An Efficient Steganographic Scheme Using Skin Tone Detection and Discrete Wavelet Transformation

Swati Kumravat
M.Tech (I.T.) 4th sem
Lakshmi Narain College of Technology
Bhopal, India
Swatikumrawat11@gmail.com

Abstract— Steganography is a technique used for secret communication, in which secret information is embedded into a cover medium. The Secret information may be some text or image or even audio clip and the cover medium may be some image, audio or some word file. In this paper, we propose a steganographic scheme for text hiding and logo hiding. We use Natural Images as cover medium for hiding secret information. Steganography scheme used in this paper is based on skin tone detection. In this scheme secret information is embedded within skin portion of image. Skin tone detection is achieved using HSV (Hue, Saturation and Value) color space. Additionally DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) methods are used for embedding of secret information.

Keywords- DWT, LSB, Skin tone detection

1. INTRODUCTION

Since the growth of the Internet one of the most important factors of information technology and communication has been the information's security. Cryptography was created as a method for securing the confidentiality of communication and many other methods have been developed to encrypt and decrypt data for keeping the message secret. Unfortunately sometimes it is not enough to keep the contents of a message confidential, it may also be necessary to keep the existence of the message confidential. The method used to apply this is called steganography. Steganography is the science of invisible communication. Steganography is accomplished through hiding of information within other information, thus hiding the presence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden completely in images [1].

Two other techniques that are closely related to steganography are watermarking and fingerprinting. Watermarking and fingerprinting are basically used for intellectual property protection. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is concealed in the host data in such a way that it cannot be removed without corrupting the host medium. Though this technique keeps the data available, but it is permanently marked. The hidden information in a watermarked object is a signature referring to the source or true ownership of the information to ensure copyright protection. In the process fingerprinting, different and explicit marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups. Consider Fig. 1, which illustrates the types of steganography [7].

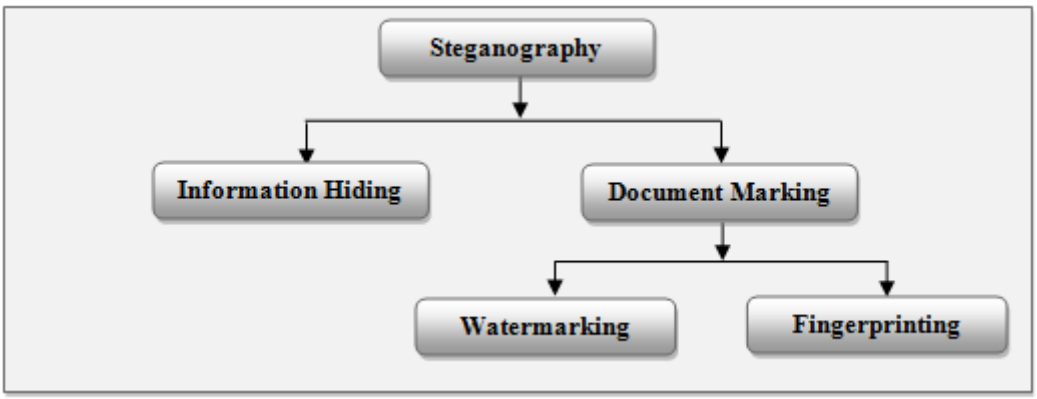

Fig. 1- Types of Steganography

In steganography secret message is the data that the sender wishes to remain confidential and can be text, images, video, audio, or any other data that can be represented by a stream of bits. The cover is the channel in which the message is embedded and serves to hide the existence of the message. The message embedding method is strongly depend on the structure of the cover, and covers are restricted to being digital images in our proposed method. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should look like the cover image under casual assessment and analysis. In addition, for higher security requirements, we can encode the message data before embedding them in the cover-image to provide further security. For this the encoder usually has a stego-key which guarantees that only recipients who know the agreeing decoding key will be able to extract the message from a stego-image. In proposed method cover image is cropped interactively and that cropped area works as a key at decoding side yielding improved security. There are two things that need to be considered while designing the steganographic system [3]:

(a.) Invisibility: Human eyes can not distinguish the difference between original and stego image.

(b.) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly [3].

2. LITERATURE REVIEW

Here we describe the classification of image steganography methods with their respective advantages and disadvantages. Performance Measure for image distortion is also described in this section.

2.1 Classification of Image Steganography Methods

A. Spatial Domain Based Steganographic Methods

The simplest and mostly used spatial domain steganographic method is least significant bit (LSB) steganography in uncompressed file formats, such as bitmaps (BMP) and TIFFs. For a 24 bit full color image represented in the RGB color model, each color layer may be decomposed into 8 bits. The secret message may be hidden by altering the least significant bit in a certain layer. More bit planes can be obtained by other bit plane decomposition algorithms in order to embed more information. Examples of available steganographic tools on spatial domains are wbStego, S-Tools and Hide v2.0. Such method can reach a high capacity; however, it does not provide robustness against simple modifications on the steganographic image and is easy to detect [8].

B. Palette Based Steganographic Methods

A color image can be illustrated in a different color model, for example, YCbCr, where the components indicate luminance, chrominance blue and chrominance red respectively. Images represented in such model are transformed into palette based color representation which is widely used through the Internet. Palette based steganography hides the steganographic message within the bits of the palette and/or the indices. Care must be taken when using this image file format ensuring that the number of colors is not exceeded. Examples of this form of embedding are BPCS and EzStego [8].

C. Transform Domain Based Steganographic Methods

Transform domain steganographic methods hide data in the coefficients of the represented domain. After mapping the signals to another domain such as discrete Fourier transform, cosine transform, Hartley transform, and wavelet transforms, the obtained coefficients are altered or replaced. The methods are more robust than spatial domain embedding techniques while maintaining good image quality. They are also independent to various image file formats either lossy or lossless image formats; however, have lower capacity. Examples include F5, Outguess and StegHide [8].

D. File Structure Based Steganographic Methods

Different image file formats have different header file structures. The secret information can be hidden not only in the data values, e.g., pixels, palette, DCT coefficients, but also in the header structure or at the end of a file. For instance, Invisible Secrets and Steganozorus hide data with the comment fields in the header of JPEG images. Camouflage, JpegX, PGE10 and PGE20 add data at the end of a JPEG image [8].

2.2 Performance Measure

As a performance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as:

$$\text{PSNR} = 10 \log_{10} \left(\frac{C^2 max}{MSE} \right)$$

Where MSE denotes the Mean Square Error which is given as:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(S_{xy} - C_{xy} \right)^2$$

And C_{max} holds the maximum value in the image, for example:

$$C_{max} \leq \begin{cases} 1 & \text{in double precision intensity image} \\ 255 & \text{in 8 bit unsigned integer intensity image} \end{cases}$$

x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego image and C_{xy} is the cover image [6].

3. PROPOSED METHOD

Proposed method presents a method of data hiding in which secret data is embedded within skin region of image. This method uses skin tone detection; discrete wavelet transform and LSB matching algorithm. These are described below:

3.1 Skin Color Tone Detection

A skin detector typically converts a given pixel into a suitable color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier describes a decision limit of the skin color class in the color space. Though this is a straightforward process has proven quite challenging. Consequently, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination and another challenge is that many objects in the real world might have skin-tone colors. This causes any skin detector to have much false detection in the background if the environment is not controlled. The simplest way to find skin pixel is to explicitly define a limit. RGB matrix of the given color image can be transformed into different color spaces to produce distinguishable regions of skin or near skin tone. There exists several color spaces. Mainly two kinds of color spaces are exploited in the literature of biometrics which are HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces. It is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within those two color spaces. Color space used for skin detection in this work is HSV. Any color image of RGB color space can be easily converted into HSV color space. Sobottaka and Pitas defined a face localization based on HSV. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints:

Smin= 0.23, Smax =0.68, Hmin =0^0 and Hmax=50^0 [3].

3.2 Discrete Wavelet Transform (DWT)

The transform of a signal is just another form of representing this signal. It does not change the information content present in it. In most Digital Signal Processing (DSP) applications, the frequency content of the signal is very important. The Fourier Transform (FT) is probably the most popular transform used to obtain the frequency spectrum of a signal. But the Fourier Transform is only appropriate for stationary signals, i.e., signals whose frequency content does not change with time. The Fourier Transform, even though it tells how much of each frequency exists in the signal, it does not tell at which time these frequency components occur. Signals such as image or speech have different characteristics at different space or time, i.e., they are non-stationary. Most of the biological signals too, such as, Electrocardiogram, Electromyography, etc., are non-stationary. To evaluate these signals, both frequency and time information are needed concurrently, i.e., a time-frequency model of the signal is needed. The Wavelet Transform provides a time-frequency representation of the signal. It uses multi-resolution technique by which different frequencies are analyzed with different resolutions. Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT) are full frame transform, and hence any alteration in the transform coefficients affects the whole image excluding if DCT is implemented using a block based method. However DWT has spatial frequency locality that means if signal is embedded it will affect the image locally. Hence a wavelet transform offers both frequency and spatial description for an image. The forward 2-D discrete wavelet transform can be implemented using a set of up-samplers, down-samplers, and recursive two-

channel digital filter banks [5].When applying discrete wavelet transform on an image, four different sub-images are obtained as follows:

(1) LL: A coarser approximation to the original image containing the overall information about the whole image. It is obtained by applying the low-pass filter on both x and y coordinates.

(2) HL and LH: They are achieved by applying the high-pass filter on one coordinate and the low-pass filter on the other coordinate.

(3) HH: Shows the high frequency component of the image in the diagonal direction. It is obtained by applying the high-pass filter on both x and y coordinates.

Since human eyes are much sensitive to the low frequency region (LL sub-image), LL is the most important component in the reconstruction process [5].

3.3 LSB Matching

The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. The basic idea of LSB matching is to embed the secret message bit at the rightmost bits of pixel value so that the embedding method does not affect the original pixel value significantly. The formula for the embedding is as follows:

$Xi' = Xi - Xi \bmod 2^k + Bi$

Where:

Xi' is i^{th} pixel value of stego-image.

Xi is i^{th} pixel value of cover-image.

k is the number of LSBs to be substituted. And

Bi is decimal value of i^{th} block in secret message.

The extraction of message from the high frequency components is given as:

$Bi = Xi \bmod 2^k$

There are two types of LSB methods, fixed-sized and variable-sized. The fixed-sized inserts the same number of message bits in each pixel of the cover-image. On inserting fixed four arbitrary bits in the four LSBs of each pixel, some false outlines can occur. The unwanted objects may arise-doubt and defeat the purpose of steganography. To solve this problem, either fewer bits must be used for message embedding or a variable sized approach should be applied [4].

3.3 Embedding Procedure

In the process of embedding following steps are involved (which is also depicted in Fig.2):

1. First of all cover image of size (M×N) is loaded.
2. Then Skin tone detection is performed to find the skin region of cover image.
3. In the skin portion detected in previous step, cropping is performed. This is performed to ensure security by hiding data within limited skin pixel positions.
4. In this step histogram equalization is performed for enhancing the quality of cropped image.
5. In key generation step pseudo key is generated for encryption.
6. Discrete Wavelet Transformation is performed in this step.
7. Secret data is embedded using LSB matching.
8. To reduces the distortion caused by the LSB substitution method we use optimum pixel adjustment(OPA).In OPA the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden [9].
9. Inverse DWT is performed.
10. Finally reconstruction of cover image with secret data is done. This reconstructed image is called Stego-image.

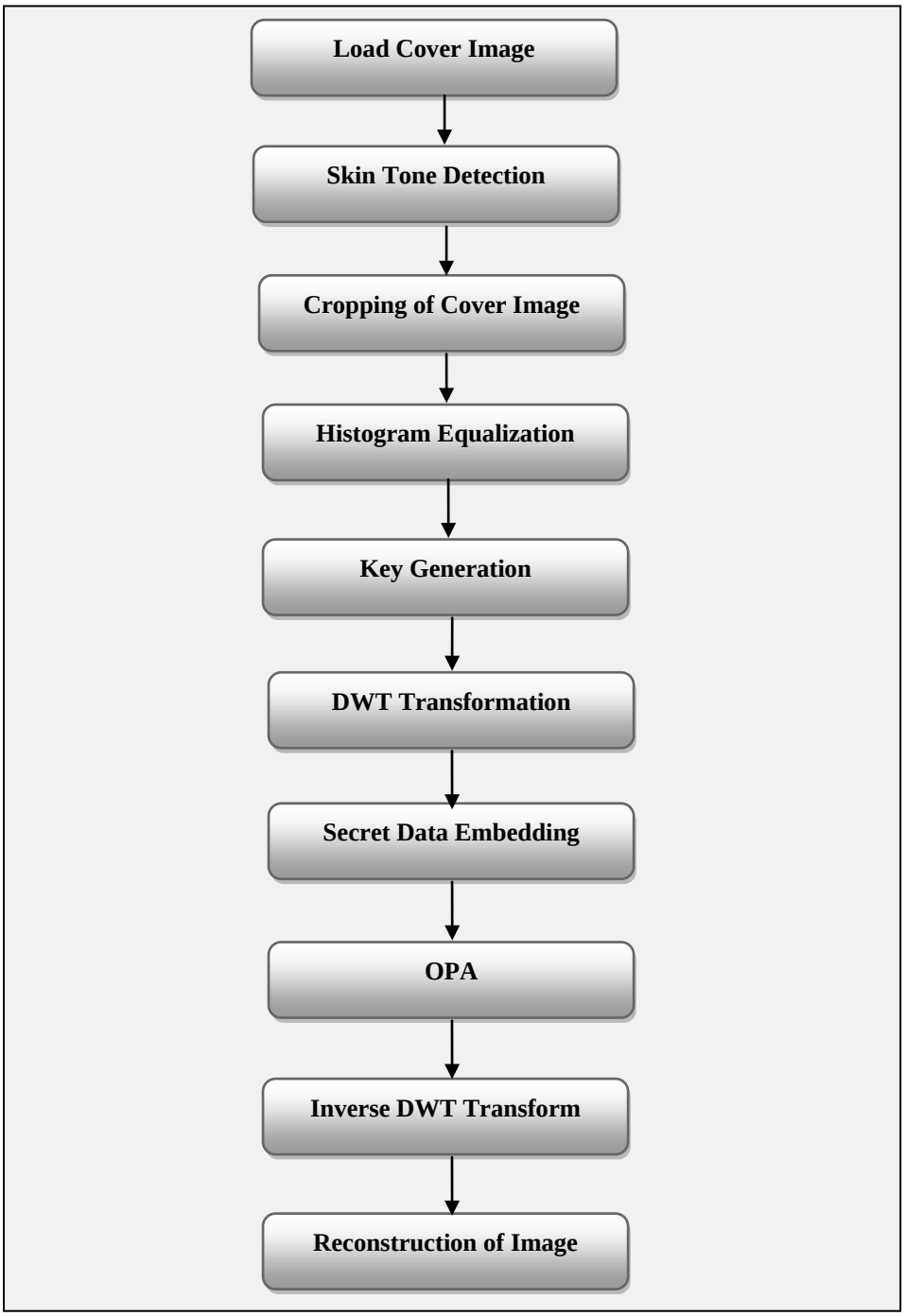

Fig.2- Embedding Process

3.5 Extraction Procedure

Extraction is the reverse process of embedding process. In this embedded secret message is extracted from the cover image and performance is evaluated in terms of PSNR. In the process of extraction following steps are involved (which is also depicted in Fig.3):

1. Stego-image is loaded.
2. Cropping of stego-image is performed.
3. DWT is performed on cropped image.
4. Secret message is extracted from transformed cropped image.
5. PSNR and MSE are calculated as a result of extraction process.

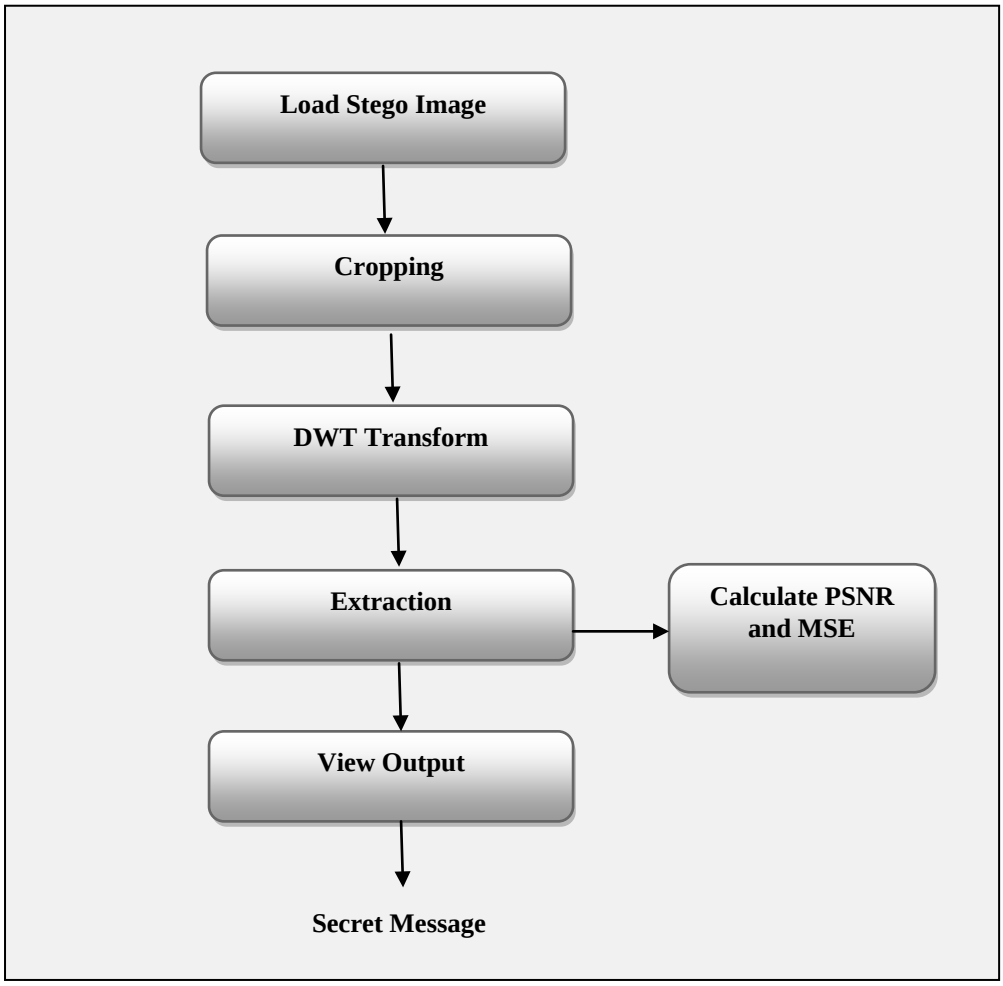

Fig.3- Extraction Process

4. CONCLUSION

In this paper image steganography is presented that uses skin portion of an image in DWT domain for embedding of secret data. Embedding of secret data in only skin region enhance the security and cropping is also help to maintain level of security because without the value of cropped region the message cannot be extracted. The Proposed method will provide better performance in terms of PSNR.

REFERENCES

[1] T. Morkel, J.H.P. Eloff and M.S. Olivier,"An Overview of Image Steganography"Information and Computer Security Architecture (ICSA) Research Group.

[2] Sunny Sachdeva and Amit Kumar,"Colour Image Steganography Based on Modified Quantization Table", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[3] Anjali A. Shejul and U.L. Kulkarni,"A DWT based Approach for Steganography Using Biometrics", International Conference on Data Storage and Data Engineering, 2010.

[4] Sushil Kumar and S.K.Muttoo, "A Comparative Study of Image Steganography in Wavelet Domain", IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101.

[5] Ahmed A. Abdelwahab and Lobna A. Hassaan,"A Discrete Wavelet Transform Based Technique for Image Data Hiding", 25th National Radio Science Conference (NRSC), March 18-20, 2008.

[6] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt,"Biometric Inspired Digital Image Steganography", 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008.

[7] Nagham Hamid, AbidYahya, R. Badlishah Ahmad and Osamah M. Al-Qershi,"Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume 6, Issue 3, 2012.

[8] Mei-Ching Chen, Sos S. Agaian, and C. L. Philip Chen,"Generalized Collage Steganography on Images", IEEE, 2008.

[9] R. Amritharajan, R. Akila and P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Volume 2 – No.3, May 2010.