embed the secret message. Here we have proposed a novel steganographic technique that combines both the spatial domain approach as well as the transform domain approach to achieve greater security. For our proposed system we have chosen LSB substitution technique while embedding using spatial domain and DWT while embedding using transform domain.

Figure 1 describes the typical scenario when using DWT. The image to which DWT is applied gets split up into 4 regions LL, LH, HL, and HH respectively. Of these regions LL region holds the visually more significant data whereas HH region holds the visually less significant data. On application of DWT to the carrier image, the high frequency components get separated from low frequency components which help us to achieve a convenient space to embed our message into it.

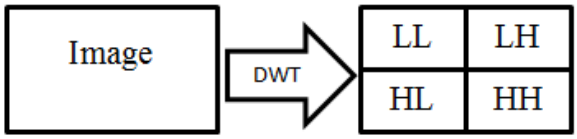


Figure 1 : DWT applied on Image

The remaining paper is organised as follows. Section2 discusses all four proposed approaches. Section 2.1 presents very basic approach of embedding data using DWT. In section 2.2 we present a technique to further improve embedding capacity by using two levels of DWT. Section 2.3 presents a novel technique that uses double layer of steganography by combining LSB substitution with DWT approach. Section 2.4 discusses the approach that combines cryptography and proposed steganographic scheme to further improve security. In Section 2.5 and 2.6 we have discussed variation of S-DES algorithm and LSB substitution techniques respectively. Section 3 discusses experimental results. Finally in section 4 we describe the conclusion.

2. PROPOSED APPROACHES

2.1 Approach1: Basic DWT

The most basic approach is to simply apply DWT to the carrier image and then the HH region of the carrier image is completely replaced by our message. Now apply inverse DWT on this modified carrier image to generate a stego image. Since HH region is visually less significant, replacement of this region does not generate observable distortions in the image and hence it can be successfully

treated as a stego image. However the embedding capacity granted by this approach is 25% of the cover image which is very low. So our approach takes a step further by replacing the LH and HL regions along with the HH region of the carrier image with our data. This has increased the embedding capacity up to 75%. This stego image is sent to the receiver who applies DWT to this image. The message pixels are extracted from the LH, HL and HH regions and then reshaped to obtain the original message back.

Figure 2 describes the technique graphically.

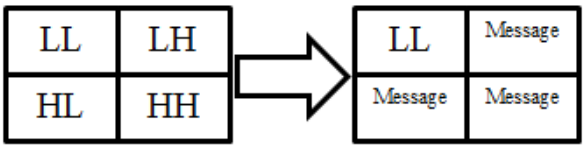


Figure 2 : Basic DWT approach

2.2 Approach2: Two Level DWT

The embedding capacity can be further improved by applying the second level of DWT to LL region which is generated after applying DWT to the entire carrier image. This generates four more regions, namely the LL1, LH1, HL1, and HH1 regions. Of these regions, the LL1 region now contains visually the most significant details whereas LH1, HL1, HH1 are still acceptable to be replaced. Hence we have successfully tried replacing these regions and the distortion in the carrier image is very low, typically not observable to human eye unless magnified using computing techniques. Thus second approach achieves 93.75% embedding capacity which is considered to be very high.

Figure 3 depicts the approach 2.

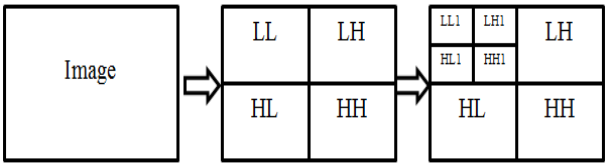


Figure 3 : Two level DWT

2.3 Approach3: Combination of Spatial and Frequency Domain Technique

Approach 1 and Approach 2 focus on improving the embedding capacity of the carrier image. The third approch focuses on providing security to the hidden data at the cost of reducing embedding capacity. The benefit is that even if an intruder gets to know the presence of hidden data; extracting the hidden data is still difficult for the intruder. This is achieved by using a double layer of steganography. Here the message image is embedded inside a carrier image by using LSB replacement technique which forms the inner stego image as shown in Figure 4. Now this inner stego image is treated as a new message and this inner stego image is hidden inside another carrier image using DWT approach to generate outer stego image (shown in Figure 5) which will be sent to the receiver. Here the inner stego image is embedded in the HH region that is obtained after applying DWT to the second carrier image. To retrieve the embedded message the receiver needs to apply DWT to the outer stego image. Then by using the HH region the receiver extracts the inner stego image after which an LSB extraction algorithm is applied to achieve the final message image.

Figure 4 : Inner Stego (LSB Replacement)

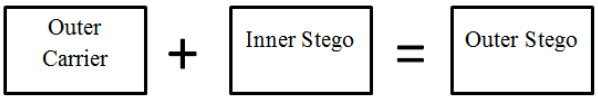


Figure 5 : Outer Stego (DWT Approach)

2.4 Approach 4: Combination of Cryptography and Steganography Scheme

Cryptography is a technique used to encode the data in such a way that even if the encoded data is visible its meaning is unknown to the intruder. A combination of Cryptography and Steganography is the crux of our last proposed approach in this paper. Here we make use of the S-DES also known as the simplified DES algorithm [10]. This algorithm has been chosen after appropriate analysis as it best suits our purpose of implementing security in Image Processing. In this approach the message image is subjected to the S-DES algorithm to generate an encrypted image. This encrypted image is hidden inside the carrier1 (inner carrier image) using LSB Replacement technique to generate inner stego image. Now, inner stego image is embedded inside the carrier2 (outer carrier image) by using DWT approach to generate outer stego image. Thus this approach combines two levels of steganography i.e. LSB replacement and DWT along with S-DES. Thus a moderate embedding capacity along with dual level of security is achieved.

2.5 Encryption Using S-Des

Our proposed system uses two variations of S-DES algorithm

1) The encryption and decryption keys are generated randomly.

2) The keys for encryption and decryption are generated by using the pixels of a key image. Here key image refers to an image whose pixel values are converted to bits and each pixel of message image is encrypted using keys obtained from every corresponding pixel of the key image.

2.6 LSB Replacement

To further improve security, instead of using simple LSB replacement our technique performs a bit-exor of bit from pixel of message image with the 7^{th} bit of pixel from carrier image and the exored result is hidden in the LSB i.e. 8^{th} bit. At the receiving end the 7^{th} and 8^{th} bits of the stego image are exored and the result obtained is treated as the corresponding message bit.

3. IMPLEMENTATION RESULTS

We have embedded a secret image in to a cover image using various approaches discussed above. Table I compares the PSNR and MSE values of all four approaches. Our experimental results show that all four approaches have very low MSE values for different cover images. Figure 6, figure 7 and figure 8 shows message image, cover image and resulting stego image for all four approaches.

3.1 APPROACH 1 and APPROACH 2

Figure 6 : DWT Approach

3.2 APPROACH 3

Figure 7 : LSB Replacement and DWT Approach

3.3 APPROACH 4

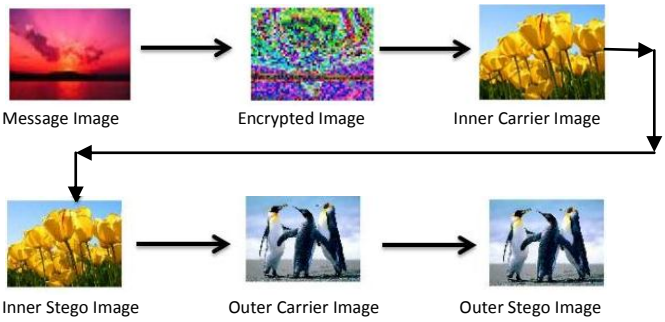
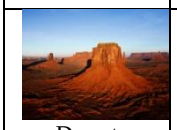


Figure 8: LSB Replacement and DWT along with S-DES

Table I: Comparison of all three approaches with respect to MSE and PSNR.

Carrier Image	Approach 1: Basic DWT		Approach 2 : Two Level DWT		Approach 3: LSB Replacement and DWT Approach		Approach 4: LSB Replacement and DWT along with S-DES	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
 Desert	0.14	56.63	0.36	52.49	7.78	39.21	9.29	38.44
 Flower	1.60	46.08	6.52	39.98	6.35	40.09	0.28	53.53
 Penguin	2.11	44.88	12.92	37.01	26.9	33.81	9.89	38.17
 Tulips	0.09	28.45	0.64	50.04	7.27	39.51	1.42	46.58

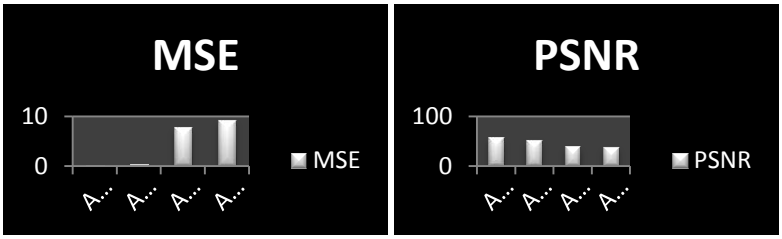


Figure 9: MSE and PSNR for Desert Carrier Image

Figure 10: MSE and PSNR for Flower Carrier Image

Figure 11: MSE and PSNR for Penguin Carrier Image

Figure 12: MSE and PSNR for Tulips Carrier Image

4. CONCLUSION

This paper introduces a novel concept of combining cryptography with steganography.

The proposed methods use a unique combination of steganographic methods in frequency domain and spatial domain. This helps to combine advantages and to overcome some of the disadvantages of both the domain schemes.

Approach 2 specified in this paper makes use of two level DWT which helps to achieve a considerably high embedding capacity because of the use of frequency domain.

Approach 3 enhances security of the system by first using LSB replacement technique of spatial domain and embedding the resultant in the carrier by using DWT.

Approach4 adds another level of security over approach 3 by first encrypting message image using S-DES algorithm. A unique method of encrypting each message pixel by using pixel values from a key image has been used.

5. 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] Dr.H. B. Kekre, Ms. Archana Athawale 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.

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

[5] R.O.EI Safy, H.H. Zayed and A. EI Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," International Conference on Networking and Media Convergence, 2009 (ICNM) 2009) on 24-25 March.

[6] 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.

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

[8] P. Chen and H. Lin, "A DWT Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4,3.

[9] M. Fahmy Tolba, M. Al-aid Ghonemy, Ismail AbDoul-Hammed Taha and Amal Said Khalifa, 'High capacity Image Steganography using Wavelet Based Fusion', @2004 IEEE.

[10] Sujay Narayana and Gaurav Prasad, 'Two new approaches for secured image steganography using cryptographic techniques and type conversions', International Journal (SIPIJ) Vol.1, No.2, December 2010.