Survey Paper of Encrypted Data Hiding using Skin Tone Detection

Rekha D.Kalambe
Student
PCST Indore,
Madhya Pradesh, India

Rakesh Pandit
Assistant Professor
PCST Indore,
Madhya Pradesh, India

Sachin Patel
Assistant Professor
PCST Indore,
Madhya Pradesh, India

ABSTRACT

Steganography is the skill of hiding the existence of data in other transmission medium to attain secret communication. It does not restore cryptography but quite boost the security using its abstruse features.

In this paper we have surveyed on a Steganography and cryptography techniques which provide highly secure skin tone data hiding.

Biometric characteristic used to apply steganography is skin tone region of images. Here important data is implanted within skin region of image which will give an outstanding secure location for data hiding.

For this skin tone detection is need to be performed. Different steps of data hiding can be applied by cropping an image interactively. Cropping of an image improved security than hiding data without cropping the whole image, so cropped region works as a key at decoding region.

Cryptography algorithm is used to convert the secret messages to an unreadable form before embedding; which provides a strong backbone for data security. This survey paper focuses on illuminating the technique to secure data or message with authenticity and non repudiation.

So with this object oriented steganogaphy we track skin tone objects in image with the higher security and satisfactory PSNR .Modern steganography's goal is to keep its mere presence undetectable.

Keywords

Setganography, data hiding skin Tone detection, cryptography, digital watermarking.

1. INTRODUCTION

1.1 Steganography

Steganography is the skills of writing secrete messages in such a way that no one, other than the sender and receiver, suspects the survival of the message, a form of security through obscurity.

Fig 1.1 Steganography

As compared to cryptography the advantage of steganography is that messages do not soak up awareness to themselves. Whereas cryptography protects the contents of a message, steganography can protect both messages and communicating parties.

1.2 Data Hiding

In computer field , information hiding is the standard of separation of the design decisions in a computer program that are most likely to change, thus shielding other parts of the program from extensive alteration if the design decision is changed.

The shields involve providing a steady interface which secures the rest of the program from the implementation.

Data hiding is a software development technique specifically used in object-oriented programming to hide internal object details.

Data hiding ensure limited data access to class members and secures object's integrity by preventing accidental or planned changes.

Fig 1.2 Data Hiding

1.3 Digital Water marking

A digital watermark is a type of indicator secretly implanted in a noise- tolerant signal such as audio or image data. It is classically used to recognize ownership of the copyright of such signal. "Watermarking" is the process of concealing digital information in a carrier signal. Both steganography and digital watermarking use steganographic techniques to implant data secretly in noisy signals. But whereas steganography aims impossible to perceive by human senses, digital watermarking attempts to control the robustness as top priority.

Fig 1.3 Digital Watermarking

1.1 1.4 Cryptography

Cryptography previous to the current era was effectively identical with encryption, the conversion of information from a clear state to apparent garbage. The creator of an encrypted message shared the decoding technique required to recover the original information only with destined recipients, thereby preventing unwanted intruder to do the same.

Fig 1.4 Cryptography

2. LITERATURE SURVEY

2.1 Skin tone detection

In Steganography secret message is the data that the intended is the medium in which the message is sender needs to remain secret. The host implanted and serves to hide the presence of the message. Skin detection is the process of finding skin-colored pixels and regions in an image, audio or a video. This process is typically used as a pre-processing step to find regions that potentially have human faces and limbs in images. Actually it is nothing but the color of human skin. Following figure shows the various samples of skin tones.

Fig. 2.1 Skin tone levels

2.2 Skin Tone detection using skin classifier

A variety of categorization methods have been used in the literature for the task of skin categorization. A skin classifier is a one-class classifier that defines a decision boundary of the skin color class in a feature room. The feature space in the context of skin detection is simply the color space chosen. Any pixel which color falls inside the skin color class boundary is labeled as skin.

Therefore, the selection of the skin classifier is straight induced by the shape of the skin class in the color space chosen by a skin detector. Compact and regularly formed the skin color class tends to greater extent classifier.

2.3 Skin Tone detection using HSV model

HSL and HSV are the two most ordinary cylindrical-coordinate representations of points in an RGB color model. The two representations reorganize the geometry of RGB in an attempt to be more intuitive and perceptually relevant than the Cartesian (cube) representation. Now days HSL and HSV are used in color pickers, in image editing software, and rarely in image analysis and computer vision.HSL stands for hue, saturation, and lightness, and is often also called HLS. HSV stands for hue, saturation, and value, and is also often called HSB.

A third model, usually used in computer vision applications, is HSI, for hue, saturation, and intensity. However, while classically consistent, these definitions are not consistent, and any of these abbreviations might be used for any of these three or several other related cylindrical models.

2.4 Skin tone Stegnograpy using RSA Encryption

RSA is public-key cryptography algorithm which is based on the presumed difficulty of factoring large integers, the factoring problem. RSA is named for Ron Rivest, Adi Shamir and Leonard Adelman,

RSA combine work with a public key and a private key. The public key might be known by everybody and it is used for encrypting messages. The encrypted messages with the public key can only be decrypted in a reasonable amount of time using the private key.

The scheme makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n.

That is, the block size must be less than or equal to log2(n); in practice, the block size is i bits, where 2i < n<2i+1. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C.

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PU = {d, n}. For this algorithm to be satisfactory for public- key encryption, the following requirements must be fulfill:

It is possible to find values of e, d, n such that Med mod n =M for all M < n.

2.5 Skin tone Stegnography using Blowfish algorithm

Blowfish is a keyed, symmetric block cipher, developed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption value in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard now receives more attention.

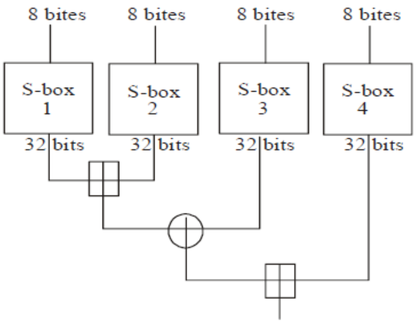

Fig. 2.2 Blow fish with S-boxes

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S- boxes.

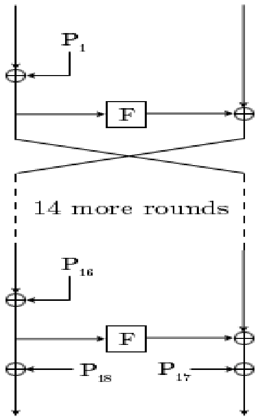

Fig 2.3 Blow fish Algorithm working

2.5.1 *Encoding Algorithms:*

- Obtain the secret text which has to be protected.
- Using the Encryption algorithm encryption is done with the secret data and transformed into eight bits-stream of data.
- Consider a cover image whose size is larger than the secret data.
- The wrap image should be divided into 8-pixel block.
- The secret message which is in bit streams is fixed into a pixel of color image by using LSB Steganography.
- Similarly, embed the entire secret text stream into the image, the image which is obtained is the stego-image (i.e. Secret data embedded into the image).
- Then image which will be obtained appears to be similar to the cover image.

2.5.2 *Decoding algorithm*

- The decoding algorithm is a reverse procedure of encoding procedure.
- Obtain the document file which contains the secret data.
- With the help of secret keys, we can try to open the protected document file which contains the image.
- Convert the document which contains the concealed data into the image file.
- Image file which is obtained is nothing but the stego-image.
- Then we need to divide a stego - image into 8-pixel block.
- Remove the original data from the 8-pixel block of the stego- image with the LSB technique.
- Data which can be obtained from stego-image is in encrypted form.
- The encrypted data will decrypt using Encryption algorithm.
- The final data which will obtain will be the sensitive data.

2.6 Skin tone Stegnography Feistel Cipher

Feistel cipher is a symmetric structure used in the construction of block ciphers, which is designed by German physicist and cryptographer Horst Feistel who did initiating research while working for IBM;

A large ratio of block ciphers uses the scheme, including the Data Encryption Standard.

The advantage of Feistel structure is that it has encryption and decryption operations are similar, even identical in some cases, requiring only a reversal of the key schedule.

Therefore the size of the code or circuitry required to implement such a cipher is nearly halved.

3. RESEARCH METHODOLOGY

3.1 Implementation issues

If we wish to implement the skin tone steganography first of all we have to find the skin region in the given image.

3.2 Predicted flow of the proposed system

Following flow chart shows the predicted behavior of the system. In skin tone steganography it is important to hide the secret data in skin color in the given image. Skin detection, cropping, encryption and hiding the secret data are the important task need to perform.

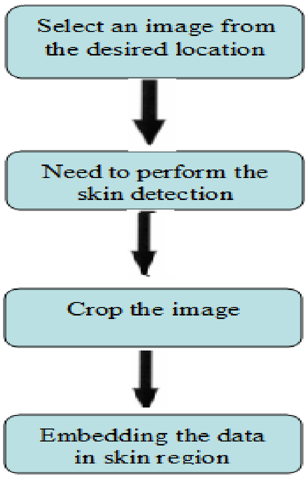
Select an image from the desired location
Need to perform the skin detection
Crop the image
Embedding the data in skin region

Fig. 3.1 Flow Chart of the Proposed System

3.3 Cropping

Cropping is the removal of the external parts of an image to improve framing, emphasize subject matter or change aspect ratio. Depending on the application, cropping is performed on a physical photograph, artwork or film footage, or achieved by digitally using image editing software.

Fig 3.2 Cropping an Image

Skin detection is the procedure of detecting skin-colored pixels and regions in an image or a video.

This procedure is classically used as a preprocessing step to find regions that potentially have human faces, skin and non skin area matches skin tone in images. Various computer vision approaches have been developed for skin detection. Skin detectors classically transform a given pixel into an appropriate color space and then use a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a decision boundary of the skin color class in the color space based on a training database of skin- colored pixels. Detecting skin-colored pixels, although seems a clear-cut easy task, which has confirmed quite challenging for many reasons.

The tone of skin in an image depends on the lighting conditions where the image was clicked. We humans are very good at identifying object colors in a wide range of lighting, this is called color constancy. Color constancy is secrecy of observation. Therefore, an important challenge in skin detection is to represent the color in a way that is invariant or at least insensitive to changes in lighting. In any given color room, skin color occupies a part of such a room, which might be a compact or large region in the space. Such region is usually called the skin color cluster. A skin classifier is a one-class or two-class classification problem. A given pixel is classified and labeled whether it is a skin or a non-skin given a model of the skin color cluster in a given color space. In the context of skin classification, true positives are skin pixels that classifier accurately labels as skin. True negatives are non-skin pixels that the classifier accurately labels as non-skin.

3.4 Securing Information Content using Encryption Method and Stegnography

Most of the existing Stegnographic methods rely on two factors:

- The secrecy of the key and
- The robustness of the Stegnographic algorithm.

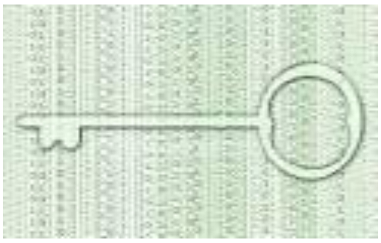

Fig 3.3 Encryption

A variety of encryption algorithms exist such as RSA,DES,AES,OAEP, Blowfish and Two fish which encrypt data strings, thus changing their state from being natural to a seemingly unnatural state.

3.4.1 Securing data using DWT technique

This is another frequency domain in which steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks leading in annoying blocking artifacts. This drawback of DCT is eliminated using DWT.DWT applies on entire image. DWT extends better energy 40 compaction than DCT without any blocking artifact. DWT splits component into frequency bands called sub bands known as

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

Since due to the sensitivity Human eyes to the low frequency part (LL sub band) we can hide secret message in other three parts without making any modification in LL sub band.

As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn’t lose the originality of image that much.

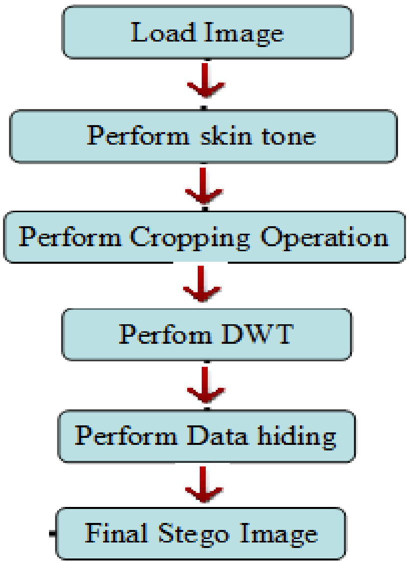

Fig 3.4 flow Of DWT technique

1. Initially load the cover object in which we will hide the secret message (text).

2. After loading the cover object, skin tone detection is performed. This enables us to know where and how much data can be hidden.

3. Cropping: From the detected skin portion, cropping is performed. This is done so that within skin pixels data is hidden at only limited pixel positions.

This feature of cropping enhances security, as any eavesdropper cannot detect secret message just by detecting the skin pixels.

4. Histogram Modification: This is performed to adjust the contrast of the colors.

5. Key Generation: This is the step where the secret message to be selected and is encrypted using RSA and OAEP.

6. DWT: Discrete Wavelet Transform is applied to the cropped skin portion.

7. Secret encrypted message is now merged into the transformed skin pixels.

8. Optimal Parity Assignment is used to assign secret code values to limited areas of cropped skin portion, so as to have least effect over the HVS (human visual system).

9. Inverse DWT: Now the transformed image has secret code which is ready to be merged with the original cover object. The first step to merge this transformed secret message embedded image, with cover object is to inverse transform it.

3.4.2 Masking and Filtering

Masking and filtering techniques are usually restricted to less no. of bits or grayscale images for hiding a message. This is achieving for example by modifying the lightning of parts of the image. As masking alters the visible property of an image, it can be done in such a way that the human eye will not observe the anomalies.

As masking uses visible aspects of the image; which become more robust than LSB modification with respect to compression, cropping and different kinds of image processing. In masking the information is not hidden at the “noise” level, instead it is inside the visible part of the image.

4. CONCLUSION

We can consider the following points while embedding the data which can be hidden into the skin tone. For this purpose we need to find the skin color/s in the selected image. Skin detection in color images and videos is a very efficient way to locate skin-colored pixels, which might indicate the existence of human faces as well as whole body. However, many objects like non skin tone area in the real world have skin-tone colors, such as some kinds of leather, sand, wood, fur, etc., which might be mistakenly detected by a skin detector.

Therefore, skin detection can be very useful in detecting skin and non skin area in controlled environments where the background is guaranteed not to contain skin tone colors.

Skin detection can also be used as an efficient preprocessing filter to find potential skin regions in color images prior to applying more computationally expensive face or hand detectors.

5. REFERENCES

[1]. Bernhard Fink, K.G., Matts, and P.J.: “Visible skin color distribution plays a role in the perception of age, attractiveness, and health in female faces.”Evolution and Human Behavior 27(6) (2006) 433–442

[2]. Anjali A. Shejul, Umesh L. Kulkarni “A Secure Skin Tone based Steganography Using Wavelet Transform”

[3]. Crystal Muang and Dunxu Hu “Skin Detection - a Short Tutorial” Department of Computer Science, Rutgers University, Piscataway, NJ, 08902, USA

[4].https://en.wikipedia.org/wiki/HSL_and_HSV

[5].http://en.wikipedia.org/wiki/Cropping_(image)

[6]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, “Securing Information Content using New Encryption Method and Steganography”

[7]. petit colas, F.A.P.: “Introduction to Information Hiding”. In: Katzenbeisser, S and Petit colas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.

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

[9]. Chang, C. C., Chen, T.S and Chung, L. Z.,”A steganographic method based upon JPEG and quantization table modification,” Information Sciences, vol.[4], pp. 123-138(2002).

[10]. Yang, Wan, Liao Xiaofeng., Xiao Di., and Wong Kwok-Wo. (2008). One-way hash function construction based on 2D coupled map lattices. Journal of Information Sciences 178 (2008) 1391- 1406

[11]. Aruna Mittal, “Object Oriented Steganography using Skin Tone Detection and RSA Encryption Scheme”.