Object Oriented Steganography based on Biometric and Spread Spectrum

Meena, Danvir Mandal

Abstract— Today major part of communication goes through internet and this communication needs to be secret and protected against malicious attacks. Steganography is the art and science of invisible communication. It not only keeps the contents of a message secret, but also the existence of message secret. There exist many different steganography techniques having different strong and weak points. In this paper steganography is based on biometric feature i.e. secret data is embedded in skin tone regions of an image. Secret data is hidden by tracing skin pixels in one of the high frequency sub band of DWT of the cover image . To enhance the high security feature secret images are dispersed within each band using a pseudo random sequence and a session key. This combined approach of using skin pixels and spread spectrum for embedding the secret images provides a high degree of security. The stego-image generated is of acceptable level of imperceptibility and distortion compared to the cover image.

Index Terms— Encryption, Dwt, Imperceptibility, Security, Skin tone detection, Stego image, Spread spectrum.

1 Introduction

THE information hiding techniques have become an important research area in recent years, ever since researchers realized that developing techniques to solve unauthorized copying, tampering, and distribution of multimedia data via Internet is urgent.

Cryptography was created as a technique for securing the secrecy of communication and many different methods were developed to encrypt and decrypt data in order to keep the message secret. But sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. This concept is implemented through the technique called **steganography**.

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography employs an innocent-looking media called a host image to imperceptibly carry secret data to an intended recipient. The image embedded with the secret data looks like a normal image. Unintended recipients of this image are unaware of the existence of the hidden data.

In steganography secret message or the data that the sender wishes to transmit confidentially can be text, images, audio, video, or any other data type that can be represented by a stream of bits. The cover or host image is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover, and in this paper cover and secret messages are restricted to be digital images. The cover-image with the secret data embedded is called the “Stego-Image”. The Stego-Image should resemble the cover image under casual inspection and analysis.

In addition to providing invisibility of hidden message, for higher security requirements the message data can be encrypted before embedding them in the cover-image to provide further protection. In spread spectrum communications, the signal energy inserted into any one frequency is too undersized to create a visible artifact and the secret image is scattered over a wide range of frequencies, that it becomes robust against many common signal distortions. Because of its good correlation properties, noise like characteristics, easier to generate and resistance to interference, Pseudo noise sequences are used for Steganography.

The different requirements that need to be considered while designing a steganographic system are:

Invisibility – To provide invisibility is the first and foremost requirement of a steganographic algorithm, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

Robustness against statistical attacks - Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. To pass without being detected, a steganographic algorithm must not leave a mark in the image as be statistically significant.

- *Meena is currently pursuing masters degree program in Electronics and communication engineering in Punjab Technical University, India. E-mail : mnureja@gmail.com*
- *Danvir Mandal is currently pursuing Ph.D. degree program in Punjab Technical University, India. E-mail: danvir_mandal@rediffmail.com*

Robustness against image manipulation – Image manipulation, such as cropping, rotation, scaling etc. can be performed on the image before it reaches its destination. These manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.
Independent of file format - The most powerful steganographic algorithms should possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

2 RELATED WORK

Generally, steganographic methods proposed in the past few years can be categorized into two types. The methods of the first type employ the spatial domain of a host image to hide secret data. In other words, secret data are directly embedded into the pixels of the host image. Steganographic methods of the second type employ the transformed domain of a host image to hide secret data. Transformation functions like the discrete cosine transform (DCT) or discrete wavelet transform (DWT) are first exploited to transform the pixel values in the spatial domain to coefficients in the frequency domain. Then the secret data are embedded in the coefficients.

LSB(Least significant Bit) Steganography -Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [1]. This method is easy and straightforward but this has low ability to bear some signal processing or noises and secret data can be easily stolen by extracting whole LSB plane.

Gray Level Modification (GLM) Steganography –it maps data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image[2].

PVD Method for Gray-Level Image – The pixel-value differencing (PVD) method [3] segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification.

In this paper a watermarking algorithm for digital images is used: the method, which operates in the frequency domain and embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. Aos [4] implemented a means of hiding the secret information in the Executable (.EXE) file, such that it is unrevealed to any anti-virus software, since anti-virus software secretly read the furtive data embedded inside the cover file. Daniela Stanescu [5] proposed a technique in which steganographic algorithm is implemented on embedded devices and also suggests on using microcontrollers or microprocessors for executing steganographic algorithms instead of using Field Programmable Gate Arrays. Jin-Suk Kang [6] described steganography using block-based adaptive threshold. Initially the bit-plane blocks of the cover image and the payload are compared and if the blocks are similar, then those blocks of the payload are embedded in the cover image. Mci-Ching Chen [7] introduced an extension to the existing steganography to improve the capacity. At the receiver, template matching techniques are used to find the location of the object file. Neha Agarwal and Marios Savvids [8] proposed a steganographic method to hide biometric data in DCT coefficients of the cover image in a more robust way. [9]Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Different steps of data hiding are applied by cropping an image interactively. Cropping results into an enhanced security than hiding data without cropping i.e. in whole image, so cropped region works as a key at decoding side. For embedding, secret images are dispersed within each band of DWT of image using a pseudo random sequence and a Session key. Secret images are extracted using the session key and the size of the images [10,11].

3 PROPOSED WORK

Proposed method introduces a new method of embedding secret data based on biometric feature such as within skin tone as it is not that much sensitive to HVS (Human Visual System) [1].This takes advantage of not embedding data anywhere in the image, data will be embedded only in selected regions . The important challenge in the skin detection is to represent the color in a way that is invariant or at least insensitive to changes in illumination. Another challenge comes from the fact that many objects in the real world might have skin-tone colors. Color space used for skin detection in this work is YCbCr .One advantage of using this color spaces is that most video media are already encoded using these color spaces. Transforming from RGB into YCbCr color space is a straight forward linear transformation. All these color spaces separate the illumination channel (Y) from two orthogonal chrominance channels (CbCr). Therefore, unlike RGB, the location of the skin color in the chrominance channels will not be affected by changing the intensity of the illumination. In the chrominance channels the skin color is typically located as a compact cluster with an elliptical shape. This facilitates building skin detectors that are invariant to illumination intensity.

Secret images are encoded using a pseudo random sequence and a session key. This encoded secret data is embedded in high frequency sub-band of Cover image decomposed using DWT. The Discrete Wavelet Transform is very suitable for identifying the areas in the cover image where a secret image can be embedded effectively due to its excellent space-frequency localization properties. Spread spectrum provides the ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer. The message is recovered with low error probability. Furthermore, the original image is not needed to extract the hidden information. The proposed recipient needs to possess only a key in order to reveal the secret message. The very existence of the hidden information is virtually undetectable by human or computer analysis. The message is recoverable even if the transmitted image undergoes attack by unknown recipients. It also provides resiliency to transmission noise, like that found in a wireless environment and low levels of compression.

4 ALGORITHM

4.1 Secret Image Hiding:

Step 1: The Cover image is loaded, skin tone detection is performed on the image. This will produce mask image that contains skin and non skin pixels.
Step 2: Cover image is decomposed into four sub bands using DWT.
Step 3: A pseudo random sequence is generated by the session based key.
Step 4: The secret image is converted into 1D Vectors and is encrypted using the pseudo random sequence.
Step 5: Encoded secret data is embedded only in skin pixels of high frequency sub-band of cover image decomposed using DWT
Step 6: The stego image is generated using IDWT.

4.2 Attacks on Stego-Image

The stego-image is transmitted. After transmission this image may be corrupted due to noise. Besides noise this image may undergo attack like rotation, scaling, cropping etc. Here two attacks (i) addition of salt and pepper noise (ii) rotation of stego image have been taken. Attacked stego-image is received at reception.

4.3 Secret Image Extraction

Step1: Session key and Sizes of the secret images are sent to the intended receiver via a secret communication channel.
Step 2: The same pseudo random sequence is generated by using the session key.
Step 3: Secret images are recovered from the received attacked stego image using Correlation function and knowing the size of the secret image.
Step 4: Extracted Secret Images are filtered to remove the unwanted signal.

5 EXPERIMENTAL RESULTS

The cover image is shown in fig 1. As the approach is object oriented, the skin pixels are detected from the cover image (Fig 2). The skin detection is performed on the basis of pre-decided threshold value.

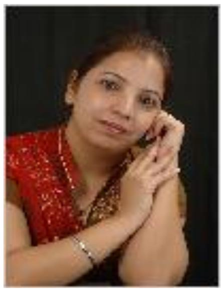

Fig.1: Cover Image

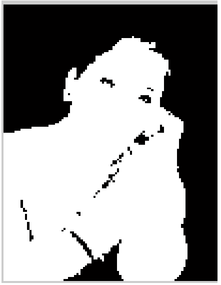

Fig.2: Detection of Skin Pixels

The secret image (Fig 3) is encrypted using spread spectrum technique. The spread spectrum generated is based on a session key. The same session key is with the receiver. The encrypted secret image is embedded into the cover image decomposed using DWT and it generates stego-image (Fig 4). The stego-image resembles the cover image. The changes are not noticeable.

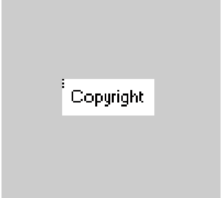

Fig.3: Secret Image

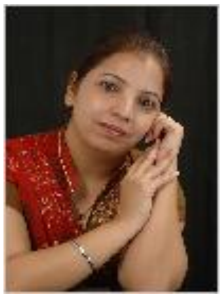

Fig.4: Stego- Image

Noise gets added in the stego-image after transmission. The noisy stego-image (Fig 5) is received. The other attack i.e. rotation of stego-image is shown in Fig 6.

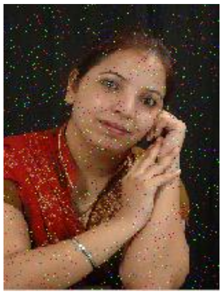

Fig.5: Noisy Image

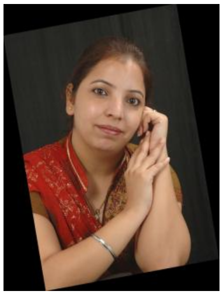

Fig.6: Rotated Image

The secret-image is extracted from the stego-image using the same spread spectrum technique. The extracted stego-image (Fig 7) has some noise. The filtered secret image is shown in Fig 8.

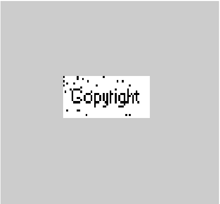

Fig.7: Recovered Image

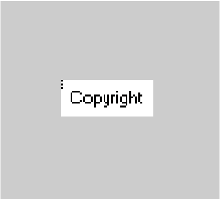

Fig.8: Recovered Filter Image

5.1 Performance Measures:

Peak Signal to Noise Ratio (PSNR)

It measures the quality of a stego image. This is basically a performance metric and use to determine perceptual transparency of the stego image with respect to cover image:

$$MSE = \left[\frac{1}{N*N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}(X_{ij} - \overline{X}_{ij})^2$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE}db$$

Similarity Measure: After secret image embedding process, the similarity of original cover image and stego images is given by similarity function

$$r = \frac{\sum (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum (x_i - \overline{x})^2}\sqrt{\sum ((y_i - \overline{y})^2}}$$

where:
Xi: the value of the pixels in the cover image
Yi: the value of the pixels in the stego image
x : the mean value of xi.
y : the mean value of yi.

Type of Image	MSE	PSNR	Similarity
Stego-Image	0.0032	24.92	0.9982
Noisy Stego-image	0.0036	24.43	0.9979
Rotated Stego-image	0.0039	24.09	0.9934

The calculated PSNR adopts dB value for quality judgment. Results show an accepted level of quality of stego-image.

6 Conclusion

The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. In this paper approach for steganography is object oriented i.e. it is based on one of the feature of image. Here the feature used is skin region of image i.e. biometric approach. Instead of using whole image, embedding data only within the skin regions provide an excellent secure location for data hiding. Encryption of message using spread spectrum before embedding enhances the security level. The quality of recovered message is not degraded even if the stego-image is attacked after transmission. The proposed approach provides invisibility and fine image quality of the stego image, higher security and satisfactory PSNR.

References

[1] Fridrich, J., Goljan, M. and Du, R.., (2001). "Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM,Special Session on Multimedia Security and Watermarking, Ottawa,Canada, October 5, 2001, pp. 27- 30.

[2] A Novel steganographic Method for Gray-Level Images AhmadT. Al-Taani and Abdullah M. AL-Issa, International Journal of Computer, Information, and Systems Science, and Engineering 3:1 2009

[3] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, 24(9-10),pp.1613–1626, 2003.

[4] Aos A Z, A W Nazi, Shihab A Hameed, Fazida Othman, B B Zaidan. (2009): "Approved Undetectable-Antivirus Steganography," International Spring Conference on Computer and Information Technology, pp. 437-441.

[5] Daniela Stanescu, Valentin Stangaciu, Loana Ghergulescu and Mircea Stratulat. (2009): "Steganography on Embedded Devices," International Symposium on Applied Computational Intelligence and Informatics, pp. 313-318.

[6] Jin-Suk Kang, Yonghee You and Mee Young Sung (2007): "Steganography using Block-Based Adaptive Threshold," International symposium on Computer and Information Sciences, pp. 1-7.

[7] Mci-Ching Chen, Sos S Agaian and C L Philip Chen. (2008): "Generalised Collage Steganography on Images," International Conference on Systems, Man and Cybernetics, pp.1043-1047.

[8] Neha Agarwal and Marios . (2009): "Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with the Single Image using Steganography, Encryption and Matching," International Conference on Computer vision and pattern recognition, pp.85-92.

[9] Anjali A. Shejul Prof. U.L Kulkarni (2010):" A DWT based Approach for Steganography Using Biometrics" International Conference on Data Storage and Data Engineering ,pp.39-43

[10] Tanmay Bhattacharya *, Nilanjan Dey ** and S. R. Bhadra Chaudhuri (2011) "A Novel Session Based Dual Steganographic Technique Using DWT and Spread" International Journal of Modern Engineering Research pp-157-161

[11] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.

[12] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science andEngineering, 2006. 4, 3: 275-290

[13] Ahmed E., Crystal M. and Dunxu H.: "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009

[14] Blossom Kaur, amandeep kaur,Jasdeep Singh (2011) : " Steganography Approach for Hiding Image in DCT Domain" International Journal of advances in engineering and technology,pp.72-78