An OPA Based Highly Secure Steganography Scheme Using Hash Based LSB Technique and Huffman Coding

Bhavna Sharma [1], Shrikant Burje [2], Anant G Kulkar

[1]Dept. of ECE, M.Tech. Student, Rungta College of Engineering & Technology Bhilai

[2]Dept. Of ECE, Reader in Rungta College of Engineering & Technology Bhilai

[3]Dept. Of ECE, Reader in Rungta College of Engineering Raipur

Abstract

Steganography is the method of hiding the existence of data in another transmission medium to achieve secret communication. Steganography method used here is based on biometrics. And the biometric feature used to implement is skin tone region of images.

Here secret data is embedded with skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding performed using Hash based Least significant bit Algorithm. Secret data is hidden in least significant bit by tracing skin pixels in the sub-band, first the secret message data was encoded with Huffman coding algorithm.

For data hiding two cases are considered, first is with noise and other is without noise. In both the cases different steps of data hiding are applied either by noise an image interactively or without noise. Both cases are compared and analyzed from different aspects. This is concluded that both cases offer enough security. Optimal parity assignment and public key cryptography is used here to provide more security to our approach.

Main feature of cropping is that this results into an enhanced security because cropped region works as a key at decoding side. This approach shows that by adopting an object oriented steganography mechanism, in the sense that, we track skin tone objects in image, we get a higher security. And simulation result shows that satisfactory PSNR (Peak-Signal-to-Noise-Ratio) is also obtained.

Keywords*:* **Steganography, PSNR, Parity, Huffman Coding, biometric, security.**

1. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity." Consequently, functions provided by Stéganô only hide message, without encryption. Indeed steganography is often used with cryptography. Cryptography on other hand is the method of encrypting data in form of secret message. The message can be deciphered only with the secret key embedded by any source. The transportation medium processing the message can sense about communication taking place. While steganography enables us, to hide our data in any file who looks likes a normal file in every aspect. Modern Steganography's purpose is to keep its mere presence imperceptible, but steganographic systems—because of their invasive nature—renders glimpse of traces in the cover medium. Even if encrypted content is not surfaced, the existence of it is. Upgrading in the cover medium alters its statistical properties, so third party security can detect the distortions in the resulting stego medium's statistical properties. The approach of identifying these distortions is termed as statistical steganalysis.

f_E : Steganographic function "embedding"

f_E^{-1}: Steganographic function "extracting"

Cover: cover data in which emb will be hidden

Emb: message to be hidden

Stego: cover data with the hidden message

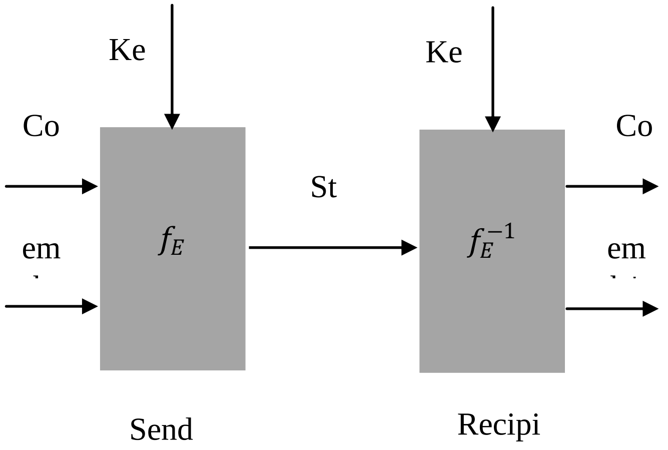

Figure 1: Graphical Version of Steganographic System

I. Digital Steganography

Digital Steganography provides its applications for the digital data. It covers complete world of digital applications like encryption of audio, video and data files. Today in the world of internet it provides numerous applications for transportation over third party channels and the encoded transmission media. The digital steganography by its characteristics is divided in three of its products i.e.

a. Secure Communication
b. Digital Watermarking
c. Digital Storage and linkage

Secure Communication is a state-of-the-art digital steganography software package developed by DMT for clandestine high bit rate multimedia communication [1, 2, 3]. The software powers the user to select a simple multimedia data file or "container" for encrypting a personal hidden text, audio sequence, video clip, or any form of data file. The body of the text messages is hashed with those of the container file to produce a key file. The key file is also known as a “Stegfile”.

The cryptography operation is used first to scramble the sacred text. Second, for steganography operation, the scrambled data is placed or "encrypted" into the least significant bits (LSB) of the container data. The leading failure point of these techniques can be seen as container file has to be specifically magnificent for particular amount as compared to that of encrypted resource. Major restraints include the requirement of knowledge for the precise and exact location of the encrypted text, the restricted container data formats, and the transport confinement of using encryption algorithms to specific countries. These difficulties are circumvented by the use of Secure Communication.

Digital Watermarking can embed any of the text or image watermark imperceptibly into an "unlabeled" image. The text watermark can be of different characters. For example, in a multi-color image of size 512 x 512, more than a few thousand characters may be embedded. For a 512 x512 size image, an image watermark with size up to 128 x 128 can be embedded entirely into the image, without any loss of image integrity. This unique "image-in-image" watermarking technique has been submitted for an international patent and is currently under reviewing status.

The main function of Digital Storage and Linkage is to securely link the personal record and digital photograph together. Furthermore it should create a hash file that can be securely saved in the database. This hash file must be unique and should only be decrypted with the pre-defined photograph and respective personal record. Tampering with any one of these files will render the decrypting process ineffective. The database administrator will be able to detect whether these files have been modified, by considering the primary hash file with the digitalized photograph. An optional password is also available to protect the hash file prior to data storage. The basic operation of Digital Storage and Linkage is illustrated in figure2.Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are including:

(i) Least significant bit insertion (LSB)

(ii) Masking and filtering

(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in image, thus embed the information in significant marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the human perceptible difference because the amplitude of the change is small.

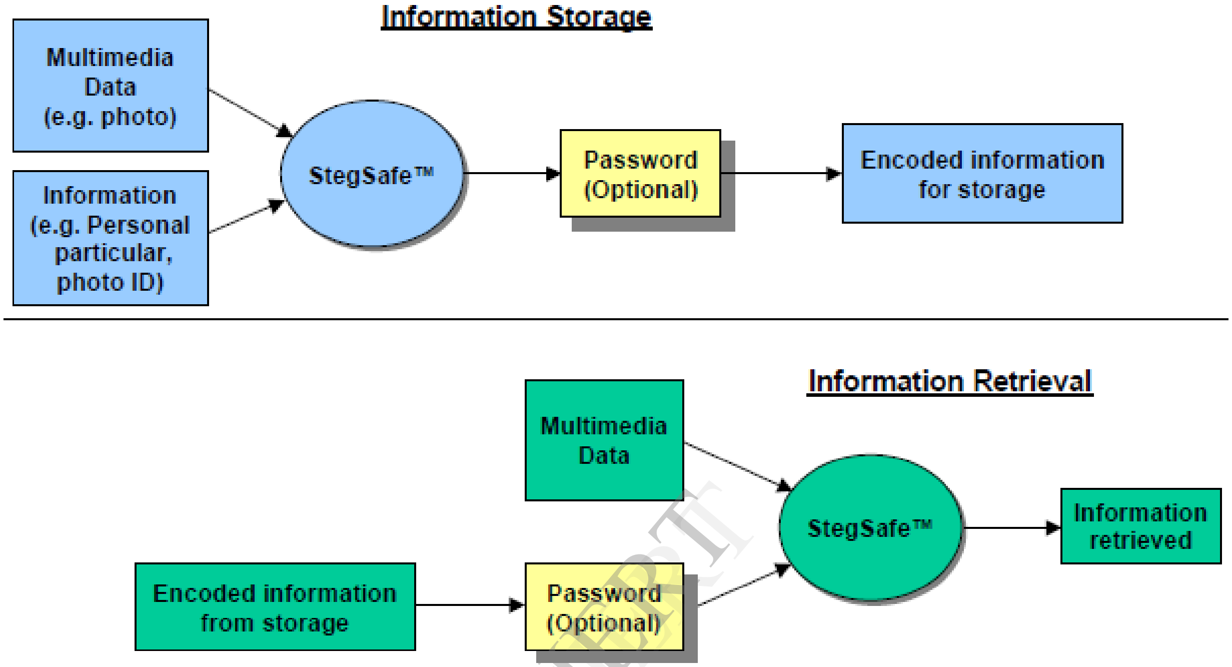
Information Storage
Multimedia Data (e.g. photo)
Information (e.g. Personal particular, photo ID)
StegSafe™
Password (Optional)
Encoded information for storage
Information Retrieval
Multimedia Data
Encoded information from storage
Password (Optional)
StegSafe™
Information retrieved

Figure 2: Digital Storage and Linkage

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

2. Related Work

S. Mohanapriya presented a paper on a technique using cryptography and steganography for securing information over mobile in MMS. Here they are using Discrete Cosine transform (DCT) for image steganography and tiny encryption algorithm for cryptography. Tiny encryption algorithm is block cipher algorithm. It is simple and fast but best for mobile application. [4]. Ankita Agrawal presented a new generalized model by combining cryptographic and steganographic Technique. These two techniques encrypt the data as well as hide the encrypted data in another medium so the fact that a message being sent is concealed. In cryptography we are using Simplified Data Encryption Standard (S-DES) algorithm to encrypt secret message and then alteration component method is used to hide encrypted message. By using these two techniques the security of secret data increases to two tiers and a high quality of stego image is obtained [5]. Garima Tomar’s project simulates an effective data hiding technique i.e. steganography based on LSB insertion and RSA encryption in order to provide seven million times better security about hidden data ,than the previous work. The Main idea of proposed scheme is to encrypt secret data by RSA 1024 algorithm, convert it in to binary sequence bit and then embedded into each cover pixels by modifying the least significant bits (LSBs) of cover pixels [6]. Malik H.'s paper proposeed an active steganalysis method for quantization index modulation (QIM)-based steganography. The proposed nonparametric steganalysis method uses irregularity (or randomness) in the test image to distinguish between the cover image and the stego image. They shown that plain quantization (quantization without message embedding) induces regularity in the resulting quantized object, whereas message embedding using QIM increases irregularity in the resulting QIM-stego. Approximate entropy, an algorithmic entropy measure, is used to quantify irregularity in the test image. The QIM-stego image is then analyzed to estimate secret message length [7].

3. Proposed Work

Algorithm for skin detection using HSV Figure 3:

First, the image in RGB was converted to HSV color space, because it is more related to human color perception. The skin in channel H is characterized by values between 0 and 50, in the channel S from 0.23 to 0.68 for Asian and Caucasian ethnics [6]

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.

a. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.

2. Compute $n = pq$

a. nIs used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute,$\varphi(n) = \varphi(p)\,\varphi(q) = (p - 1)\,(q - 1)$where φ is Euler's totient function.

4. Choose an integer e such that,$1 < e < \varphi(n)\ and\ gcd\ (e, \varphi(n)) = 1$ i.e., e and φ(n) are coprime.

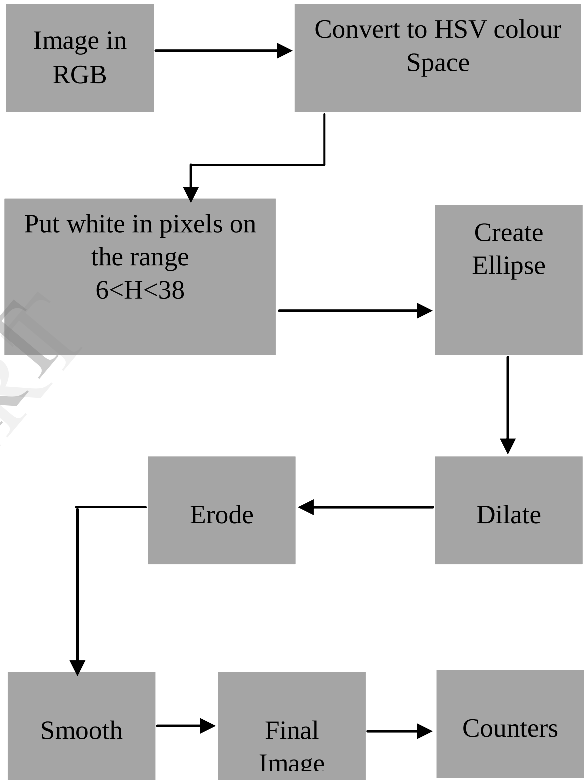
Image in RGB
Convert to HSV colour Space
Put white in pixels on the range 6<H<38
Create Ellipse
Dilate
Erode
Smooth
Final Image
Counters

Figure 3: Skin Detection Scheme

a. *'e'*Is released as the public key exponent.

b. *'e'*Having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

5. Determine d as $d - 1 \equiv e\ (mod\ \varphi\ (n))$ i.e., d is the multiplicative inverse of e (modulo φ(n)).

a. This is more clearly stated as solve for, *'d'* given de ≡ 1 (mod φ(n))

b. This is often computed using the extended Euclidean algorithm.

c. ‘*d*’ Is kept as the private key exponent.

By construction, $d \cdot e \equiv 1$ (mod φ(n)). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. P, q, and φ(n) must also be kept secret because they can be used to calculate d.

Optimal Parity Assignment: Let the image palette contain N colors $c_1, c_2, \dots, c_N$ with parities $P_i, P_i \in \{0,1\}$.The parity assignment determines an isolation s_i for the $i-th$ color (s_i is the distance from color c_i to the closest color with different parity). The colors occur in the original image with frequencies, $P_1, \dots, P_N, P_1 + \dots + P_N = 1$. Provided the message carrying pixels are selected non-adaptively, for a message of length k, approximately k_{P_i} pixels of color c_i will contain message bits. The average square of the distance between the original and the stego-image can be expressed as:

$$\frac{1}{2} kE(P_1, \dots, P_N) = \frac{1}{2} k \sum_{i=1}^{N} p_i s_i^2$$

The Continuous Wavelet Transform and the Wavelet Series

The Continuous Wavelet Transform (CWT) is provided by equation (12), where x(t) is the signal to be analysed. Ψ(t) is the mother wavelet or the basis function. All the wavelet functions used in the transformation are derived from the mother wavelet through translation (shifting) and scaling (dilation or compression).

$$X_{WT}(\tau, s) = \frac{1}{\sqrt{|s|}} \int x(t) \Psi^* \left(\frac{t-\tau}{s} \right) dt$$

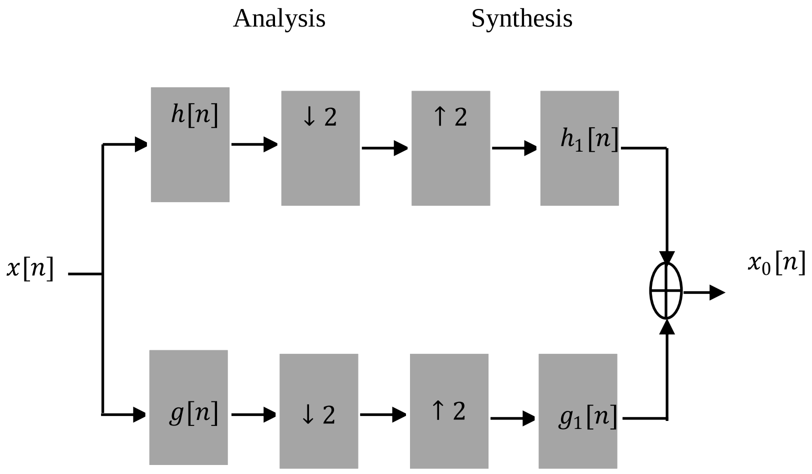

Figure 4.8: The schematic diagram to realize discrete wavelet transform. Here the filter names are changed

4. Results

Table 1: shows the variations of PSNR and MSE for different images

Sr. No.	Cover Image	PSNR	MSE
1	Test image 1	51.9769	30.9727
2	Test image 2	58.3469	28.5297
3	Test image 3	59.9614	27.9823
4	Test image 4	62.3456	27.1364
5	Test image 5	64.1389	26.7823

Table 2: describes the variations in MSE and PSNR for cover image 1 with different noise channels

Noise	Cover Image	PSNR	MSE
JPEG compression	Cover Image 1	3.6489	176.7254
Salt and pepper noise	Cover Image 1	3.5891	177.5642
Gaussian noise	Cover Image 1	3.9864	165.8451
Rotation	Cover Image 1	4.2165	176.9345
Cropping	Cover Image 1	4.9687	151.1324
Speckle noise	Cover Image 1	4.6785	166.2156
Contras adjustment	Cover Image 1	4.7695	158.3241

Table 3: describes the variations in MSE and PSNR for cover image 2 with different noise channels

Noise	Cover Image	PSNR	MSE
JPEG compression	Cover Image 2	5.3412	144.2563
Salt and pepper noise	Cover Image 2	5.4257	146.6796
Gaussian noise	Cover Image 2	5.7861	132.4981
Rotation	Cover Image 2	6.6324	127.9345
Cropping	Cover Image 2	6.2345	128.9641
Speckle noise	Cover Image 2	69.354	121.2345
Contras adjustment	Cover Image 2	6.7543	123.8465

5. Conclusion and Future Scope

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. Proposed framework is based on steganography that uses Biometric feature i.e. skin tone region. Skin tone detection plays a very important role in Biometrics and can be considered as secure location for data hiding. Secret data embedding is performed in Wavelet domain using fast wavelet transforms. The DD-DWT outperforms than DWT as well as DCT. Using Biometrics resulting stego image is more tolerant to attacks and more robust than existing methods. Results shows in terms of peak signal-to-noise ratio, and clearly shows that our technique outperforms the previous approaches in skin tone based steganography.

6. References

[1] Ho, A.T.S., "Method and Apparatus for Camouflaging Data", PCT/SG98/00023, 18 March, 1998

[2] Ho, A.T.S. and Tam, S.C., "Methods for Embedding Image, Audio and Video Watermarks in Digital Data", PCT/SG98/00039, 1 June, 1998

[3] Ho, A.T.S., Tam, S.C., Tan, Siong Chai, and Yap, Lian Teck, "Methods of Digital Steganography for Multimedia Data", SG9803458-0, 28 October, 1998.

[4] S.Mohanapriya, "Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 5, May 2012

[5] Ankita Agarwal, "Security Enhancement Scheme for Image Steganography using S-DES Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[6] Garima Tomar, "Effect of Noise on image steganography based on LSB insertion and RSA encryption", IOSR Journal of Engineering, Mar. 2012.

[7] Malik H., Subbalakshmi K.P., Chandramouli R., "Nonparametric Steganalysis of QIM Steganography Using Approximate Entropy", IEEE, April 2012.