International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Data Hiding using Skin Detection, DWT Technique and RSA with Bit Shift Method

Jayoti Kumari[1], Khushboo Yadav[2]

[1]*M. Tech Scholar, Dept. of Computer Science & Engineering, RPSGOI Mahendergarh,Haryana,India*

[2]*Associate Professor, Dept. of Computer Science & Engineering, RPSGOI Mahendergarh,Haryana,India*

Abstract— *Steganography is a useful tool that helps to achieve secret communication. Till now the available methods hide the secret data over the image on a fixed pattern that makes a user identify the pattern easily. We are providing a dynamic pattern extraction approach using biometric. According to proposed approach we will perform some biometric operation detects the skin area from the image. After detecting the skin area, edge detection is performed. As the edges will be detected we will use this area as the pattern to hide the data over the image. The secret data is compressed using the DWT technique and then further compressed secret information is encrypted using RSA algorithm with bit shift method. This proposed technique provides more security to the data.*

Keywords: Biometrics, DWT,RSA, PSNR, Security, Skin tone detection, edge detection

I.INTRODUCTION

Steganography derived from Greek, literally means "covered writing".[2] Steganography is a technique that embedding the secret information into an another image so that unknown user cannot identify that secret information.

A. *RGB & YCbCr (Yellow, Chromatic Blue, Chromatic red) Color Space*

RGB color space is the most commonly used color space in digital images. It encodes colors as an additive combination of three primary colors: red(R), green (G) and blue (B). One main advantage of the RGB space is its simplicity. However, it is not perceptually uniform, which means distances in the RGB space do not linearly correspond to human perception. In addition, RGB color space does not separate luminance and chrominance, and the R,G, and B components are highly correlated. The luminance of a given RGB pixel is a linear combination of the R, G, and B values. Therefore, changing the luminance of a given skin patch affects all the R, G, and B components. In other words, the location of a given skin patch in the RGB color cube will change based on the intensity of the illumination under which such patch was imaged! This results in a very stretched skin color cluster in the RGB color cube.

YCbCr (*Y* refers to intensity, *Cb* refers to Chromatic blue and *Cr* refers to Chromatic red) is a transformation color space. RGB images are transformed into YCbCr color because this color space will remove the correlation of R,G,B colours from the given image which results less noticeable distortion. The data is embed into the chromatic red part. [4]

B. ANCIENT STEGANOGRAPHY

Throughout history steganography is used for secret transformation of information among the people. During Second World War, to write the secret information on the paper, invisible ink was used to so that the paper appears to an average person as just a blank piece of paper. Liquids such as milk, vinegar, fruit juices were used to read out the message. In Ancient Greece, they shave the head of the messenger to hide the secret information at its head and then wait to grow up the hairs and after that the information is extracted by again shave the head of the messenger at the destination site.

C. STEGANALYSIS

The term steganalysis is basically an art and science which detect hidden secret message using steganography. It is similar to cryptanalysis applied to cryptography. Goal of steganalysis is to identify the packages, detect either there is any message encoded or not, if there is any message than recover that message.

II. PURPOSE

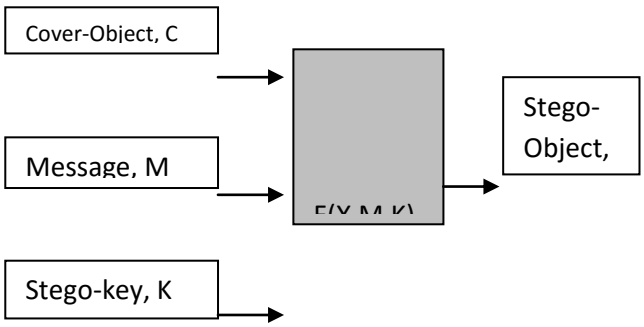
"The concept of hiding information in other content has existed for centuries; the formal study of information hiding is called steganography." Steganography allows a sender to embed a hidden file or message inside a cover file. A cover file is simply a file that is used to embed hidden data into. This cover file may be a graphics image, an audio file (such as a WAV or MP3 file).

III. PRESENT METHODS AND TECHNIQUES

Steganography is implemented in digital image using various methods. The simplest method to implement

steganography is LSB (Least Significant Bit). It embeds bits of secret data over the least significant bits of cover image.

Basic Steganography Model:



Message is that secret information that sender always wants to make it confidential.

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message [10]

IV. PROPOSED WORK

A. *Proposed algorithm*:

Step 1: Cover image is loaded & skin color detection is performed for the biometric image.

Step 2: If the image is not biometric then apply canny edge detector algorithm for the non-biometric image.

Step 3: Once the edges of cover image are found then load the secret image.

Step 4: After loading the secret image, DWT technique is applied to compress the secret image as compressed image will less distort the cover image.

Step 5: Then RSA encryption algorithm with bit shift method is performed.

Step 6: Encrypted message is then embed behind the cover image.

Step 7: Stego image with better quality is obtained.

All the above steps are followed to hide the secret data over the cover image. The correlation property is exploited in an proposed technique.

$IM_w(x,y)= IM(x,y)+k*X(x,y)$.

In the above equation, k is a gain factor and IM_W is the steganographed image. With the increases of k factor the robustness of the hidden message also increases. X(x, y) is an PN pattern which create a steganographed image.PN pattern is added to the cover image IM(x, y).

The Proposed algorithm is compared for more than 4 images on the basis of their corresponding MSE and PSNR value.

By comparing the values we find that the proposed method gives better result.

B. Calculate PSNR value:

There are various steps to find the PSNR value:

Step 1: Calculate the MSE value as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where MSE is mean squared error of an image. I is an input image of m*n dimension and K is a noisy image.

Step 2: After determining the MSE value, the PSNR value is evaluated as:

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

Where PSNR is peak signal to noise ratio. MAX is a maximum value of the input image.

Higher value of PSNR indicate good quality of the image.

C. RSA Algorithm:

Secret image after compressed by DWT is encrypted by RSA algorithm. RSA with bit shift method is used where bits of each byte of image pixels is changed to improve the security of image.

There are various steps to implement RSA algorithm:

1. Choose two large prime numbers p, q randomly.

2. Compute n = pq.

3. Calculate φ (n) as follow:

φ (n) = (p-1)(q-1)

4. Choose an integer e such that e is relatively prime to φ (n).

$$1 < e < \varphi(n)$$

such that

$$\gcd(\varphi(n), e) = 1$$

5. Determine d, $1 < d < \varphi$, such that

$$d = e^{-1} (\mathrm{mod}(\varphi(n)))$$

6. Encryption:

Plaintext M < n

Ciphertext $C = M^e \bmod n$

7. After the encryption bit shift method is used where left four bits of a byte are XOR with the right four bits and resultant bits are set at the place of right 4 bits.

8. Decryption:

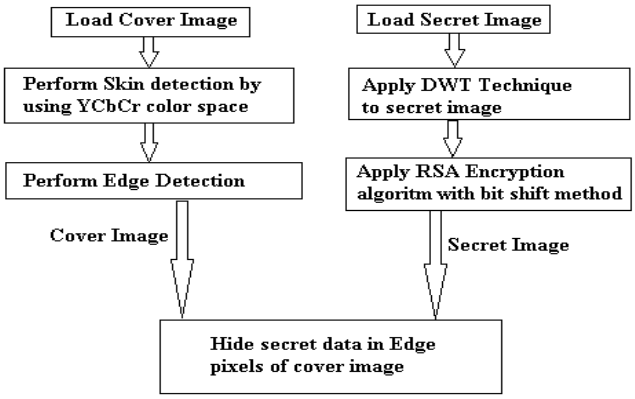
Ciphertext C

Plaintext $M = C^d \bmod n$

The above algorithm encrypts the image which is than hide behind the cover image.

V.Embedded Flowchart

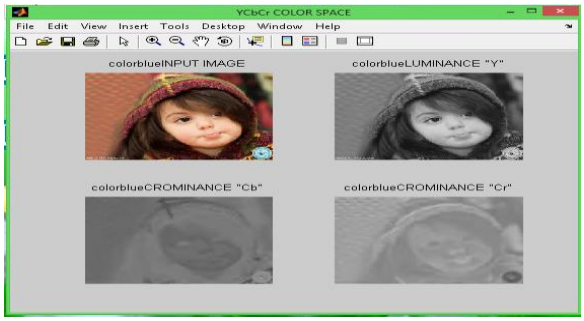
The flowchart shows that first the cover image is loaded and then skin tone detection is done when the cover image is biometric and if the image is non-biometric then edge detection algorithm is applied. After that the secret image is loaded and DWT method is applied to it which will give compressed secret image. Then this image is encrypted by using the RSA with bit shift method. Encrypted image is then embed into the edge pixels of the cover image. This method of data hiding is more secure as secret image only uses the edge pixels and data is not dispersed in the whole cover image. As distortion of cover image is less and then the image quality of stego image is good.



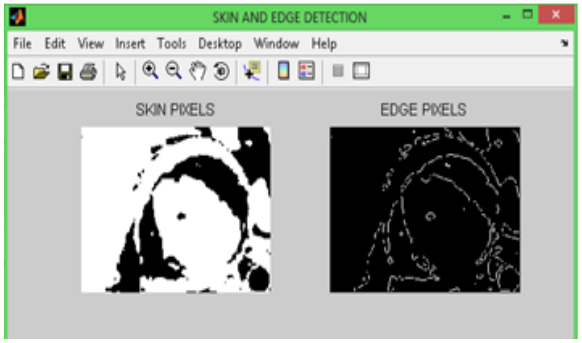
VI. RESULTS AND COMPARISON

Several experiments have been performed to compare the performance of images.

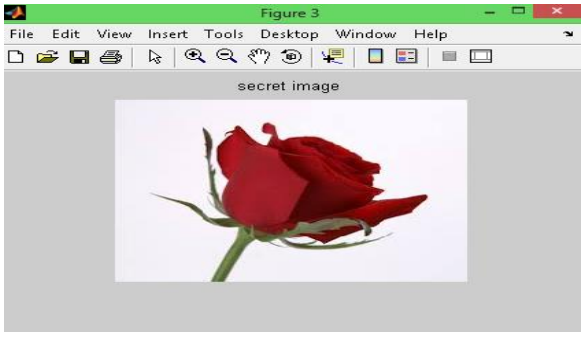
1. The image is converted into Ycbcr color space.



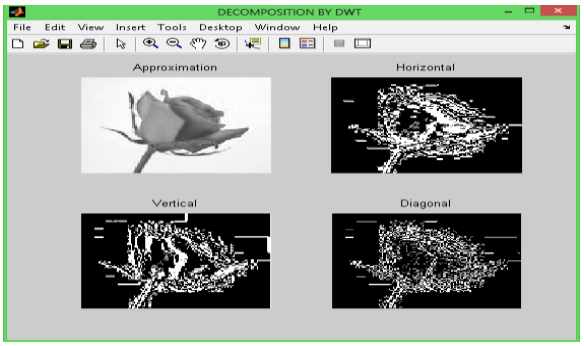
2. Skin detection and Edge detection:



3. Secret Image which is hide behind the Cover image:



4. Decomposition by DWT:

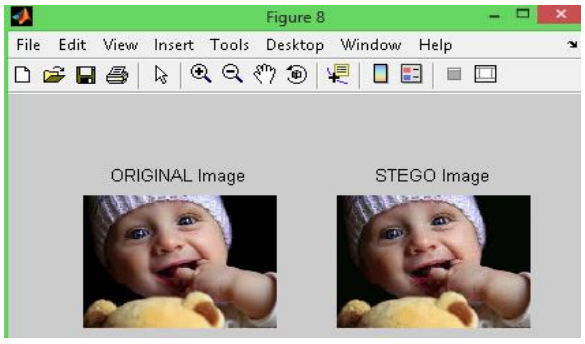


5. Compressed secret image

6. Original image and stego image

Image-1: Original image and stego image

As above results are evaluated for one image and the experiment is performed at more than 4 images as



mage-2:Original image and stego image

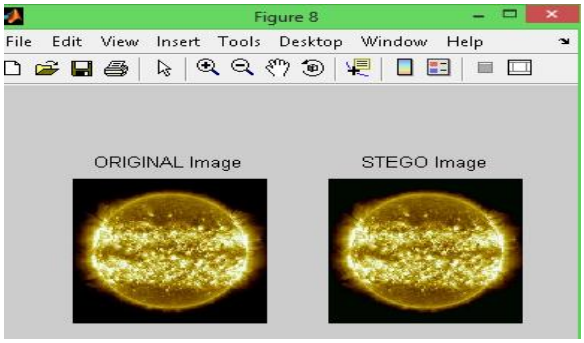


Image-3: Original image and stego image

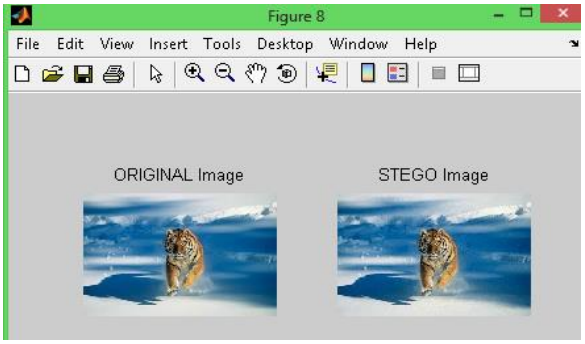


Image- 4: Original image and stego image

Cover Images	Secret Images	PSNR value by LSB method	PSNR value by Proposed algo	Time Taken(sec)
Baby.jpg	Flowr.jpg	30	33.667	2.953
Lion.jpg	Rose.jpg	29	34.083	4.187
moon.jpg	Child.jpg	32	37.864	3.108
lion.jpg	Teddy.jpg	30	34.083	3.046
baby.jpg	Moon.jpg	37	43.667	3.078

Table no.1 Comparisons of stego image quality

The above table give information about the time taken by the DWT technique . The above table shows the cover image, Secret image, PSNR value by proposed method and this PSNR value is compared with PSNR value evaluated by the LSB method

CONCLUSION

As steganography is concerned with security purposes and it is consider as a fascinating scientific area . In this paper Biometric Steganography and non-biometric stegnography is presented. The skin area and the edge pixels are evaluated and secret data which is encrypted with RSA algorithm is embedded into specific area .As data is embedded in certain region rather than whole image so security as well as quality of stego image is enhanced.

REFERENCES

[1] AbbasCheddad, JoanCondell, KevinCurran and Paul Mc Kevitt, "Securing Information Content, using New Encryption Method and Steganography".

[2] Amritha.G,MeethuVarkey, "Biometric Steganographic Technique Using DWT and Encryption" in International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, March 2013.

[3] Abdulaziz, N.K. and Pang, K.K., (2000) "Robust Data Hiding for Images", WCC - ICCT 2000, Vol. 1, 21-25, Aug. 2000, pp. 380 – 383.

[4] Amin,M.M., Salleh, M., Ibrahim, S., et al. (2003) "Information Hiding Using Steganography", 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, January 14-15, 2003, pp. 21-25.

[5] Canny,J.,(1986) "A Computational Approach to Edge Detection",, IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 8, 1986, pp.679-714.

[6] Petitcolas, F.A.P., (2000) "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas.

[7] Popa, R.,(1998) "An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Science and Software Engineering, May 25, 1998.

[8] Cachin,C.(1998),"An Information-Theoretic,Model for Steganography", in proceeding, 2nd Information Hiding Workshop, vol. 1525, 1998, pp. 306-318.

[9] AbbasCheddad, JoanCondell, KeviCurran, and Paul Mc Kevitt,(2000), "skin tone based, steganography in video files exploiting the YCbCr color space".

[10] RajanSJamgekar, Geeta ShantanuJoshi(2013)," File Encryption and Decryption,Using Secure RSA", Vol-1, Issue-4.