International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 55-58
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

A SECURE COLOR IMAGE STEGANOGRAPHY USING RSA ALGORITHM

Ganavi M
Asst .Prof Department of CS&E
JNNCE, Shivamogga, Karnataka, India

Namitha H
Department of CS&E
JNNCE, Shivamogga, Karnataka, India

Abstract— **Steganography is the science and art of invisible communication. The secret data can be disguised in content, for example, image, audio, or video. This Method gives a novel image steganography technique to transmit secret image and key in cover image utilizing Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). There is no visual contrast between the stego image and the cover image. The extracted image is closer to the secret image. This is demonstrated by the high PSNR (Peak Signal to Noise Ratio), value for both stego and recovered secret image. The outcomes are contrasted and the consequences of similar techniques and it is found that this procedure is basic and gives better PSNR values over others.**

Keywords—**IWT, DWT, PSNR, RSA**

I. INTRODUCTION

As of late, in the field of the scholarly world and industry there was a quick improvement in data covering up and in data security and it has likewise increased critical advancement. There are two branches one is digital watermarking and another is steganography. digital watermarking is utilized as a part of electronic items for duplicate compose assurance, though concealing the secret data in a spread normally called as covering media is called steganography[1]. Utilizing steganography aside from the recipient no one will comprehend what the secret message and hence can't recover it.The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. There are few requirements of steganography they are

Security: Security refers that any information or messages hidden must not be recognized. The system which has very high security is mostly preferred. The closer the stego-image is the higher the security. This is measured using Peak Signal to Noise Ratio (PSNR).

$$PSNR= 10 \log L^2/\sqrt{MSE}\ dB$$

Where, L= maximum value, MSE= Mean Square Error

$$MSE= 1/N \sum^{N}_{i=1} \left| X_i-X_i^{'} \right|$$

Where, X=original value, X'= stego value and N= number of samples.

Capacity: The maximum amount of the digital space that can be used to hide the information is referred as the capacity of the steganographic system.

Transparency: The transparency will refer the measure of lack of visual changes between carrier image and the stego-image. If changes are lower than transparency will be better.

Robustness: Ability of receiver will refer to robustness of receiver to identify the message as well as the resistance for conventional attacks like compressing, adding noise, scaling etc..

Invisibility: Not being able for humans to identify distortion in the stego-object.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

A. Discrete Wavelet Transform-

The DWT has been presented as an exceedingly productive and adaptable strategy for sub band disintegration of science[2] the 2D-DWTis these days build up as a key operation in picture handling. It is multi-dimension examination rots pictures into wavelet co-efficient and scaling limit.DWT is utilized by advanced pictures. Numerous DWTs are accessible. Contingent upon the application fitting one ought to be utilized. The least complex is haar transform. For shrouding instant information number wavelet change may be utilized. At the point where DWT is connected to the picture it is decayed into 4 sub-groups: LL, HL, LH and HH. LL part has the at most noteworthy components. Therefore whether the data is covered up in LL part the stego-image may withstand pressure or different controls. In any case, now and again mutilation might be delivered in stego-image and after that another sub-groups may be utilized. This is as shown in fig 1[4].

Image contains of pixels that will be organized in 2 dimensional grids, each pixel tells to what can as well be called image intensity. In spatial space nearby pixel qualities are exceptionally belonging and henceforth more.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 55-58
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

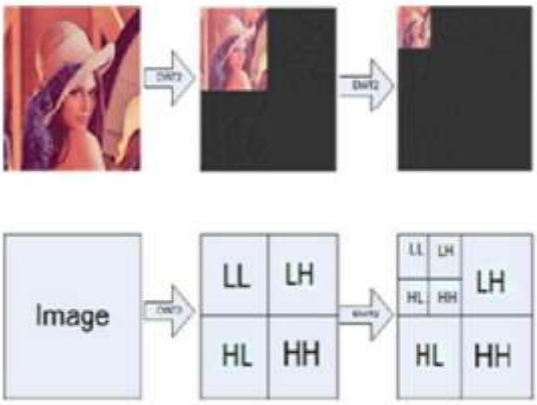


Fig 1:2 level 2D DWT

B. Integer wavelet Transform-

These wavelets change charts numbers to whole numbers. If there should be an occurrence of DWT, if the information comprises of whole numbers (as on account of images), the subsequent yield no more comprises of numbers [3]. Consequently the ideal recreation of the first image gets to be troublesome. Notwithstanding, with the presentation of Wavelet changes that guide whole numbers to whole numbers the yield can be totally portrayed with numbers. The LL sub-band on account of IWT gives off an impression of being a nearby duplicate with littler size of the first image while on account of DWT the subsequent LL sub-band is misshaped somewhat, as appeared in Fig.2 [5].

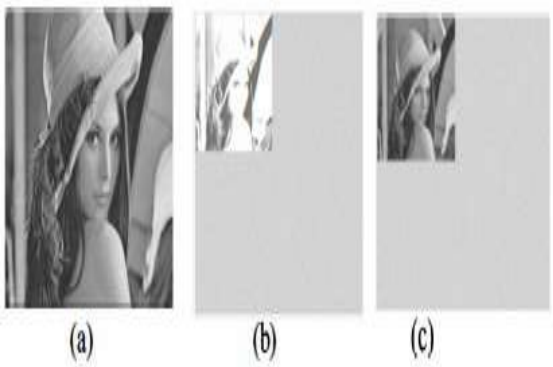


Fig 2: (a) Original image Lena. (b) One level DWT in sub band LL (c) One level IWT in sub-band LL.

B. RSA Algorithm-

RSA is the algorithm used by modern computers for encrypting and decrypting data. RSA is asymmetric cryptographic algorithm.
The algorithm is as follows
Step 1. Let ekek□1:::e1e0 be the binary representation of e.
Step 2. Set the variable C to 1.
Step 3. Repeat steps 3a and 3b for i = k; k □ 1; :::; 0:
Step 3a. Set C to the remainder of C2 when divided by n.
Step 3b. If ei = 1 then set C to the remainder of C _M when divided by n.
Step 4. Halt. Now C is the encrypted form of M.

Proposed Algorithm

(a) Key Generation

The generation can be explained using the below algorithm.

Step 1: Color image M has to be represented in YCbCr color space.

Step 2: Perform one level 2D DWT for secret image N and the Cr component of M.

Step 3: Transform grid resulted after this has of four sub-bands namely, NLL, NHL, NLH and NHH for the secret image N. For Cr component of M is MLL, MHL, MLH, MHH.

Step 4: The sub-bands or sub-images NLL and MLL are sub-divided to non-overlapping blocks BMk1 (1<=k1<nc) and BNi (1<=i<ns) of size 2*2 in which nm and nn will be the total of non-overlapping blocks that is gained from the sub-bands or sub-images MLL ,NLL.

Step 5: Each block BNi will be checked with block BMk1. These pair of the blocks that has the minimum Root Mean Square Error will be calculated. The key will be used to calculate the Bni. The IDWT is applied to obtain the Cr component.

Step 6: The obtained key will be encrypted using RSA.

(b) Key Embedding

The generated key can be embedded in the carrier image using IWT. The algorithm is as depicted.

Step 1: Obtain the integer wavelet transform of the Cr component of cover image.

Step 2: Replace the LSB planes of high frequency component of the transformed picture with the bits of the key.

Step 3: Perform the IIWT of the out coming image to obtain stego Cr component.

Step 4: Present the image that is obtained in RGB color space to get the stego-image J.

(c) Key Extraction

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 55-58
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

The algorithm for obtaining the key is as follows.

Step 1: Convert stego-image J to YCbCr color space.

Step 2: Obtain the integer wavelet transform of the Cr component of the stego image J.

Step 3: Get key from the LSB planes of the high frequency component of transformed image. Covert it back to RGB.

Step 4: Decompress and decrypt the key to get the original key.

(d) Secret image Generation

Once the key is obtained the secret image should be generated using the depicted algorithm.

Step 1: Transform stego-image J into one level 2D DWT.

Step 2: The result of the transformation is 4 sub-bands JHH JHL JLH JLL.

Step 3: Partition sub-band JLL to 2*2 non-overlapping blocks. Key will be used for obtaining the blocks that has the near approximation to original blocks in secret-image.

Step 4: The blocks generated are then arranged to gain sub-band NLL new. Assuming that NHH new, NHL new, NLH new are zero matrix of dimension same as NLL new, 2D IDWT is obtained.

Step 5: The image obtained is secret image N.

III. Experiment and Result

The project is carried out by considering two sets of cover images and secret images. The carrier images used are the Lena, Peppers and Madrill. The secret images used are Earth, Football, and Moon. This is shown in fig 3 and fig 4. The size of the cover images taken is 256*256 and the size of the secret images is 128*128. The size of the carrier image is more than the size of the secret image. The stego-image is as shown in fig 5.


Fig 3: Cover images


Fig 4: Secret images

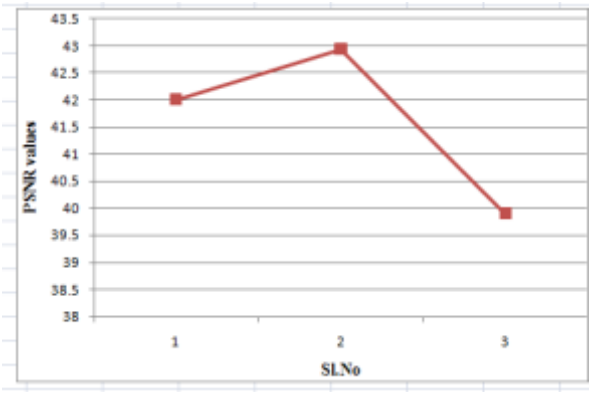


Fig 5: Stego-images

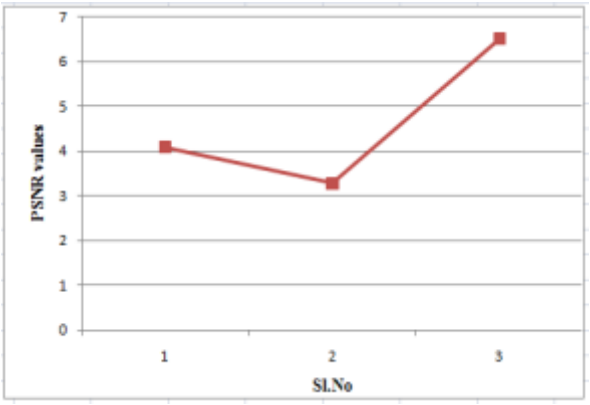
International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 10, ISSN No. 2455-2143, Pages 55-58
Published Online August - September 2016 in IJEAST (http://www.ijeast.com)

Table 1: Experiment Results

Cover image	Secret image	PSNR	MSE
Lena.jpg	Earth.jpg	45.01	4.09
Mandrill.jpg	Football.jpg	45.94	3.29
Peppers.jpg	Moon.jpg	44.9	6.50



(a)



(b)

Fig. 5: Comparison of metrics with respect to different images (a) PSNR (b) MSE

IV. CONCLUSION

Invisibility and security ARE the primary factors of any steganography system. In this method it is observed that the secret image itself is not embedded in the carrier image but a key is generated, using carrier image and secret image. By implementing this method high PSNR values can be obtained compared to the other existing methods. More the PSNR value the more secure the system is. As the key and the secret image are hidden in the least significant bit planes it becomes difficult for any observer to find the existence of the message. Instead of considering the least significant bit planes, the middle bit planes can be used to hide the key. This gives more security to the system. Encryption methods like Blowfish and RC6 can be made use to encrypt the key, which will further increase the security and also the encryption key should to be embedded in the cover image.

V. REFERENCES

[1] Katzenbeisser, S. and Petitcolas, F.A.P., (2000) Information Hiding Techniques for Steganography
and Digital Watermarking. Artech House, Inc., Boston, London.

[2] M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa, (2004) "Using Integer Wavelet Transforms inColored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems,Volume 4, pp. 75-85.

[3] Guorong Xuan et. al, (2002) "Distortionless Data Hiding Based on Integer Wavelet Transform",
Electronics Lelters, Vol. 38, No. 25, pp. 1646-1648.

[4] Mandal, J.K., Sengupta, M., (2010) "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC).", Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[5] Hemalatha S, Priya R. Kamath*:* A secure color image steganography in transform domain *by*, Manipal University, Manipal, Karnataka, India 2013.