Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Robust Image Steganography Embed and Extraction by Using Combinational Transform Technique

R. Siva Sankar
M. Tech (DECS)
Electronics and Communication Engineering
Gudlavalleru Engineering College
Andhra Pradesh, India

T. S. R. Krishna Prasad
Associate professor
Electronics and Communication Engineering
Gudlavalleru Engineering College
Andhra Pradesh, India

Abstract*— The super development in communication technology and utilization of unrestricted domain channels (i.e. Internet) has significantly facilitated transfer of information. Though, such open communication channels have higher susceptibility to security threats inflicting unauthorized expertise access. Steganography is the art and science of communicating in a method which hides the existence of the data. Steganalysis is one more fundamental matter in know-how hiding which is the artwork of detecting the presence of steganography content. On this paper a method for image steganography as well as steganalysis making use of the basics of Discrete cosine transforms (DCT) and discrete wavelet transforms (DWT) in transform domain. Here the proposed process consists of each DCT and DWT for developing the stego image and overcome the drawbacks of DCT based steganography and DWT based steganography.

***Keywords*— Steganography, steganalysis, stego image, DCT and DWT.**

I. INTRODUCTION

Steganography is the art and science of hiding information by using embedding messages inside different, apparently innocent messages. Steganography approach “covered writing” in Greek. As the intention of steganography is to hide the presence of a message and to create a covert channel, it can be obvious as the complement of cryptography, whose purpose is to cover the content material of a message. One other form of know-how hiding is digital watermarking, which is the system that embeds data called a watermark, tag or label into a multimedia object such that watermark can also be detected or extracted later to make an declaration in regards to the object. The item may be an snapshot, audio, video or text simplest. A famous illustration of steganography is Simmons’ Prisoners’ predicament .An assumption may also be made on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is often called then the secret key steganography where as pure steganography approach that there is none prior know-how shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is referred to as public key steganography. Close to all digital file formats can be used for steganography, but the picture and audio files are more compatible in view that of their high measure of redundancy. Fig. 1 below indicates the unique classes of steganography procedures. There are one of a kind approaches to implement steganography particularly least significant bit (LSB), discrete cosine transform (DCT) & discrete wavelet transform (DWT) system. There are two forms of domains in which steganography is implemented i.e. Spatial domain & frequency domain.

II. SYSTEM MODEL

A classical steganographic process’s protection relies on the encoding approach’s secrecy. Even though the sort of method would work for a time, as soon as it is recognized, it is simple adequate to reveal the entire bought media(e.g., pictures) passing with the aid of to examine for hidden messages finally, this kind of steganographic method fails. Present day steganographic method makes an attempt to be detectable provided that secret information is famous particularly a secret key. In this case, cryptography will have to be worried, which holds that a cryptographic system’s safety should rely exclusively on the important thing fabric. For steganography to remain undetected, the unmodified cover medium ought to be kept secret, on the grounds that if it is exposed, a comparison between the cover and stego media right away exhibits the changes.
Three common forms of stego methods are to be had:

- Pure stego systems - no key is used.
- Secret-key stego systems - secret key is used.
- Public-key stego systems - public key is used.

The technique that is followed in this paper will use secret key to encrypt the hidden message that will be encapsulated inside a cover media.

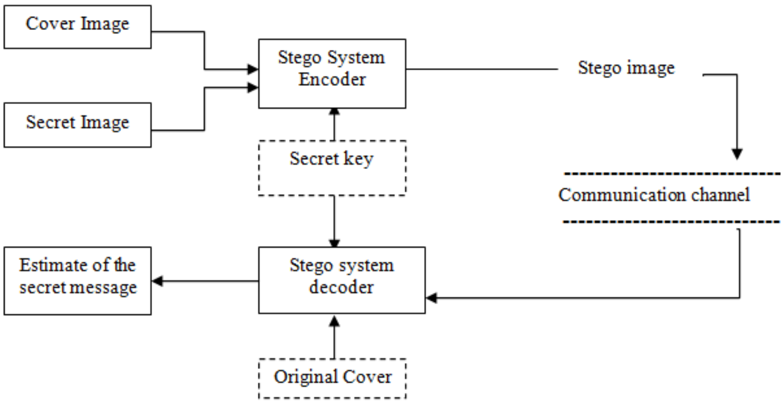


Fig.1: Block diagram of steganography

A. Spatial Domain Based Steganography

In this system the least significant bits of the cover object is replaced without modifying the complete cover object. It's a easiest process for data hiding but it is rather susceptible in resisting even simple attacks comparable to compression, transforms, and so on.

B. Transform Domain Based Steganography

The quite a lot of grow to be domains tactics are Discrete Cosine Transforms (DCT), Discrete Wavelet Transforms (DWT) and Fast Fourier transform (FFT) are used to are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc.

III. EXISTING METHODS

Discrete cosine transform based image steganography

DCT is a mechanism used in the JPEG compression algorithm to transform successive 8x8-pixel blocks of the photograph from spatial domain to 64 DCT coefficients each and every in frequency domain. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The modification of a single DCT coefficient influences all sixty four image pixels. Considering the fact that this change happens in the frequency domain and now not the spatial domain, there are not any visible visual differences. The expertise DCT has over other transforms is the ability to reduce the block-like appearance ensuing when the boundaries between the 8x8 sub-imagebecome visible (known as blocking artifact). The disadvantage is that this method only works on JPEG files seeing that it assumes a distinct statistical distribution of the quilt knowledge that's generally discovered in JPEG files. So the secret message is embedded with the aid of editing the coefficients of the mid frequency sub-band, in order that the visibility of the image is probably not affected. The general equation for a 1D (N knowledge gadgets) DCT is defined by way of the next equation:

$$C(u) = a(u) \sum_{i=0}^{N-1} x_i \cos(\frac{(2i+1)4\pi}{2N})$$

Where u = 0, 1, 2…….N-1

The general equation for 2D DCT is defined by the following equations

$$C(u,v) = a(v) \sum_{i=0}^{N-1} \left[a(u) \sum_{i=0}^{N-1} x_i \cos(\frac{(2i+1)u\pi}{2N})\right] cos\,(\frac{(2i+1)v\pi}{2N})$$

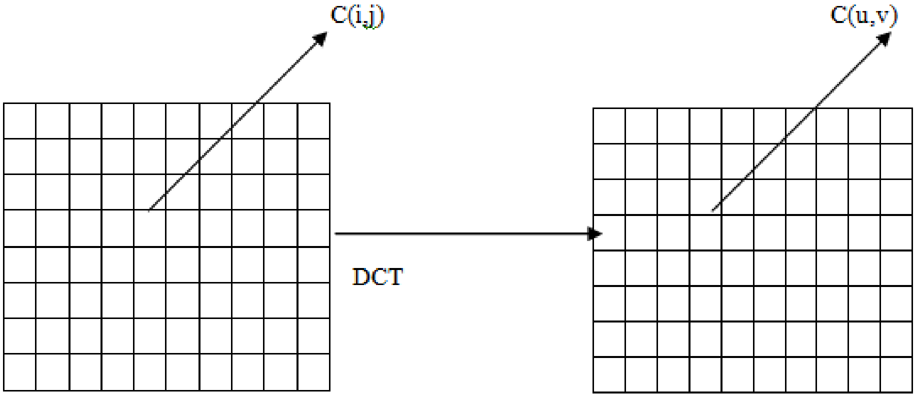


Fig.2: Discrete Cosine Transform of an Image

where u, v = zero, 1, 2….N-1 right here, the enter image is of measurement N X M. C(i, j) is the depth of the pixel in row i and column j; c(u, v) is the DCT coefficient in row u and column v of the DCT matrix. DCT is used in steganography as image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, DCT is utilized to each block. Every block is compressed by means of quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

Discrete Wavelet Transforms based Image steganography:

Discrete Wavelet change into (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is headquartered on small waves, called wavelets, of varying frequency and constrained length. Wavelet change into provides both frequency and spatial domain of an image. Not like conventional Fourier transform, temporal knowledge is retained in this transformation approach. Wavelets are created by using translations and dilations of a fixed function called mother wavelet. This part analyses suitability of DWT for image watermarking and gives advantages of utilizing DWT as against other transforms. For 2-D image, applying DWT corresponds to processing the image by way of 2-D filters in every dimension. The filters divide the image into four non-overlapping sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the DWT coefficients at the same time the sub-bands LH1, HL1 and HH1 represent the first order of DWT coefficients..

To receive the following coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some ultimate scale Nis reached. When N is reached we can have 3N+1 subbands together with the multi-decision sub-bands LLN andLH, HL and HH where x stages from 1 until N. As a result of its first-class spatio frequency localization homes, the DWT is very suitable to determine the areas in the host image where a watermark can be embedded effortlessly. Most of the time many of the image is focused on the diminish frequency sub-bands LL and as a result embedding watermarks in these sub-bands may just degrade the image greatly. Embedding within the low frequency sub-bands, nonetheless, mightdevelop robustness significantly. On the other hand, the excessive frequency sub-bands HH incorporate the edges and textures of the image and the human eye isn't customarily sensitive to alterations in such sub-bands. This allows the watermark to be embedded without being perceived by means of the human eye.

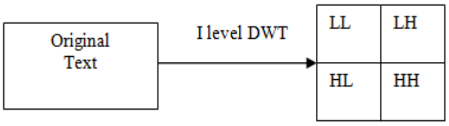


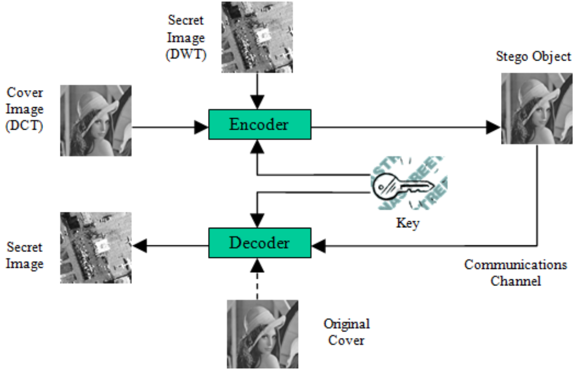
Fig.3: Wavelet Decomposition

Drawbacks of existing system:

Decrypted secret image and stego image quality for DCT algorithm is better compared to DWT algorithms, while in the case of capacity and processing time DWT are good compared to DCT. So that's why in this paper the proposed system consists of both DCT and DWT to get the better results.

IV. PROPOSED METHOD

Proposed method consists of both the transform techniques like DCT and DWT techniques and it uses the properties of both the transform techniques. Here in this paper DWT is applied on the hidden image and DCT is applied on the cover object to embedding and extracting the data.



V. RESULT AND DISCUSSION

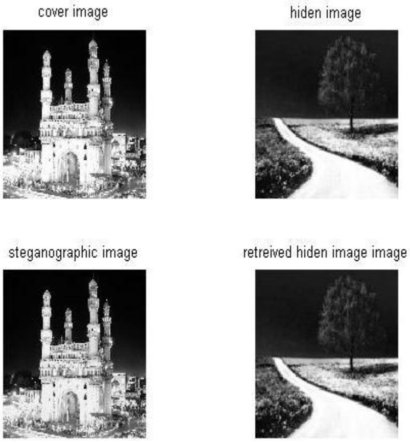


Fig.4: DWT based steganography

Fig 4 represents the simulation results for DWT based image steganography .Here firstly take an image and convert into grey image and perform three level wavelet decomposition.For cover frame we have to take another image and convert it into grey scale image. These both images are given to the stego encoder and DWT applied. From stego encoder we get the stego output. Then stego output given to the decoder which can retrieve the original information.

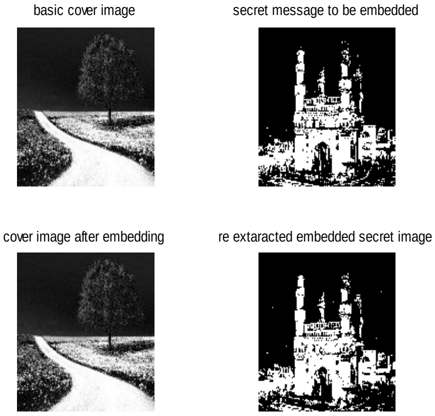

basic cover image
secret message to be embedded
cover image after embedding
re extaracted embedded secret image

Fig.5: DCT based steganography

Fig 5 represents the simulation results for DCT based image steganography .Here firstly take an image and convert into binary image. For cover frame we have to take another image and convert it into grey scale image. These both images are given to the stego encoder and perform DCT operation. From stego encoder we get the stego output. Then stego output given to the decoder which can retrieve the original information. Finally we have to calculate PSNR and MSE.

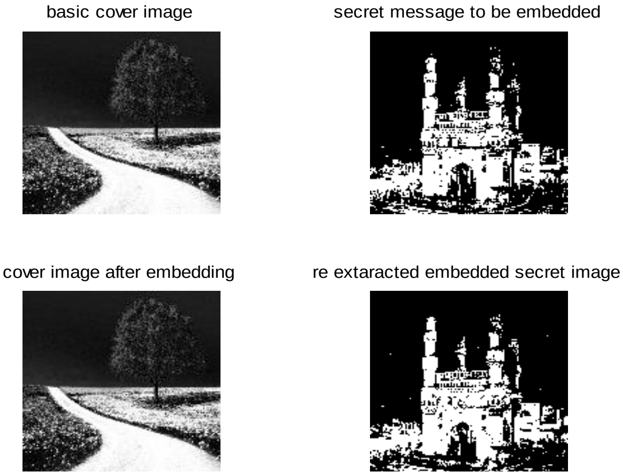

basic cover image
secret message to be embedded
cover image after embedding
re extaracted embedded secret image

Fig.6: Combined Transform Based Steganography

Fig 6 represents the simulation results for Combinational transform means both transforms are used image steganography .Here firstly take an image and convert into binary image and apply DWT on that image. For cover frame we have to take another image and convert it into grey scale image. These both images are given to the stego encoder and perform DCT from stego encoder we get the stego output. Then stego output given to the decoder which can retrieve the original information. Finally we have to calculate PSNR and MSE.

Comparisons result shown as Combined transform based steganography produces better results than others.

Table 1: Comparision results of PSNR and MSE

Technique	PSNR	MSE
DCT	50.7840	0.5428
DWT	31.6152	0.9454
COMBINED	50.8135	0.5428

VI. CONCLUSION

The purpose of knowledge hiding is to preclude peepers from discovering the key messages embedded in the cover image.Our experimental outcome show the proposed procedure supplies suited image high-quality and a big message ability. Overall, the proposed system suits the requirement of steganography with a higher message capacity and good image exceptional. In future these combinational techniques are also performed on the various cover medias like audio and video.

REFERENCE

[1] Jessica Fridrich, MiroslavGoljan, and Rui Du, ―Detecting LSB Steganography in Color and GrayScale Images‖, Magazine of IEEE Multimedia, Special Issue on Multimedia and Security, pp.22- 28, October-December 2001.

[2] P.Chen, and H.Lin,"A DWT approach for image steganography", International Journal of applied Science and Engineering", volume.4, 3:pp 275:290,2006.

[3] B.Lai and L.Chang, "Adaptive Data hiding for images based on Haar discrete wavelet transform", Lecture notes in computer science, volume 4319/2006.

[4] Souvik Bhattacharyya, Indradip Banerjee and GautamSanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier",Journal of Global Research in Computer Science IGRCS 2010.

[5] Kumar, V., Kumar, D,Performance evaluation of DWT based image steganography , Advance Computing Conference (IACC), 2010 IEEE 2nd International

[6] Deepak Singla and RupaliSyal,"Data Security Using LSB& DCT Steganography In Images",/International Journal Of Computational Engineering Research,ppno:359-364,2012.