Digital Image Steganography: An FFT Approach

Conference Paper *in* Communications in Computer and Information Science · April 2012

DOI: 10.1007/978-3-642-30567-2_18

Tamer Rabie
University of Sharjah

Digital Image Steganography: An FFT Approach

Tamer Rabie

Canadian University of Dubai,
School of Engineering, UAE
tamer@cud.ac.ae

Abstract. This work describes a framework for image hiding that exploits spatial domain color properties of natural images combined with spectral properties of the Fourier magnitude and phase of these images. The theory is that as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, double the capacity of previous methods, higher security, and robustness to tampering. Experimental results are presented throughout the paper which demonstrate the effectiveness of this novel approach.

Keywords: Steganography, Fourier Magnitude, Fourier Phase, Image Hiding.

1 Introduction

The proliferation and exchange of multimedia data over the internet and wireless networks has brought with it new prospects for covert communication. Data hiding techniques, commonly known as steganography, when dealing with hiding secret messages in a cover media [18], [20], [17], or watermarking when copyright protection of multimedia data is involved [29], have received a great deal of attention in recent years [2], [25], [10], [12], [13].

Techniques for data hiding inside digital images have been generally confined to one popular approach, namely the manipulation of the Least Significant Bit (LSB) of an image pixel value and the rearrangement of image colours to create LSB or parity bit patterns, which correspond to the message being hidden [4], with variants that try to improve three different aspects; capacity, security, and robustness [3]. Capacity refers to the amount of information that can be hidden in the cover medium, security refers to an eavesdropper's inability to detect hidden information, and robustness refers to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

This paper builds on the original frequency domain data hiding framework first introduced by the author in [20], [21] which exploits spectral properties of the Fourier magnitude and phase of natural images which has allowed for a fresh new approach to image hiding in the frequency domain.

R. Benlamri (Ed.): NDT 2012, Part II, CCIS 294, pp. 217–230, 2012.

2 Background

The importance of Fourier magnitude and phase of the carrier image, as related to the problem of data hiding and watermarking, has been rarely discussed in the literature [26], [8], [23],[16]. In the early work of [23] they introduce the notion of data hiding in images in which only the magnitude of the discrete Fourier transform (DFT) coefficients are altered to embed the hidden information bits. While this technique proposes a similar idea to our approach, it differs completely in the actual methodology. In [8], a method of data embedding based on the convolution of the hidden message data with a random phase carrier is presented with results that promise robustness to printing and scanning. The shortcomings of that technique, which bears no resemblance to the novel approach discussed in this paper, is the requirement of a phase carrier which must be deconvolved from the cover host image to reveal the hidden message.

3 Significance of Magnitude and Phase

It is well known that for many images, the phase of the Fourier transform is more important than the magnitude [9], [14], [15], [23]. Specifically if

$$F(u,v) = |F(u,v)|.\exp(j.\theta(u,v)) \tag{1}$$

denotes the two-dimensional (2D) Fourier transform of an image *f(x,y),* then the inverse Fourier transform of the phase of this 2D signal *exp(j.θ(u,v))* has many recognizable features in common with the original signal, whereas the inverse Fourier transform of the magnitude |*F(u,v)*| generally bears no resemblance to the original. This is illustrated in figure 1 where figure 1-(a) is an RGB color image and figure 1-(b) is the phase-only image, i.e., the inverse Fourier transform of *exp(j.θ(u,v)).*

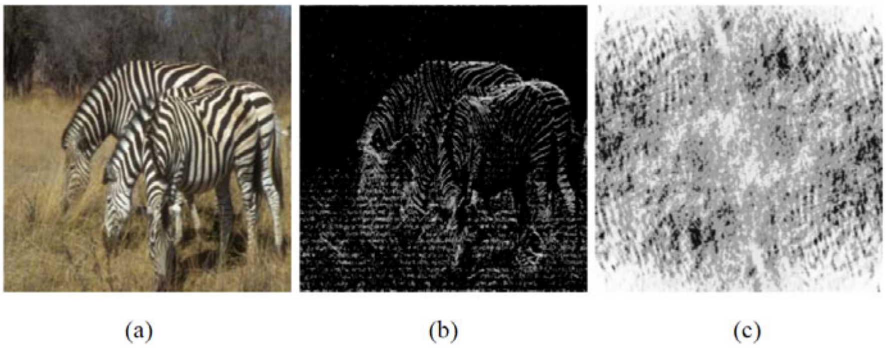


Fig. 1. (a) Zebras image, (b) Inverse Fourier transform of exp(j.θ(u,v)) (the phase-only image of the Red-channel of the Zebras image). (c) Inverse Fourier transform of |F(u,v)| (the magnitude-only image of the Red-channel of the Zebras image).

Clearly, the phase-only image retains many of the features of the original. By contrast, the magnitude-only image, i.e., the inverse Fourier transform of |*F(u,v)*|, shown in figure 1-(c), bears no resemblance to the original image. As is evident in this example, the phase-only image often has the general appearance of a high-pass filtered version of the original with additive broadband noise.

The importance of phase also extends to one-dimensional signals. It has been shown that the intelligibility of a speech sentence is retained if the inverse transform of the Fourier phase of a long segment of the speech signal is combined with unity magnitude to obtain the phase-only equivalent speech [14]. In fact, in listening to this processed sentence, total intelligibility is retained although the speech has the general quality associated with high-pass filtering and the introduction of additive white noise. The magnitude-only speech has some structure which provides a speech like characteristic but with no speech intelligibility.

4 Fourier Magnitude Information Hiding

The discussion in the previous section suggests that, as long as the Fourier phase of an image is maintained intact, the overall appearance of an image remains specious if the Fourier magnitude of the image is slightly modified. This hypothesis leads to a data hiding technique that promises high fidelity, capacity, security, and robustness of hidden message embedding and extraction which allows a virtually unsuspicious stego image to be transmitted unnoticed. The word stego will be used throughout the paper to describe the carrier image after having the hidden message embedded inside it.

The extent to which the Fourier magnitude of the carrier image can be overloaded (with the hidden message embedding) depends on the amount of degradation that one is willing to allow to the stego image. Experimental results show that a typical hidden message image may be as large as half the size of the carrier image for an unnoticeable amount of noise artifacts in the stego image.

Our choice of a carrier image is influenced by the most common image type exchanged over the internet, namely the Joint Photographic Experts Group (JPEG) image format. We thus start with a 24-bit Red, Green, Blue (RGB) color JPEG image as the carrier. One of the major concerns with typical data hiding techniques that use RGB color carrier images is the visible artifacts that may occur in the stego image due to embedding data directly in the individual (R,G,B) channels (which alter the carrier's LSB of color values in common data hiding techniques). To overcome this potential problem, which compromises the security and raise suspicion of hidden data in the image, we adopt a color/brightness (also known as chrominance/luminance) separation strategy.

There are several advantages to the separation of color from brightness information in image processing. Perceptual experimental evidence has established that the human visual system has a much higher sensitivity to changes in brightness than to color. Moreover, there seems to be general agreement that spatial resolution is markedly lower in chromatic (chrominance) channels than in the achromatic (luminance) one, hence high frequency information, i.e. fine details and edges, come mainly from the luminance channel [27], [5]. Thus, in developing our data hiding framework we avoid altering the luminance information in the carrier image altogether. This is a stark shift from mainstream data hiding techniques used today.

We choose to separate the color carrier image using the CIE *L*a*b** color space [24], [11]. *L*a*b** space is a nonlinear transformation of *RGB* space that specifies color in terms of human perception in a way that is independent of the characteristics of any particular imaging device. The *L*a*b** color space separates the *RGB* image into a luminance channel (*L*), and two chrominance channels (*a, b*). In general the luminance channel suffers less noise artifacts than the chrominance channels [22]. Detailed information about the CIE color spaces can be found on their website at http://www.cie.co.at.

These luminance/chrominance properties discussed above prompt us to embed two hidden messages inside the Fourier magnitude of the chrominance channels (one hidden message in the chrominance-*a* channel and a second hidden message in the chrominance-*b* channel) while preserving the luminance channel unaltered for optimal visual quality. This has an added advantage of reduced noise artifacts in the stego image with zero degradation in the original intensity brightness values, as well as increasing the capacity of data hiding by embedding double the amount of data since we are embedding in two chrominance channels instead of one luminance channel. The 2D Fourier transform of both the chrominance-*a* and chrominance-*b* channels are first computed and the magnitude spectrum is separated from the phase spectrum. Let *Ca(u,v)* be the Fourier transform of the chrominance-*a* channel and *Cb(u,v)* be the Fourier transform of the chrominance-*b* channel of the carrier image which can be expressed in polar form as:

$$\begin{aligned} \mathrm{Ca(u,v)} &= \mathrm{Ma(u,v).exp(\ j.\theta a(u,v)\ )}\ , \\ \mathrm{Cb(u,v)} &= \mathrm{Mb(u,v).exp(\ j.\theta b(u,v)\ )} \end{aligned} \tag{2}$$

where $Mx = |Cx(u,v)|$ is the chrominance spectral magnitude of channel *x*, and $\theta x(u,v)$ is its phase.

The technique used to embed a hidden message image into the Fourier magnitude of the chrominance channels of the carrier image is to replace the high-frequency areas in the Fourier magnitude spectrum with the values of the hidden message's image. This type of embedding prevents aliasing of the hidden message when extracted (which appears as a mirroring of parts of the hidden image from one side onto the opposite side and causes data loss). Figure 2 shows the 'before' and 'after' figures of the chrominance-*a* magnitude spectrum of a typical carrier image (figure 2-(a)) when a hidden message image is embedded in the high frequency areas of this magnitude spectrum to produce a modified chrominance-*a* magnitude spectrum (figure 2-(b)).

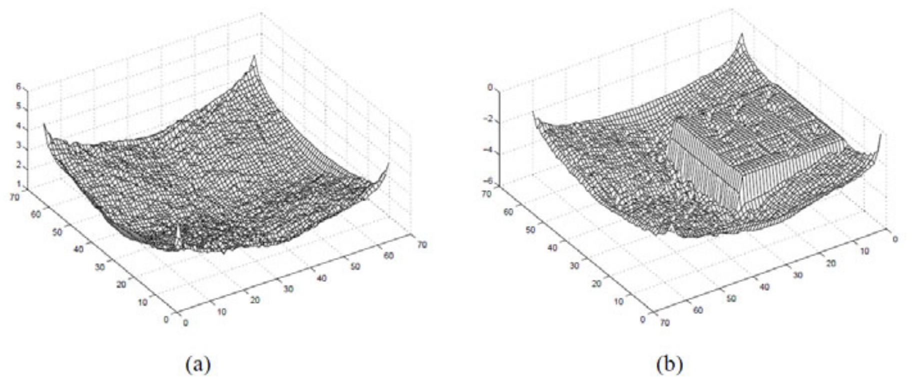


Fig. 2. (a) A typical chrominance-a magnitude spectrum of the original carrier image before embedding occurs and (b) the embedded hidden image message in the high frequency region of this magnitude spectrum

Similarly a second hidden message image is embedded in the high frequency areas of the chrominance-*b* magnitude spectrum of the same carrier image to produce the modified chrominance-*b* magnitude spectrum. These modified chrominance Fourier magnitudes *Ma'(u,v)* and *Mb'(u,v)* are then combined with the complex Fourier phase of the original chrominance channels to produce the Fourier stego spectrum of the chrominance channels as shown in equation (3), which when transformed back to the spatial domain gives us a modified chrominance-*a* channel (*a'*) and a modified chrominance-*b* channel (*b'*). Combining this with the *L* channel (*L,a',b'*) and transforming back to the (*R,G,B*) color space, will produce the space-domain stego image which contains the hidden information. This is clearly depicted in the diagram of figure 3.

$$\begin{aligned} Ca'(u,v) &= Ma'(u,v).\exp(\, j.\theta a(u,v)\,) \\ Cb'(u,v) &= Mb'(u,v).\exp(\, j.\theta b(u,v)\,) \qquad (3) \end{aligned}$$

5 Recovery of Hidden Information

Extraction of the hidden message image takes place in reverse order to the hiding process. Referring to figure 3 (bottom-up), first the (R,G,B) stego image is converted to the L*a*b* color space and the chrominance-*a* and chrominance-*b* channels are separated from the Luminance channel. The 2D Fourier transform of these extracted chrominance-*a,b* channels are then computed and their magnitude spectra are separated from their phase spectra. It is these magnitude spectra that contain the hidden secret images. The first hidden image is extracted from the high-frequency areas in the Fourier chrominance-*a* magnitude spectrum and the second hidden image is extracted from the high-frequency areas in the Fourier chrominance-*b* magnitude spectrum, making sure that the for-loop that is used to extract the hidden images is the same for-loop that was used to embed these hidden images.

This embedding-extraction loop can be considered as a security *key* for recovering the hidden data. Without knowing the correct embedding loop, it becomes a guessing game for successfully recovering the hidden information.

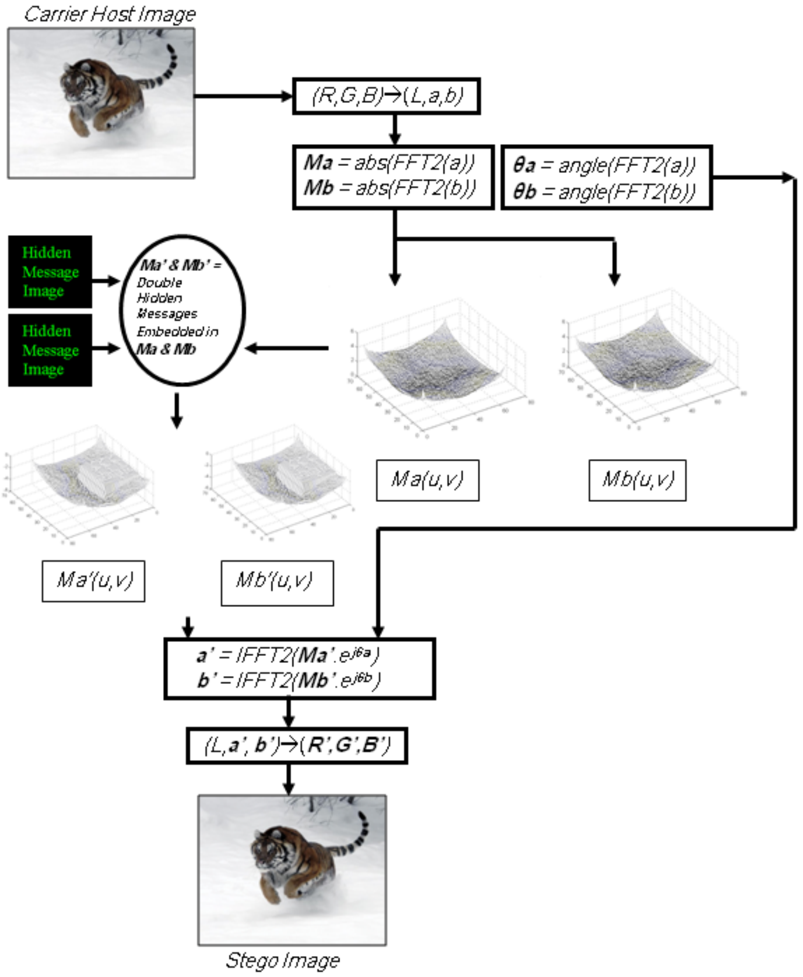


Fig. 3. Block diagram showing the general steganography algorithm used to hide two message images inside the Fourier magnitude spectra of the chrominance-a and chrominance-b channels of the carrier image respectively after separating luminance from color information to preserving the luminance channel unaltered for optimal visual quality of the generated stego image

To accurately compare our FFT-based data hiding techniques described in this paper with the most common methods used for data hiding it becomes necessary to assess the data loss issues (fidelity of stego and recovered data) that are inherent in steganography algorithms. Steganographic systems that modify least-significant bits of the carrier image are often susceptible to visual attacks [28]. Visual attacks mean that one can see steganographic messages on the low bit planes of an image because they overwrite visual structures, which exists to some degree in all the image's bit layers; this usually happens in BMP and GIF images. This is not true for our Fourier magnitude steganography method. The data hiding takes place in the frequency domain, and only the magnitude spectrum of the chrominance-*a* and chrominance-*b* channels of the carrier image are modified, leaving the luminance channel unaltered.

Suspicious visual pattern artifacts may occur when data hiding takes place in the FFT magnitude of the luminance channel instead of the other two chrominance channels (figure 4-top). For our FFT-based technique, the implication of embedding two hidden images in the high frequency areas of the Fourier magnitude of the chrominance-*a,b* channels is an additive noise component in the spatial domain of the chrominance-*a,b* channels which appear as minor color artifacts in the stego image. The amplitude of the noise that appears in the stego image is proportionate to the variance of the hidden message image. The smaller the changes in the hidden image, the lower the noise that affects the colors of the stego image, and vice versa.

Figure 4 shows a comparison between embedding a kitten 8-bit gray scale image (256 gray levels) in the high-frequency areas of the Fourier magnitude of the luminance channel (luminance stego shown in the top image set) and the same hidden kitten image embedded in the Fourier magnitude of the chrominance-*a* channel while not hiding any message in the chrominance-*b* channel for the sake of comparison with Luminance hiding (chrominance-*a* stego image shown in the middle image set). Looking at both the luminance and chrominance-*a* stego images it is clear that embedding the kitten gray scale image in the Fourier magnitude of the chrominance-*a* channel produces significantly less artifacts in the resulting stego image. Also when extracting the hidden kitten image it is very clear that the extracted kitten image from the chrominance-*a* stego image (bottom right image) has less noticeable artifacts in it than the extracted kitten image from the luminance stego image (bottom left image). Only when magnifying the chrominance-*a* stego image that one starts to see very unnoticeable color artifacts that do not affect the image and are unsuspicious, while it is clear from the magnified luminance stego image that it exhibits severe pattern noise artifacts that are much more suspicious.

Figure 5 shows the results of embedding two 8-bit gray scale hidden images; the first is the kitten image and the second is a hand writing image, into the 24-bit Tiger color carrier image. The resulting color stego image shown in figure 5-(top) has no suspicious degradation which is visually confirmed from the high fidelity of the color stego image. Figure 5-(bottom) shows the two extracted hidden images from the color stego of figure 5-(top). It is clear that the extracted hidden images maintain their high quality and suffer minor degradations.

6 Security Levels

The data hiding process presented in this paper is based on manipulating spectral magnitude multiplied by spectral phase of color images (see equations (1) and (2)), which is equivalent to manipulating the convolution of the spatial-domain magnitude image with the spatial-domain phase image (such as those in figure 1(b) and (c)). This has the effect of scattering the hidden image three times across all pixels of the carrier image; once when the embedded hidden image is transformed together with its magnitude spectrum host from the frequency domain to the space domain, and secondly, when this magnitude image is convolved with the phase image to produce the stego chrominance-*a* channel image, and finally when the colour stego (*L,a,b*)-based image is transformed to the (*R,G,B*) color space, effectively distributing the hidden image information in the chrominance-*a* channel to all (*R,G,B*) channels, further enhancing the security of the final stego image. This FFT-based steganography method, thus, provides a three-layer security measure that can be exploited in secure data transmission over insecure networks.

7 Robustness to Stego Medium Tampering

To demonstrate the robustness of this image hiding technique to tampering degradations in the stego image, we simulate different tampering effects and attempt to extract the hidden image from the tamper-degraded stego image. We present a series of tampering applied to a red rose flower stego image which was embedded with the handwriting message image. The left column of figure 6 shows a series of Flower stego images with increasing areas of the images being removed. The right column of the figure shows the corresponding extracted hidden handwritten message images. It is clear that up to a 60% loss in the data of the stego image we will still be able to extract a relatively legible hidden message image, while at 98% data loss, the ghost of the image is still there but obviously unreadable. In these cases, a qualitative evaluation of the extracted hidden message image is more important than quantitative numbers, and clearly this image hiding technique works for severe cases of data loss in the stego image.

Finally, in figure 7, we show two more tampering examples on the Flower stego image and the resulting extracted hidden message image. Figures 7-(a) and (b) show the Flower stego image with repaint tampering, and the corresponding extracted hidden message images. It is clear that even though with the increase in repaint tampering in the stego images, a corresponding increase in degradation occurs in the extracted hidden message images, the extracted handwritten message images are still legible to a high degree.

Figure 7-(c) shows a tampered Flower stego image where the central area of the Flower is rotated by 90 degrees, and the corresponding extracted hidden message image. Figure 7-(d) shows an extreme case of rotation tampering where 80% of the Flower stego image is flipped vertical. The corresponding extracted hidden message image shown has been flipped horizontally after extraction from the tampered stego image to remove the mirror effect in the handwritten text due to the vertical flip of the stego image. In all these cases the extracted handwriting is still readable which demonstrates the robustness of our technique to these different types of tampering.

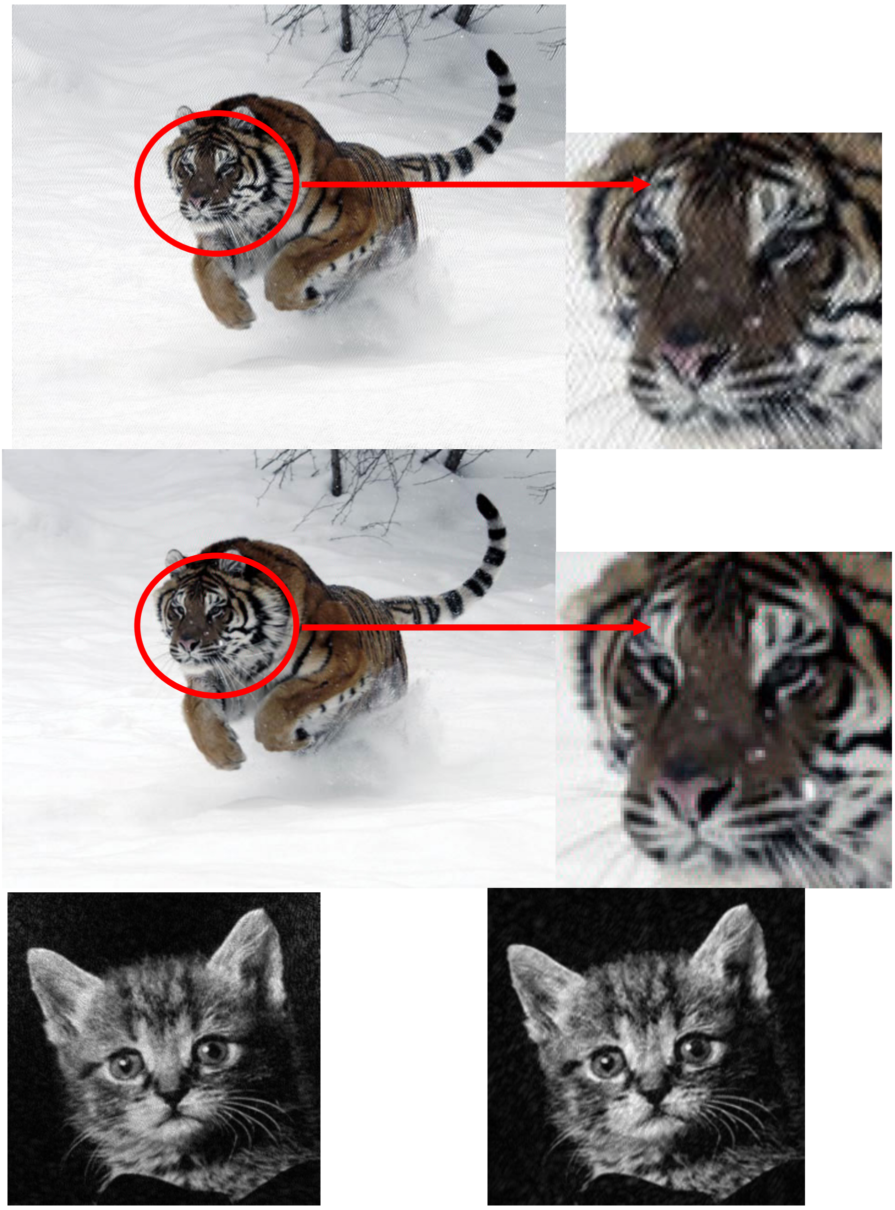


Fig. 4. (Top) Luminance stego image showing severe pattern artifacts, and (Middle) Chrominance_a stego image showing unnoticeable color artifacts, (Bottom Left) extracted kitten image from Luminance stego, (Bottom Right) extracted kitten image from Chrominance_a stego image

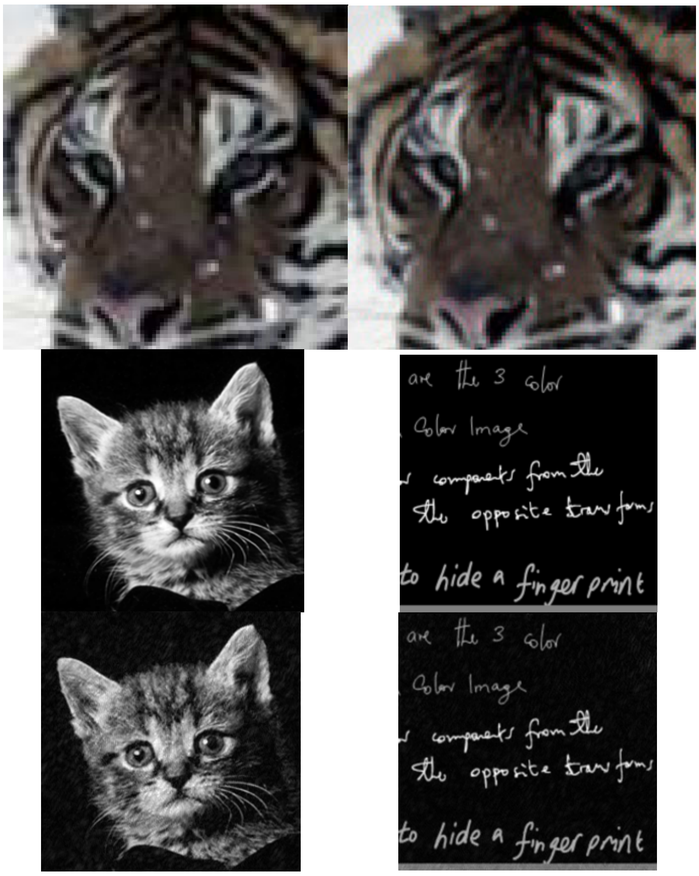
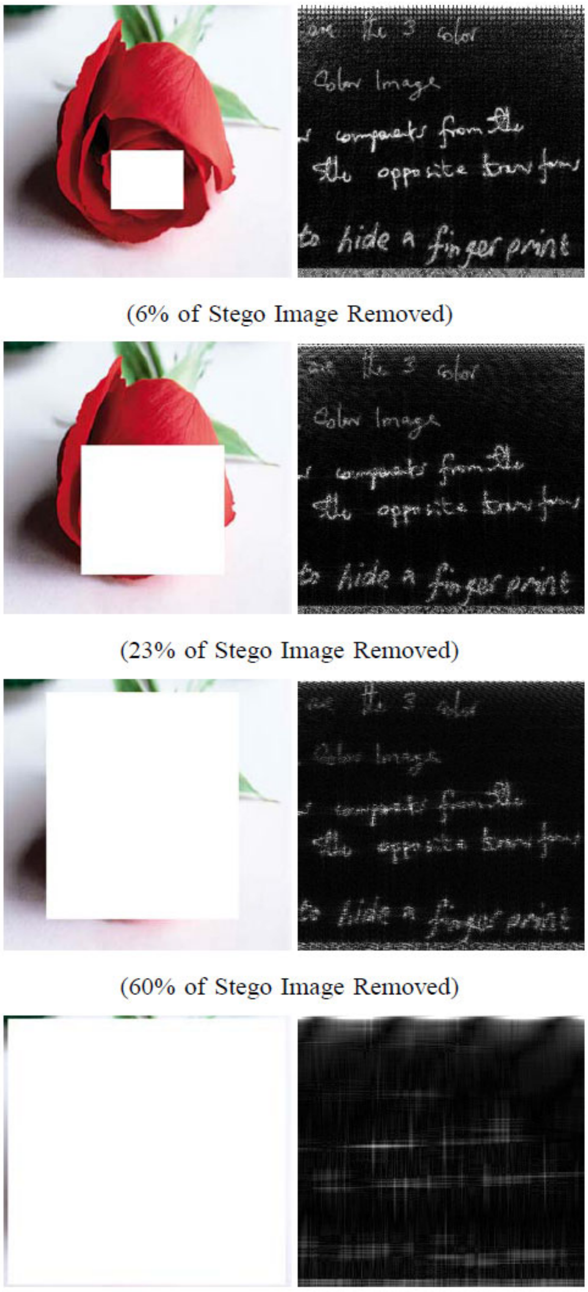


Fig. 5. (Top Left) Magnified area of original Tiger host image, (Top Right) Magnified area of the stego image with two different gray scale images embedded in its Chrominance_a and Chrominance_b spectra, showing unnoticeable color artifacts due to embedding the two hidden images, (Middle) Original Kitten and Hand Writing hidden images, (Bottom Left) extracted Kitten image from Chrominance_a and (Bottom Right) extracted Hand Writing image from Chrominance_b, both showing minor degradations due to the embedding/extracting process



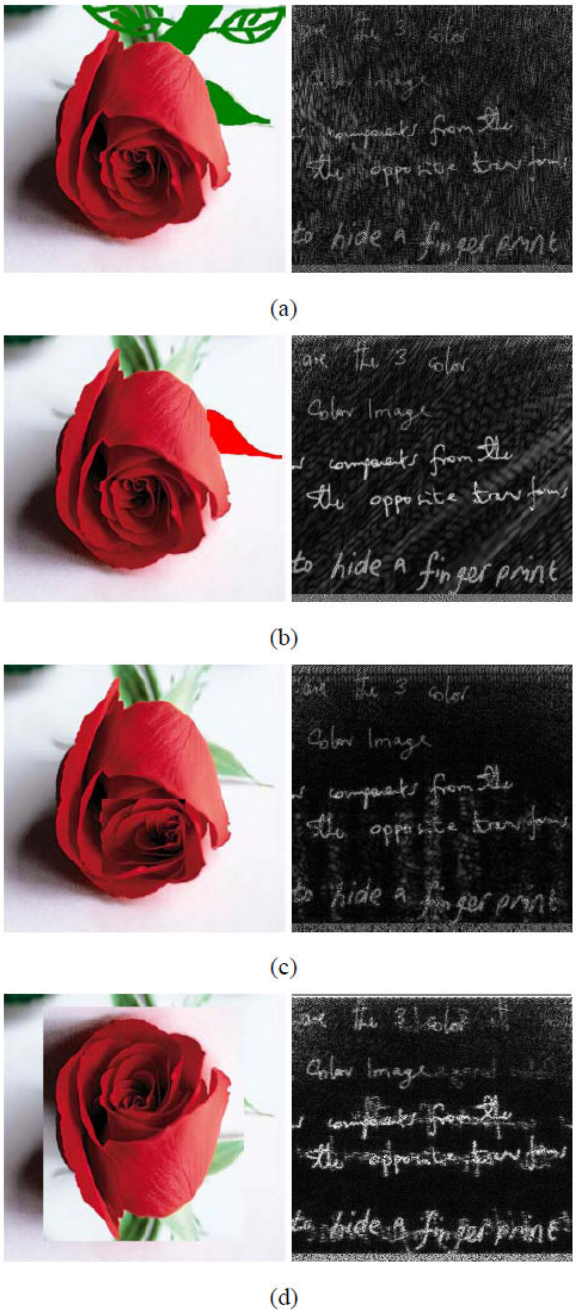
(6% of Stego Image Removed)

(23% of Stego Image Removed)

(60% of Stego Image Removed)

(98% of Stego Image Removed)

Fig. 6. A series of Flower stego images with increasing data loss tampering and their corresponding extracted hidden message images



(a)

(b)

(c)

(d)

Fig. 7. The Flower stego image with repainting and rotation tampering, and their corresponding extracted hidden message images

To understand how this image hiding technique is robust to these types of severe tamperings, we must recall that the hidden message image is not simply embedded in the individual pixels of the space-domain carrier image, but rather, in the frequency spectrum of the magnitude of the chrominance-*a* channel of the carrier image, and, as explained earlier, this is equivalent to scattering the hidden message image data over all the carrier image pixels. This explains why when 60% of the stego image data are lost or removed we can still retrieve the hidden message, albeit with some degradations. In other words, as long as 40% or more of the stego image data remains intact, we can extract the hidden message image with reasonable integrity.

8 Conclusion

This paper presented improvements to the original FFT-based data hiding framework which doubles the capacity of the stego image by allowing double the amount of data to be embedded in a color carrier image. This framework exploits spatial domain color properties of natural images combined with spectral properties of the Fourier magnitude and phase of these images to allow two relatively large sized hidden images (each to a maximum of half the size of the carrier image) to be robustly embedded and extracted with minor degradation. The advantages of this technique have been expressed throughout the paper and can be summarized in that this paradigm leads to a data hiding technique that provides high fidelity, double capacity with negligible degradation, high security, and robustness to tampering.

References

1. Castleman, K.: Digital Image Processing. Prentice-Hall, Upper Saddle (1996)
2. Chan, C.K., Cheng, L.: Hiding data in images by simple LSB substitution. Pattern Recognition 37, 469–474 (2004)
3. Chen, B., Wornell, G.: Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans. Information Theory 47(4), 1423–1443 (2001)
4. Curran, K., Bailey, K.: An evaluation of image based steganography methods. International Journal of Digital Evidence 2(2), 1–40 (2003)
5. Forssen, P.-E., Granlund, G., Wikiund, J.: Channel representation of colour images (Tech. Rep. LiTH-ISYR-2418), Computer Vision Laboratory, Department of Electrical Engineering, Linkoping University, SE-581 83 Linkoping, Sweden (2002)
6. Guerchi, D., Harmain, H., Rabie, T., Mohamed, E.: Speech Secrecy: An FFT-based Approach, Special Issue on Evolving Computer Science Applications. International Journal of Mathematics and Computer Science, Lebanon 3(2), 1–19 (2008)
7. Guerchi, D., Rabie, T.: Narrowband CELP Hiding by Wideband Speech. In: The Ninth IASTED International Conference on Signal and Image Processing (SIP 2007), Honolulu, Hawaii, USA (2007)
8. Honsinger, C.: Data embedding using phase dispersion. In: IEE Seminar on Secure Images and Image Authentication (Ref. No. 2000/039), London, UK, pp. 5/1–5/7. Eastman Kodak Co., Rochester (2000)

9. Huang, T., Burnett, J., Deczky, A.: The importance of phase in image processing filters. IEEE Trans. on ASSP 23(6), 529–542 (1975)
10. Jain, A., Uludag, U., Hsu, R.: Hiding a face in a fingerprint image. In: Proc. International Conference on Pattern Recognition (ICPR), Quebec City, Canada (2002)
11. Dan, M.: Photoshop Lab Color: The Canyon Conundrum and Other Adventures in the Most Powerful Colorspace. Pearson Education, Berkeley, Calif. (2006) ISBN 0321356780
12. Marvel, L.M., Charles, G., Boncelet, J., Retter, C.T.: Spread spectrum image steganography. IEEE Trans. Image Processing 8(8), 1075–1083 (1999)
13. Nozaki, K., Niimi, M., Eason, R.O., Kawaguchi, E.: A Large Capacity Steganography Using Colour Bmp Images. In: Chin, R., Pong, T.-C. (eds.) ACCV 1998. LNCS, vol. 1351, pp. 112–119. Springer, Heidelberg (1997)
14. Oppenheim, A., Lim, J.: The importance of phase in signals. Proc. IEEE 69(5), 529–541 (1981)
15. Oppenheim, A., Lim, J., Curtis, S.: Signal synthesis and reconstruction from partial Fourier-domain information. Journal of the Optical Society of America 73(11), 1413–1420 (1983)
16. O'Ruanaidh, J., Dowling, W., Boland, F.: Phase watermarking of digital images. In: Proc. IEEE International Conference on Image Processing (ICIP), Lausanne, Switzerland, September 16–19, vol. 3, pp. 239–242 (1996)
17. Provos, N., Honeyman, P.: Hide and seek: an introduction to steganography. In: IEEE Security and Privacy Magazine, pp. 32–44. IEEE Computer Society (2003)
18. Rabie, T.: Data Secrecy: An FFT Approach. In: Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, ch. 2. IGI Global (April 2010)
19. Rabie, T., Guerchi, D.: Magnitude Spectrum Speech Hiding. In: IEEE International Conference on Signal Processing and Communication (ICSPC 2007), Dubai, UAE, November 24-27 (2007)
20. Rabie, T.: Frequency-domain data hiding based on the Matryoshka principle. Int. J. Advanced Media and Communication 1(3), 298–312 (2007)
21. Rabie, T.: A Novel Compression Technique for Super Resolution Color Photography. In: Proceedings of the IEEE International Conference on Innovations in Information Technology (IIT 2006), November 19-21, pp. 1–5. Jumeirah Beach Hotel, Dubai (2006)
22. Rabie, T.: Adaptive hybrid mean and median filtering of high-ISO long-exposure sensor noise for digital photography. SPIE Journal of Electronic Imaging 13(2), 264–277 (2004)
23. Ramkumar, M., Akansu, A., Alatan, A.: A robust data hiding scheme for images using DFT. In: Proc. IEEE International Conference on Image Processing (ICIP), pp. 1–5 (1999)
24. Schanda, J.: Colorimetry, p. 61. Wiley-Interscience (2007) ISBN 9780470049044
25. Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B.S., Chandrasekaran, S.: Robust image-adaptive data hiding using erasure and error correction. IEEE Trans. Image Processing 13(12), 1627–1639 (2004)
26. Tan, C.: Image Camou-Flaging using Phase Randomization(2002), `http://pachome2.paci.c.net.sg/chewkeong/ImgCamou.pdf`
27. Watson, A.: Perceptual-components architecture for digital video. Journal of the Optical Society of America A 7(10), 1943–1954 (1990)
28. Westfeld, A., Pfitzmann, A.: Attacks on Steganographic Systems. In: Pfitzmann, A. (ed.) IH 1999. LNCS, vol. 1768, pp. 61–76. Springer, Heidelberg (2000)
29. Wu, M., Liu, B.: Data hiding in image and video: part I – fundamental issues and solutions. IEEE Trans. Image Processing 12(6), 685–695 (2003)