ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2013

A STEGNOGRAPHY SCHEME USING RSA AND OPA ALGORITHS WITH HISTOGRAM MODIFICATION IN SKINTONE DECETION

Bhavna Sharma[1], **Shrikant Burje**[2]

M.Tech. Student [DE], Dept. Of ECE, Rungta College of Engineering Bhilai, India[1]

Vice Principal, Dept. of ECE, Rungta College of Engineering Bhilai, India[2]

ABSTRACT: More than just a science, *Steganography* is the art of secret communication or the science of invisible communication Steganography conceptually implies that the message to be transmitted is not visible to the informal eye. The main objective of Steganography is mainly concerned with the protection of contents of the hidden information. Images are ideal for information hiding, Because of the large amount of redundant space is created in the storing of images. In this paper, we propose a new method of Steganographic techniques for digital images, which having RSA and OPA (optimal Parity Assignment) algorithm .These two Algorithm methods are used in Digital image to improve security. In image a secret data is embedded within skin region of That will provide an excellent secure location for data hiding. Histogram equalization is performed in the skin portion in order to enhance the intensity of the image. The RSA algorithm involves key generation and encryption. The parity assignment directly affects the energy of image modifications due to message embedding. Obviously, if close colors are assigned opposite parities, the energy of the modifications will be smaller.

***KEYWORDS*:** OPA, RSA, skin region, histogram

I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" [1] defining it as "covered writing". A steganographic system thus incorporates mist content in random or unauthorized cover structure so as to escape from illegal and unauthorized suspicion. Long ago, people used encrypted tattoos or transparent ink to transport sacred content. In present scenario, advanced communication approaches powered by digitalization is a globally used media. Steganography is the method and approach of hiding communication of digital data. In image steganography the information is hidden exclusively in images. Digital images are composed of pixels. Each pixel represents the color (or gray level for black and white photos) at a single point in the image, so a pixel is like a tiny dot of a particular color. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. The JPEG is the most suitable format to be used as cover image for image steganography since JPEG is the most common compression standard used for still images (Tseng and Chang, 2004). Furthermore, the majority of steganography techniques used for JPEG images, such as JSteg and Outguess, adopt the standard JPEG compression.

II. LITERATURE SURVEY

We give an overview of different types of steganography with the emphasis on image steganography. This section discusses some of the selected steganographic methods. These particular Methods are used as a subject in our analysis Consider a variant of boundary pixel steganography proposed by Liang et al. [2]. Boundary pixel steganography hides a message along the edges, where white and black pixels meet—these are known as boundary pixels. Note that the boundary pixels are those pixels within the image where there is colour transition occurred 22 between white and black pixels. The boundary pixels should not be confused with the four borders of an image. To obtain higher imperceptibility, the pixel locations used for embedding are permuted and distributed over the whole image. The distribution of message bits is controlled by a pseudorandom number generator whose seed is a secret shared by the sender and the receiver of the hidden message. This seed is also called stegokey.

Pan et al.[3] developed a steganographic method that embeds secret messages in binary images this method is more flexible, in terms of choosing the cover image block. The Panet et al. method uses every block within an image to carry a secret message. This gives it a greater embedding capacity. The security is also improved by having less alteration of the cover image.

The steganographic method developed by Chang et al. [4] can be considered a variant improved from the binary image steganography developed by Pan et al.[3]. In general, this method offers the same embedding rate as the Pan et al. method, which is r = log2 (mn + 1) bits per block (m × n is the block size).However, this method is superior to the Pan et al. method in the sense that it alters one pixel (at most) to embed the same amount of message bits within a block (as opposed to two pixels in the Pan et al. method). Thus, this method provides a higher level of security by reducing the alteration of the stego image.

Another steganography using a block-based method to embed secret messages in binary images is that developed by Wu and Liu in [5]. This technique also starts by partitioning a given image into blocks. To avoid synchronisation problems (which lead to incorrect message extraction) between embedding and extraction, this technique embeds a fixed number of message bits within a block. In their implementation details, the authors opt to embed one message bit per block. The embedding algorithm is based on the odd-even relationship of the number of black pixels within a block.

III. METHODOLOGY

Here we introduce a new approach of data hiding in image .Here secret data is embedded within 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. Histogram equalization is performed in the skin portion in order to enhance the intensity of the image. Additionally secret data embedding is performed using Hash based LSB technique, and message is secured and encoded through Huffman coding, this approach outperforms the traditional frequency domain approach. Secret data is hidden in one of the least significant bits by tracing skin pixels in that sub-band. For data hiding two cases can be considered, first is with cropping and other is without cropping, cropping give some reliable results as compare with without cropping scenario. This study shows that by adopting an object oriented steganography mechanism, in the sense that, we track skin tone objects in image or video frame, we get a higher security. And simulation result shows that satisfactory PSNR (Peak-Signal-to-Noise Ratio) is also obtained. The detection of skin colors in images is a very essential and increasingly popular technique in digital vision for detecting and tracing humans. As in visual cue, skin color is robust and inexpensive to compute, makes it useful as an attention-grabbing mechanism for further expensive computations. It has been studied that skin color from all ethnicities, clusters tightly in hue-saturation (HS)-space. If we ignore intensity it would immediately introduces some invariance to lighting conditions. Histogram Equalization method is applied to enhance the global contrast of many images, specifically when the usable data of the image is introduced by close contrast values. By the virtue of this adjustment, the intensities can be effectively distributed on the histogram. It give space to areas of lower local contrast to achieve a higher contrast. Histogram equalization can accomplish this via effectively spreading out the most frequent intensity values.

An RSA Algorithm used for encryption has two inputs i.e. a **public key** and a **private key.** The public key is accessible to the public and works for encrypting the sacred data. The messages which are ought to be encrypted by the use of public key can only be decrypted in a considerable amount of time if we use the private key. Image is compress by lossless compression method, here we use Huffman compression method Huffman compression is a variable length coding whose performance varies with the input image bit stream. The compression is straight foreword proportional to smoothness of the image. Greater the smoothness and higher the redundancy better will be the compression. Subjective and objective measures are the two approaches used conventionally to test the distortion of the processed image. Subjective measure is not every time reliable because the human vision is metric in analyzing the distortion of the stego objects. Human vision may vary with every individual; hence this approach is not preferred. In objective measure, the mean square error (MSE) represents the cumulative squared error between the stego image and cover image. A lower figure of MSE conveys lower error/ distortion between the cover and stego image. The equation of MSE to assess the stego and cover object is given by:

$$\text{MSE}=\frac{1}{m*n}\sum_{i-1}^{m}\sum_{j-1}^{n}(A_{ij}-B_{ij})^{2}$$

Whereas Aij represents pixel in the cover image and Bij represents pixel in the stego image; m, n represents the height and width of the image respectively. It is measured in constant and the unit is decibel (dB).

Peak Signal to Noise Ratio (PSNR) is a metric which calculate the distortion in decibels, between two images. Higher the PSNR indicates a better reconstructed or stego image. The PSNR is represented by the following equation:

$$\text{PSNR}=10*\log_{10}\frac{(Max)^{2}}{MSE}$$

The OPA algorithm is the parity assignment algorithm, directly affects the energy of image modifications due to message embedding. Obviously, if close colors are assigned opposite parities, the energy of the modifications will be smaller. A natural question to ask is whether it is possible to further improve the performance by using an optimized palette parity assignment. For a practical method, which does not have access to the original image, the palette parity assignment has to be reconstruct able from the modified image at the receiving end.

IV. Result

Detected skin portion from the original image using HSV transform, this works on the hue, saturation and value for particular skin tone and pixel are classified according to that HSV values in fig.1

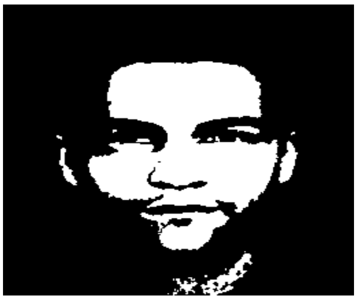
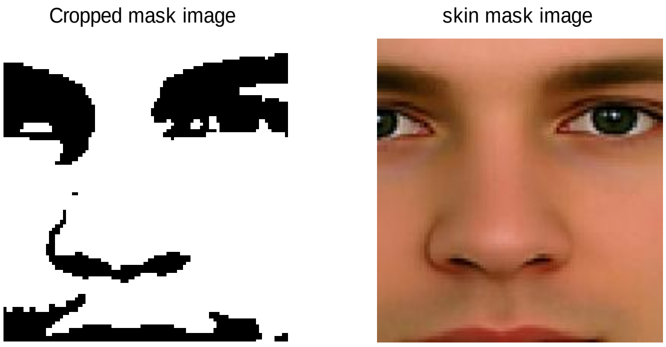


Fig.1 of skin detection

Cropped skin portion from detected skin portion, figure shows cropped mask image and skin mask image fig.2



Cropped mask image

skin mask image

Fig 2 skin cropping and masking

Modification of intensity level in the cropped skin portion using histogram equalization, this level up the intensity values in the cropped skin portion in fig.3

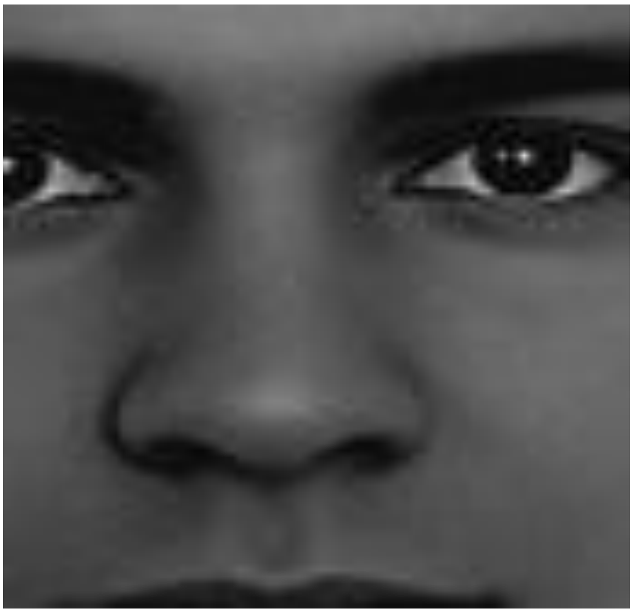


Fig 3 by using Histogram Equalization

Huffman Encoded Message Embedded and encrypted in histogram equalized cropped skin image using Hash based LSB technique fig 4

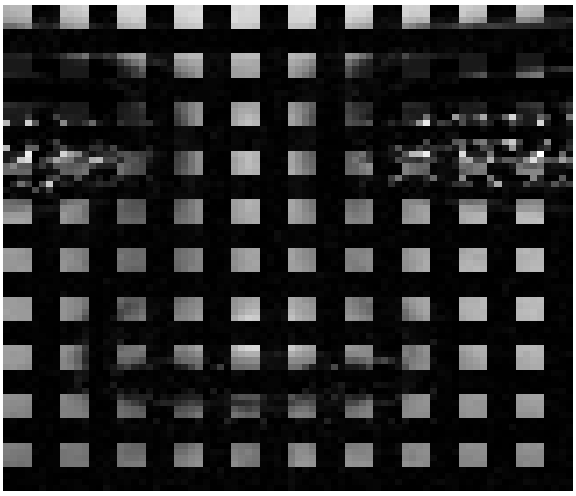


Fig 4 Embedded and encrypted image

Sr. No.	Cover Image	PSNR	MSE
1	Test image 1	63.9995	30.069

Noise	Cover Image	PSNR	MSE
JPEG compression	Cover Image 1	23.6489	76.7254
Salt and pepper noise	Cover Image 1	23.5891	77.5642
Gaussian noise	Cover Image 1	23.9864	65.8451
Rotation	Cover Image 1	24.2165	76.9345
Cropping	Cover Image 1	24.9687	51.1324
Speckle noise	Cover Image 1	24.6785	66.2156
Contras adjustment	Cover Image 1	24.7695	58.3241

V. 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 using Hash based LSB technique and message is encoded through Huffman coding scheme. 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.

REFERENCES

[1.] R A Isbell, “Steganography: Hidden Menace or Hidden Saviour”, Steganography White Paper, 10 May 2002.

[2.] G.-l. Liang, S.-z. Wang, and X.-p. Zhang. Steganography in binary image by checking data-carrying eligibility of boundary pixels. *Journal of Shanghai* University (English Edition), 11(3):272–277, 2007

[3.] H.-K. Pan, Y.-Y. Chen, and Y.-C. Tseng. A secure data hiding scheme for two-color images. 5th IEEE Symposium on Computers and Communications,pages 750–755, 2000.

[4.] C.-C. Chang, C.-S. Tseng, and C.-C. Lin. Hiding data in binary images. *1stInternational Conference on Information Security Practice and Experience*,3439:338–349, 2005.[11] S. Chatterjee and A. S. Hadi. *Regression*

[5.] M. Wu and B. Liu. Data hiding in binary image for authentication and annotation. *IEEE transactions on multimedia*, 6(4):528–538, 2004

[6.] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment”, SANS Institute, January 2002.

[7.] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001.

[8.] Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 147:03, June 2000.

[9.] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April 1998

[10.] Venkatraman, S., Abraham, A. & Paprzycki, M., “Significance of Steganography on Data Security”, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004.

[11.] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM,47:10, October 2004.

[12.] Murray, J.D. & Van Ryper, W. 1996. Encyclopedia of graphics file formats. O'Reilly Publishers.