Secret Image Sharing Scheme with Steganography and Authentication Based on Discrete Wavelet Transform

Akshay Girdhar, and Akwinder Kaur

***Abstract*—** Secret image sharing is a technique to protect the sensitive data. Secret image sharing combined with steganography and transform domain improves authentication ability. The primary objective of the paper is to design a novel algorithm for hiding the secret data in the transform domain. The underlying concept is based on the discrete wavelet transform. A technique comprising of Haar filter and wavelet based method is described for the secret image sharing. The discrete wavelet transform is used to embed the secret into the cover image and the inverse transform is used to recover the secret. The proposed technique provides robustness, better image quality and authentication ability. The stress is laid to improve the authentication ability of the secret image. The results have been compared with the state-of- the-art technique and the outcomes shows that the results are very promising. The system is intended to assist the programmers to give a second thought so that the data can be transmitted secretly.

***Keywords*—** Authentication, Discrete Wavelet Transform, Secret image sharing, Steganography.

I. Introduction

SECRET image sharing has gained popularity in the last few years and research has been done on different aspects.

With the rapid development of Internet and multimedia technology, digital images are of great significance nowadays. Secret image sharing is a technique to prevent a secret from malicious modification, destruction and unauthorized disclosure by splitting the secret into several shares and recovering the secret from sufficient shares [1]. Usually images are ideal for information hiding because a large amount of redundant space is created in the storing of images. The secret is transmitted through the hidden media in such a manner that the very existence of the secret becomes undetectable and thereby unnoticed to the naked eye.

Steganography means concealed writing. Steganography refers to the hiding of a secret behind the camouflage images. For hiding the data, there exist a variety of different techniques, but the proposed scheme uses the discrete wavelet transform to hide the data in the cover image and thereby shows promising results. The steganography techniques must satisfy: (a) the integrity of the hidden message after it has been embedded inside the cover object must be correct. (b) The cover object must remain unchanged or almost unchanged to the naked eye [2].

Akshay Girdhar, Associate Professor, IT Deptt., Guru Nanak Dev Engineering College, Ludhiana (Punjab), India

Akwinder Kaur, M.Tech. CSE Student, Guru Nanak Dev Engineering College, Ludhiana (Punjab), India

Guo and Georganas [3] introduced an algorithm that makes use of a generalized secret sharing scheme in cryptography to address the problem that multiple owners create an image jointly, distinct keys are given to only an authorized group of owners so that only when all the members in the group present their keys can the ownership of the image be verified. Any owner alone cannot verify the image ownership. In addition, experimental results showed that the proposed algorithm had the desired properties such as invisibility, reliable detection, and robustness against a wide range of image-processing operations. Lin and Tsai [4] proposed a secret image sharing method by selecting the number of authentication bits proportional to block size, contrary to method which uses four bits to authenticate blocks regardless of the block size. The method improved authentication for increased block size and can authenticate individual stego blocks as well. It produced good quality stego images.

Chang et al. [5] presented a steganographic method for embedding a color or a grayscale image in a true color image. Three types of secret images could be carried by the proposed method: hiding a color secret image, hiding a palette-based 256-color secret image, and hiding a grayscale image in a true color image. Secret data are protected by the conventional crypto system data encryption standard (DES).

In order to improve the robustness of steganography Ghasemi et al. [6] discussed the application of wavelet transform and genetic algorithm in a novel steganography scheme. A genetic algorithm based mapping function to embed data in discrete wavelet transform (DWT) coefficients in 4x4 blocks on the cover image is employed. The optimal pixel adjustment process is applied after embedding the message.

Singh et al. [7] discussed about the steganography technique based on mainly the joint photographic expert group (JPEG). This technique is based on the 2-D Block-discrete cosine transform (DCT), where DCT was used to transform the original image (cover image) blocks from the spatial domain to frequency domain.

Zhang et al. [8] presented a robust method for restoring embedded image from corrupted stego image. This method provides good visual quality. For each corrupted pixel, its value is corrected by adjusting the unreliable bits.

Wu and Sun [1] developed a meaningful secret image sharing scheme with authentication and remedy abilities. One dimensional cellular automata, DWT and the hash function are adopted in this scheme. The stego images are allowed to be verified to determine whether they are tampered or not. Once they are tampered, shared bits retrieved from these tampered areas cannot be used to reconstruct the secret image.

http://dx.doi.org/10.15242/IIE.E1213594

The aim of the proposed paper is (a) To design an algorithm for hiding the secret data into the transform domain. (b) To remove the noise from the corrupted stego image during transmission. Novelty in our work is that the proposed paper proves to be better in terms of visual quality, possesses lesser errors.

This paper is organized as follows: Section II discusses the proposed scheme in detail. Section III discusses the achieved results and compares the proposed scheme with the state of the art algorithms. Section IV concludes the paper.

II. Proposed Scheme

The proposed scheme is based on steganography and authentication. For steganography, the proposed technique embeds the secret message into the cover image by using the discrete wavelet transform. The aim of using DWT is that it transforms the discrete signal from the time domain into the frequency domain. Due to the multi-resolution nature of the wavelet transforms, the DWT yields high compression ratios and better visual quality.

To prevent the unauthorized persons from tampering the secret message signal, the authentication mechanism has been adopted. The authentication mechanism works in such a manner that if the secret message has been tampered then it cannot recover that secret during the extraction phase. So the authorized owner comes to know that the secret has been modified [9]. Usually, such incidental provision of false stego images are considered to be simple manipulations on the stego images such as tampering or cropping. This assumption is adopted in the related studies [5] as well.

The prerequisite to the proposed technique is that cover image and the secret image should have the same size.

In general, the proposed technique consists of these phases: (a) embedding phase, (b) authentication phase, (c) extraction phase, (d) restoration phase.

A. Embedding Phase

In the embedding phase, the secret message signal is embedded into the cover image using the Haar DWT.

Fig.1 shows the embedding procedure being followed. Initially, the cover image is used and Haar wavelet transform is applied to it. A 2-dimensional Haar-DWT consists of two operations: one is the horizontal operation and the other is the vertical one. Before embedding the secret into the cover image, the message signal is distorted by applying randomization. The technique of randomization scatters the secret throughout the whole surface so that the secret cannot be easily identified [10]. Further the result of Haar wavelet transform and message signal is combined in order to get the resulting stego image. The embedding is such that first the visual quality of the results has no serious downtrend, and second it is difficult to recognize that any data is hidden in the stego images. The embedding procedure satisfies both of these requirements [11].

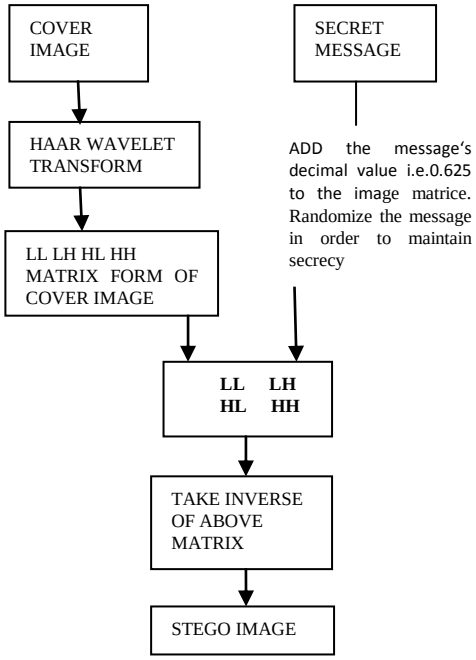


Fig.1 Embedding Model

B. Authentication Phase

In the authentication phase, the dealer can verify whether the stego images provided by the owner are tampered or not [12]. The verification procedure involves that if the secret has been tampered then during the extraction phase, the dealer would not be able to retrieve the original secret. The proposed technique enhances the data security by secret sharing. Instead of hiding data directly into the cover image pixels, the proposed technique embeds data in the form of scattered pixels.

C. Extraction Phase

In the extraction phase, the secret has to be recovered from the stego image received by the receiver.

Fig.2 shows the extraction procedure being followed. The cover image is decomposed into multi-resolution subbands [13]. The inverse DWT is applied to the stego image. The subbands of the cover image and stego image are subtracted in order to retrieve the secret. Thresholding is performed in order to regain the pixels which have been tampered due to noise addition. During the extraction phase, the stego image and the cover image are taken to recover the secret.

D. Restoration Phase

Digital images are easily corrupted by noise during transmission [1]. Firstly, identify unreliable bits i.e. the bits that have been altered in order to tamper the secret of each pixel in the embedded image by detecting noise in the stego image. Secondly, it determines corrupted pixels. For each corrupted pixel, the value of the corrupted pixels is corrected by adjusting the tampered bits. Restoration implies recovering the secret without any noise.

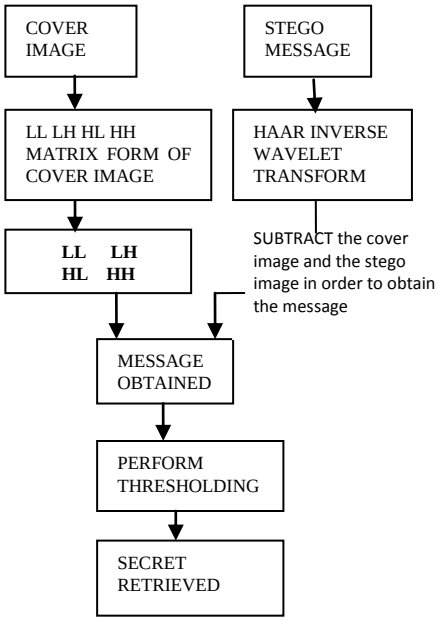


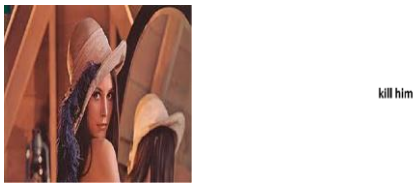
Fig.2 Extraction Model

III. Performance Analysis

The cover images of 512 x 512 size and payload images are considered in the different formats.

Fig.3 shows the cover image and the payload image. After the embedding phase, the resultant stego image appears named as wimage.fits. The fits format is better than JPG as it stores the thresholding values in terms of double, not as an 8-bit digit.

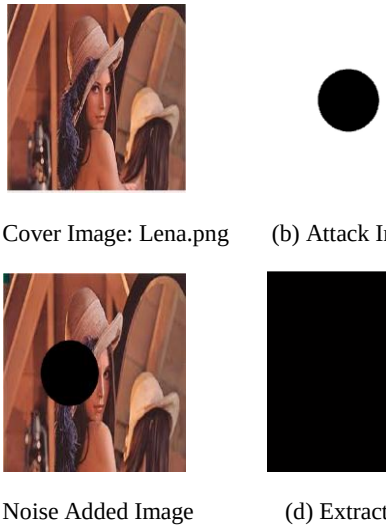
(a) Cover Image: Lena.png (b) Payload Image: M1.jpg



(c) Stego Image: wimage.fits (d) Extracted Payload

Fig.3 Cover image Lena.png and Payload image M1.png

In case of attack by an unauthorized person, the results are demonstrated in Fig.4. Some noise is put onto the image of Fig.4 (a) , as an intended attack to the image, yielding the noisy image of Fig.4 (c) which is then authenticated by the proposed technique and the result is shown in Fig.4 (d). The secret is not retrieved when it has been altered [8]. So a blank image appears authenticating that the secret has been tampered.

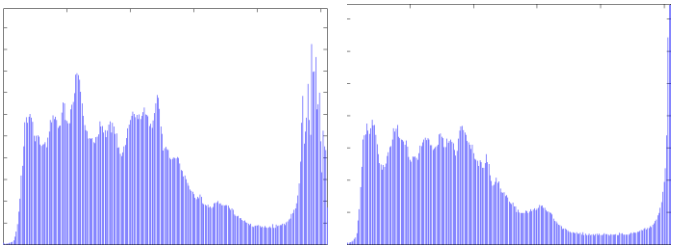


(a) Cover Image: Lena.png (b) Attack Image: A1.jpg

(c) Noise Added Image (d) Extracted image

Fig.4. Cover Image Lena.png and Attack Image A1.jpg

Fig.5 illustrates the histograms generated in case of the proposed technique and the existing technique [1], taking the test image to be stego image generated by Lena.png. The proposed technique results in a brighter image as there are more data points on the right side and center of the graph.



(a) Proposed Technique (DWT) (b) Existing Technique (DCT)

Fig.5 Comparison based on Histogram of the stego image

Table I shows the Peak Signal-to-Noise Ratio (PSNR) values of cover image and stego image as well as of the extracted payload and original payload. The distortions present in the stego image are calculated using Peak Signal-to-Noise Ratio (PSNR).

TABLE I
PSNR Values

Cover Image	Payload	PSNR dB (Cover image to stego image)	PSNR dB(payload to extracted payload)
Lena.png	M1.jpg	41.24	56.81
Home.jpg	M1.jpg	49.65	56.81

dB:Decibel

Table II shows the comparison of PSNR and mean square error (MSE) for the secret image sharing using DCT and the proposed technique based on DWT. The PSNR and MSE values have been computed using the images given in Fig.3.

The technique with smallest variance is the best prediction in the sense that it minimizes the variance. The proposed technique has a lesser MSE as compared to existing technique [1].

Higher PSNR indicates that the reconstruction is of higher quality. Thereby the proposed technique has higher PSNR and provides better image quality.

TABLE II
COMPARISON OF PSNR AND MSE

Comparison	Algorithm	MSE	PSNR dB(Cover image to stego image)
Existing Technique [1]	Discrete Cosine Transform	16.87	20.67
Proposed Technique	Discrete Wavelet Transform	7.46	41.24

IV. CONCLUSION

This work dealt with the secret image sharing scheme in the DWT domain as related to image science. A new and efficient secret image sharing technique for embedding the secret messages into images without producing any major changes has been proposed. For comparative study, it has been seen that this technique is better than technique proposed by Wu and Sun (DCT based technique) in terms of image quality and tampering results. Embedding capacity of this technique is much better than the existing techniques in the frequency domain such as DCT. Beside this technique provides robustness which can avoid various image attacks, noise addition. Hiding secret data into the transform domain (e.g., embedding data into the quantized DWT coefficients) is promising, but more issues such as the hiding capacity can be further studies. These can be the future work of the proposed technique.

REFERENCES

[1] X. Wu and W. Sun, "Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform," Journal of Systems and Software, vol. 86, no. 4, pp. 1068-1088, 2013. http://dx.doi.org/10.1016/j.jss.2012.11.021

[2] H. S. M. Reddy and K. B. Raja, "High Capacity and Secure Steganography Using Discrete Wavelet Transform," International Journal of Computer Science and Security, vol. 3, no. 6, pp. 462-472, 2010.

[3] H. Guo and N. D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme," Multimedia Systems, vol. 9, no. 3, pp. 249-260, 2003. http://dx.doi.org/10.1007/s00530-003-0096-1

[4] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication,"Journal of Systems and Software, vol. 73, no. 3, pp. 405-414, 2004. http://dx.doi.org/10.1016/S0164-1212(03)00239-5

[5] Y. H. Yu, C. C. Chang and I. C. Lin, "A new steganographic method for color and grayscale image hiding," Computer Vision and Image Understanding, vol. 107, no. 3, pp. 183-194, 2007. http://dx.doi.org/10.1016/j.cviu.2006.11.002

[6] E. Ghasemi, J. Shanbehzadeh and N. Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," Proceedings of the International Multiconference of Engineers and Computer Scientists, vol. 1, pp. 16-18, March 2011.

[7] M. Singh, R. Sharma and D. Garg, "A New Purposed issue for Secure Image Steganography Technique based on 2-D Block DCT and DCT," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 29-33, July 2012.

[8] X. Zhang, T. Liang, Z. Tang and X. Dai, "Restoration of embedded image from corrupted stego images," Signal Processing, vol. 92, no. 7, pp. 1691-1698, 2012. http://dx.doi.org/10.1016/j.sigpro.2012.01.004

[9] C. N. Yang and C. B. Ciou, "A Comment on "Sharing secrets in stegoimages with authentication"," Pattern Recognition, vol. 42, no. 7, pp. 1615-1619, 2009. http://dx.doi.org/10.1016/j.patcog.2009.01.024

[10] M. T. Parvez and A. A.-A. Gutub, "RGB Intensity Based Variable-Bits Image Steganography," in APSCC, IEEE, 2008, pp. 1322-1327.

[11] C. L. Liu and S. R. Liao, "High-performance JPEG steganography using complementary embedding strategy," Pattern Recognition, vol. 41, no. 9, pp. 2945-2955, 2008. http://dx.doi.org/10.1016/j.patcog.2008.03.005

[12] C. C. Chang, Y. H. Chen and H. C. Wang, "Meaningful secret sharing technique with authentication and remedy abilities," Information Sciences, vol. 181, no. 14, pp. 3073-3084, 2011. http://dx.doi.org/10.1016/j.ins.2011.03.002

[13] H. S. M. Reddy and K. B. Raja, "Wavelet based Secure Steganography with Scrambled Payload," International Journal of Innovative Technology and Exploring Engineering, vol. 1, no. 2, pp. 121-129, July 2012..