International Journal of Research in Engineering, Science and Management
Volume-2, Issue-8, August-2019
www.ijresm.com | ISSN (Online): 2581-5792

Image Steganography using Time and Frequency Domain

Shabina N. Ahmed[1], Subhash Chandra[2], Vinod Todwal[3]
[1]*M.Tech. Student, Department of Computer Science, Rajasthan College of Engineering, Jaipur, India*
[2]*Assistant Professor, Department of Information Technology, Rajasthan College of Engineering, Jaipur, India*
[3]*Assistant Professor, Department of Computer Science, Rajasthan College of Engineering, Jaipur, India*

***Abstract*: Image steganography allows the user to hide the data into an image for secure transmission of any text data. Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal. Before understanding how can we hide an image inside another, we need to understand what a digital image is. We can describe a digital image as a finite set of digital values, called pixels. Pixels are the smallest individual element of an image, holding values that represent the brightness of a given color at any specific point. So we can think of an image as a matrix (or a two-dimensional array) of pixels which contains a fixed number of rows and columns.**

***Keywords*: DWT, DCT, Image Watermarking, Spatial Domain, Frequency Domain.**

1. Introduction

In computer science field, the term Least Significant Bit (LSB) refers to the smallest (right-most) bit of a binary sequence. Replacing the LSB is one of the easiest way to embed secrete message in an image pixels and will called LSB based steganography. Any LSB based steganography scheme will either change the value of the pixel or will make the pixel value remain unchanged, in case of change, the change will be very tiny which is either the pixel value increase/decrease by 1 value only. This depend on the value of the secrete message and the LSB value of the selected pixel. In a color image there are 8 bit for each primary color represent the image. Since there are 256 (i.e. 28) possible intensities of each primary color, therefore changing the LSB of a pixel results in a small changes in the intensity. These changes cannot be perceived by the human eye, thus the message is successfully hidden.

Steganography is an art of activity the data within the cover like the simplest way that, it's like straightforward cover, though its hidden information. In this paper, secret image is activity into two completely different domains like as IWT (Integer Wavelet Transform) and DWT (Discrete Wavelet Transform). The cover image and secret image coefficient values square measure embedded by 1024*1024 exploitation fusion process techniques. We tend to applied numerous combinations of DWT and IWT on each images and obtained a decent quality stego images. Each domain offers safer with secret key and sure robustness of our algorithm. This dual wavelet transform utilized in Color Image Steganography Method (DWTSM) in Blue Channel (B-Channel) provides high capability and security. This proposed algorithm is tested with image quality parameters and compared to other algorithms. The experimental Results show that dual based approach achieved high capability and high security of our system in B-Channel and conjointly improves the performance of steganography system. The proposed algorithm achieved high PSNR quantitative relation 45 to 55 and other parameter values achieved the best solution and this methodology compared to different combination of transform.

Steganography is the process of hiding of a secret message within an ordinary message and extracting it at its destination. Anyone else viewing the message will fail to know that it contains secret/encrypted data. The word comes from the Greek word “steganos” meaning “covered” and “graphei” meaning “writing”.

2. Related work

S. R. Bhadra Chaudhuri et al., [1] proposed a steganographic technique for hiding multiple images in a color image based on DWT and DCT. High frequency components are modified for hiding method so there must be constraint on the secret image size. Sabyasachi Pattnaik et. al., [2] presented a dual transform technique for robust steganography for secret and secure communication. It has excellent PSNR with high levels of security. Umashankar Dewangan et. al., [3] proposed a Development and Analysis of Stego Image Using Discrete Wavelet Transform. The Experimental results showed the high invisibility of the proposed model even with large message size. Yambem Jina Chanu et. al., [4] proposed a Steganography Technique based on SVD. Ali Al-Ataby et. al., [5] proposed a modified high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image with high levels of overall security.

Rowayda A. Sadek et. al., [6] proposed a SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges. Image examined and provided good results although they are image dependent. Nilanjan Dey et. al., [7] proposed a Novel Approach of Color Image Hiding using RGB Color planes and DWT. Acceptable imperceptibility and distortion compared to the cover image and the overall security is high. Shikha Sharda et. al., [8] proposed Performance Analysis of Image Steganography based on DWT and Arnold Transform. PSNR values of the Arnold Transform based method are better than existing methods.

Ashish Chawla et. al., [9] proposed a Modified Secure Digital Image Steganography Based on DWT Using Matrix Rotation Method. Certain strength in addition to good perceptual invisibility. K.B. Shivakumar et. al., [10] proposed the performance comparison of robust steganography based on multiple transformation techniques. Excellent PSNR with high levels of security. Anahita Shojaei-Hashemi et. al., [11] proposed an Universal Image Steganalysis against Spatial-domain Steganography based on Energy Distribution of Singular Values. Results confirm the supremacy of the proposed Steganalysis scheme over its counterparts.

The goal of steganography is hiding a message in a media while the goal of cryptography is encryption of the message [12]. According to goal of steganography, the message hiding must be done in common media such as JPEG images. Generally, it is performed in various types of media such as image, audio and video. According to goal of steganography, the message hiding must be done in common media such as JPEG images. The steganography in images without compression or with lossless compression (such as BMP format) seems more challengeable than in case of images with lossy compression (such as JPEG format) due to loss of information [13]-[15].

Steganography techniques in the image can be divided into two categories, I) Steganography in the pixel domain (space domain), and II) in the transform domain such as frequency domain. In the case of pixel domain, the steganography operation is directly performed on the pixels [15]-[16].

In transform domain steganography, the message embedding is performed in transformed image. The image is transformed from the space domain into a new domain such as frequency domain [17]-[21]. This transforming can be done with different transforms such as Fourier and Wavelet transform [19].

Some examples of steganography in the transform domain based on wavelet transform are given in [22]-[23]. The distortion is considered as the form of a sum of relative changes between the cover and embedded images that is represented in the transform domain. In [23], the author defines a universal distortion function called universal wavelet relative distortion (UNIWARD) for steganography in the frequency space. The distortion is considered as the form of a sum of relative changes between the cover and embedded images that is represented in the transform domain and, in [23], it is computed in the wavelet domain as a sum of relative changes of coefficients in a directional filter bank decomposition of the cover image.

Practically steganography methods in the transform domain hide a message in an image better those based on space domain. In addition to the fact that these methods are resistant against a variety of signal processing systems, changes made as a result of inserting secret information using these methods are not sensible to the human vision system [14]. For this reason, the proposed method aims to the steganography in JPEG images based on transform domain.

3. Proposed work

In the presented paper the cover image is taken to be of square size of 1024X1024 either an RGB image or a grayscale image. The cover image then will be processed with the DCT image transformation and then the DCT operated matrix will be passed through the DWT operation which will then generate the frequency sub-bands and hence except the Low-Low frequency band other bands will be used in order to embed the secrete data bits.

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain. When performing image compression, our best bet is to perform the KLT or the Karhunen–Loève transform as it results in the least possible mean square error between the original and the compressed image. However, KLT is dependent on the input image, which makes the compression process impractical.

DCT is the closest approximation to the KL Transform. Mostly we are interested in low frequency signals so only even component is necessary hence its computationally feasible to compute only DCT. Also, the use of cosines rather than sine functions is critical for compression as fewer cosine functions are needed to approximate a typical signal (See Douglas Bagnall's answer for further explanation).

Another advantage of using cosines is the lack of discontinuities. In DFT, since the signal is represented periodically, when truncating representation coefficients, the signal will tend to "lose its form". In DCT, however, due to the continuous periodic structure, the signal can withstand relatively more coefficient truncation but still keep the desired shape.

The wavelet transform has gained widespread acceptance in signal processing and image compression. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet called mother wavelet by dilations and shifting [8]. The DWT has been introduced as a highly efficient and flexible method for sub band decomposition of signals. The 2DDWT is nowadays established as a key operation in image

processing. It is multi-resolution analysis and it decomposes images into wavelet coefficients and scaling function. In Discrete Wavelet Transform, signal energy concentrates to specific wavelet coefficients. This characteristic is useful for compressing images. Wavelets convert the image into a series of wavelets that can be stored more efficiently than pixel blocks. Wavelets have rough edges, they are able to render pictures better by eliminating the blocking modules. In DWT, a timescale representation of the digital signal is obtained using digital filtering techniques.

The input text taken here is preferably the urls. URLs will be embedded into the frequency sub-bands after being treated by the DCT/DWT transformation for avoiding the typecasting issues. The embedding process will be done on the Uniform Spread Spectrum concept for the test analysis and to check its authenticity.

4. Results

Proposed work generated results as shown in the table below.

Table 1
Results

Frame	PSNR	cMSE	SSIM	FSIM
Image 1	50.432	1.68745	0.998452	0.998313
Image 2	55.765	1.58755	0.99806	0.998028
Image 3	47.876	2.5414	0.998989	0.998824
Image 4	54.23	1.59784	0.99105	0.998819

PSNR: Peak Signal to Noise Ratio
CMSE: Composite Mean Square Error
SSIM: Structural Similarity Index of Image
FSIM: Feature Similarity Index for Image Quality Assessment

5. Conclusion

The above generated results are carried out over 300 different images and hence generates a good visual description of the cover images. The proposed algorithm works over the RGB and the Grayscale images simultaneously is the first of its kind. The algorithm can be further enhanced for the video steganography as well.

References

[1] Tanmay Battacharya, Nilanjan Dey and Bhadra Chauduri S.R., “A Session Based Multiple Image Hiding Technique using DWT and DCT”, International Journal of Computer Applications, vol. 38(5), pp. 18-21, 2012.
[2] KB. Shiva Kumar and Khasim T, and K B Raja, “Dual Transform Technique for Robust steganography”, International conference on Computational Intelligence and Communication Systems, pp. 173-178, 2011.
[3] Umashankar Dewangan, Monisha Sharma, and Swagota Bera, “Development and Analysis of Stego Image Using Discrete Wavelet Transform”, International Journal of Science and Research (IJSR), Vol 2, pp. 142-148, 2013.
[4] Yambem Jina Chanu, Kh. Manglem Singh and Themrichon Tuithung, “Steganography Technique based on SVD”, International Journal of Research in Engineering and Technology, vol. 6, pp. 293-297, 2012.
[5] Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,” International Arab Journal of Information Technology, vol. 7 (4) , pp . 1-7, 2010.
[6] Rowayda A. Sadek, “SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges”, International Journal of Advanced Computer Science and Applications, vol. 3, ,2012.
[7] Nilanjan Dey, Anamitra Bardhan Roy, and Sayantan Dey, “A Novel Approach of Color Image Hiding using RGB Color planes and DWT”, International Journal of Computer Applications, vol.36, 2011.
[8] Shikha Sharda and Sumit Budhiraja, “Proposed Performance Analysis of Image Steganography based on DWT and Arnold Transform”, International Journal of Computer Applications, vol. 69, pp. 46-50, 2013.
[9] Ashish Chawla and Pranjal Shukla, “A Modified Secure Digital Image Steganography Based on DWT Using Matrix Rotation Method”, International Journal of Computer Science and Communication Engineering, vol. 2, pp. 20-25, 2013.
[10] K. B. Raja and H S Manjunatha Readdy, “Wavelet Based Non LSB Steganography “, International Journal of Advanced Networking and Applications, vol. 3(3), pp. 1203-1209, 2011.
[11] Anahita Shojaei-Hashemi, Hamid Soltanian-Zadeh, Shahrokh Ghaemmagham and Mahmoud Kamarei, “Universal Image Steganalysis against Spatial-domain Steganography based on Energy Distribution of Singular Values”, The 7th International Conference on Information Technology and Applications (ICITA 2011), pp. 179-183, 2011.
[12] Joseph, A., and V. Sundaram. "Cryptography and steganography–A survey." (2011).
[13] Denemark, Tomáš, Patrick Bas, and Jessica Fridrich. "Natural Steganography in JPEG Compressed Images," Electronic Imaging, vol. 7, pp. 1-10, 2018.
[14] Qazanfari, Hamed, Hamid Hassanpour, and Kazem Qazanfari. "A short-term learning framework based onrelevance feedback for content-based image retrieval." Intelligent Systems and Signal Processing (ICSPIS), 2017 3rd Iranian Conference on. IEEE 2017.
[15] Musavi, Seyed Mohammad Mehdi, Usof Torabi, Steganography techniques in images: A review, ECMM01 conference, 2018, Karaj. (In Persian)
[16] Ullah, Azmat, and Mohsin Ijaz. "Stego App: Android based Image Steganography Application using LSB Algorithm." (2018).
[17] Rashidi, Bagher, and Ahmad Faramarzi, JPEG images Steganography using the LSB method and wavelet transform, 5th international conference of electrical engineering and computer with emphasis on indigenous knowledge-COMCONF05, 2017, Tehran. (In Persian)
[18] Khorsand Movaghar, Raheleh, Hossein Khaleghi Bizhaki and Hamidreza Manuchehri Naeini, Application of genetic algorithm in image steganography, First National Symposium on Robotics and Artificial Intelligence -PNUOPEN01, 2014, Ahvaz. (In Persian)
[19] Badamchian, Mahram, Mahmoud Ahmadian Attari, Hamid Abrishami Moghaddam, Babak Afshinpour, Presentation of a novel steganography method resistant to lossy JPEG compression, specially for medical images, 15th Iranian Conference on Electric Engineering (ICEE15), 2007. (In Persian)
[20] Ayalvari, Somayeh and Mobina Yakhkeshi, Steganography in JPEG images. 3rd national conference on computer science 2015, Sanandaj. (In Persian)
[21] Waghmare, Wrushali, S. I. Nipanikar, and P. V. Mulmule. "Holo- Entropy and Advanced Encryption Standard for Wavelet-Based Image Steganography." International Journal of Research in Engineering, Science and Management, vol. 1, no. 10, October 2018.
[22] Holub V, Fridrich J, “Designing steganographic distortion using directional filters,” in Fourth IEEE International Workshop on Information Forensics and Security. Tenerife, 2–5 December 2012.
[23] Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security, vol. 1, 2014.