iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8046

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Secure and Authentic Dual Steganography through HLSB with Blowfish Algorithm and DWT Technique

Er. Babita[1], Er. Gurjeet Kaur[2]
[1]*M. Tech Scholar, Deptt. of CSE, Sant Baba Bhag Singh University Jalandhar, India*
[2]*Assistant Professor, Deptt. of CSE, Sant Baba Bhag Singh University Jalandhar, India*

Abstract: ***Steganography and cryptography are two terms which are used for sending private information in a secret form. This paper represent a method for privacy so that information is not only in encrypted form but also not visible to intruder that is generated by combination of both techniques steganography and cryptography. There are many method used for both techniques. For cryptography AES, RSA, DES etc. algorithms are used and for steganography LSB, DWT, DCT etc. are used. But in this paper two methods are used. First technique Hash-LSB with blowfish algorithm is used and then DWT algorithm is used for double security. First of all, encrypted the secret message through BLOWFISH algorithm and embedded that encrypted message with cover image with using Hash- LSB. After that the stego image to be embedded into another cover image with using DWT for double security. All system is based on PSNR, MSE and BER parameters. Proposed method offered better results than existing methods.***

Keyword: ***Cryptography, Steganography, Encryption, Intruder***

I. INTRODUCTION

In today's era of technology, security of our personal information is a big issue such that the data or information cannot be misused for an illegal purpose through hackers. There are two processes exist that are used for sending information in secret way. To protect data from malicious attacks, Cryptography and Steganography are used [10]. Both are well-known and widely used techniques which used for information security for confidentiality of data exchange.

Cryptography The word cryptography originated from 2 Greek words "Kryptos" which means secret writing [11]. Cryptography is an ancient art of protecting a private data from unauthorized users and also used for user authenticity [23]. Cryptography is a method of storing and transmitting. In cryptography convert the plaintext into cipher text (a process called encryption), then back again (known as decryption).There are various types of Cryptography: symmetric key cryptography, which makes use of a single key by both sender and receiver, and asymmetric or public key cryptography systems in which both sender and receiver uses two keys: private key that is known to self only and public key that is made public and is known to everyone. The message is encrypted using the intended receiver's public key and sent across the network and the intended receiver decrypts the message using their own private key. A lot of data encryption algorithms are available and proposed by researchers with variations. Each of the algorithms has their pros and cons. Another technique that can help in this situation is Steganography which ensure that the existence of data remains hidden. It hides the message so there is no knowledge of the existence of the hidden message in the first place. It is defined as the art and science of sending hidden messages in such a way that no one else, apart from the intended recipient knows the message's existence. The message's text can be hidden into another media type file such as image, text, sound or video. The various types of data in steganography can be audio, video, text and images etc. Both of the techniques will fail, if used without each other. Cryptography fails when the intruder on the network is able to decrypt the message and Steganography fails when the intruder detects that something secret message is present in another media file as a cover. So a combined approach of both the techniques is essential for ensuring a secure data transmission in such an unsafe and open network environment. In this paper we hide secret encoded data in digital image. In which cryptography covert message in encrypted form so that it is not possible for unauthorized party to understand it. In this paper we are going to develop a new system by using both processes steganography and cryptography. New system developed for better security. In this paper blowfish algorithm is used for encryption the data.

II. LITERATURE REVIEW

Vijay Kumar and Dinesh Kumar *el al* (2010) presented [8] a digital image steganography technique in which DCT was combined with DWT. The experimentation was done using different attacks. The results show that PSNR value increase as compare to previous system. The proposed method first extracts the DCT coefficients of secret image by using DCT technique. After that,

image features are extracted from cover image and from DCT coefficients by applying DWT technique on both separately. This paper showed high robustness against many image processing attacks.

Atallah M *el al* (2012) introduce [12] A New Method in Image Steganography with Improved Image Quality. In which Steganography is word taken from the two Greek words as "steganos" and "graphie" which mean "concealed" and "writing" respectively. Jointly it referred as concealed (hidden or covered) the message. Various techniques are used for the purpose of image steganography. In this paper the technique used by the author works by recognizing the similar bits between message and image. The comparison is done by using the LSB benchmark technique.

Md. Khalid, Iman Rahmani and kamiya arora, Naina Pal el al (2014) introduced [1] the digitally signature method which implements the authentication, integrity and non- repudiation and apply the AES algorithm on digitally signed message to form the encrypted message to implements the confidentiality and partial security. Embed that message into the image with using the LSB to produce the stego image.

Kamal and Lovnis Bansal *el al* (2014) used [6] the combination of both DCT and LSB method using 32*32 DCT segmentation plan. In which RSA algorithm used for implement the asymmetric cryptography for better integrity and for no loss of data and in which neural networks are used for extract the data bits with least affecting the original patterns of image.

Nikita Sharma, Meha Khera *el al* (2015) introduce [9] the Hash –LSB with RSA algorithm and DWT techniques in combined form, in which chances of security in terms of lesser detectability, and lesser distortion in an image would be more because here the message is encrypted first before embedding into an image.

Prof Ms. Ashwini B. Akkawar, Prof. Komal B. Bijwe et al (2016) gave a review [10] which compare the techniques for dual steganography along with their strength and weaknesses. Firstly, DES Encryption is used for Image Steganography and then using the LSB technique and AES algorithm for dual security. Finally, steganography inside steganography techniques used for overcome all the drawbacks of previous once and give rise to improved version of dual steganography. They are using the AES and DES algorithm for encryption but there are more algorithm available for security those gave the better performance as compare to these algorithm.

III. PROBLEM STATEMENT

Combining the HLSB Steganography algorithm along with BLOWFISH algorithm which encrypted the secret data and using DWT technique with using new Second cover image for double security. Also check the image quality which is measured in terms of PSNR. Our objective is divide the cover image in RGB planes and hides the encrypted data in RGB planes by applying HLSB technique and using DWT technique on it with using another cover image for double security. Finally compare the result with base paper on the basis of PSNR, MSE and BER.

IV. TECHNIQUES USE

In this paper two techniques are proposed .Both of these techniques are from different domains. These techniques are:

Hash-LSB with BLOWFISH Algorithm

Discrete wavelet Transform (DWT) Technique

A. Hash-LSB (Least Significant Bit) technique

In hash- LSB technique, the least significant bit position where the secret data is to hidden is determined by using the hash function. It finds the location of least significant bit of each RGB pixel of image, and then secret message bit are embedded in the RGB pixel of image independently. Firstly the cover image is broken or fragmented into RGB format. Then Hash-LSB will use the value from the hash function to integrate or hide data into the LSB of RGB pixel. In the technique, the secret message is converted into binary form as binary bits, each 8 bits at a time are included in the least significant values of RGB pixel image covering about 3, 3 and 2 bits respectively. Under this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel and 2 LSB bits are embedded in blue pixel. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green color. Therefore choose the 2 bits of blue color. Thus the quality of the image will be not sacrificed.

B. Hash function

The hash function deals with the LSB position and the pixel position of each image, and also with the number of LSB bits. Hash value takes a variable size input and returns a fixed-size digital output string. Hash function is also used to detect duplicate folder in large files. Hash function given by: i= j % k Where, i is the position of LSB bit within the image pixels, j represents the position of each hidden image pixel and k is number of bits of LSB.

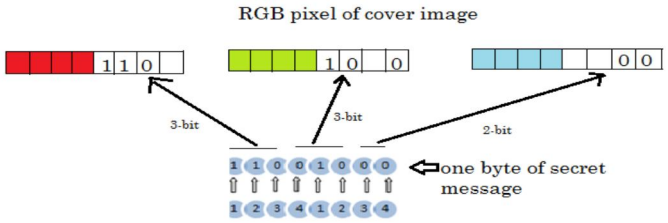


Fig.1 Hash-LSB Process

C. Blowfish Algorithm

In proposed system the encryption of the secret Information is done by using BLOWFISH algorithm. Blowfish has 16 rounds.

1) The input is a 64-bit data element, x.
2) Divide x into two 32-bit halves: xL, xR.
3) Then, for i = 1 to 16:
4) xL = xL XOR Pi
5) xR = F(xL) XOR xR
6) Swap xL and xR
7) After the sixteenth round, swap xL and xR again to undo the last swap.
8) Finally, recomine xL and xR to get the ciphertext

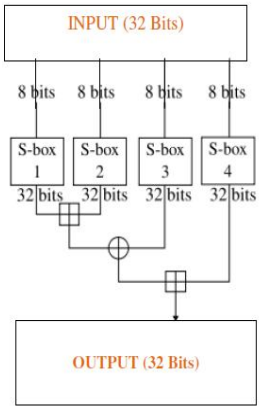


Fig.2 Graphical Representation

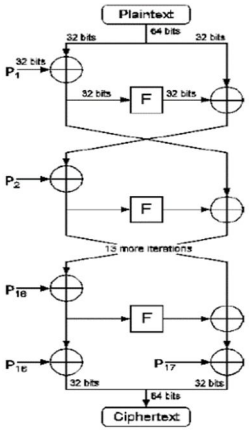


Fig.3 Graphical representation of F

D. DWT Technique

Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis**.** The DWT technique represents an image as a sum of wavelet functions, which is known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are sampled. The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. When DWT is applied on an image, it divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. We will take a cover image as a cover object and another small image take as secret message. In embedding process, first we convert cover image in wavelet domain. After the conversion we manipulate high frequency component to keep secret image data.

V. PROPOSED WORK

The proposed work is to combine these techniques (hash-LSB with BLOWFISH algorithm and DWT technique) to make message transmission between two parties more secure. In this work we are first encrypting the secret message using BLOWFISH algorithm. By applying BLOWFISH algorithm we obtain cryptography because it encrypts the message and convert it into unreadable form so that if unfortunately the message is revealed the intruder does not get any idea about the actual message. Then by applying Hash-

LSB we are embedding the message into the cover image and obtain a stego image. Then we are using DWT technique to embed this stego image into another cover image to obtain a final secure stego image.

A. Steps followed in proposed work

1) Embedded Process

Step 1: Take a Cover Image

Step 2: Secret message is first converted into encrypted form using BLOWFISH Algorithm.

Step 3: Then the encrypted message is converted into binary bits.

Step 4: 8 bits at a time are embedded in LSB of RGB pixel values of cover image in the order of 3, 3, and 2 respectively.

Step 5: 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB.

Step 6: Their position is obtained by the formula:

$$k = p \% n$$

k is the LSB bits position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB.

Step 7: After embedding the data in cover image, a stego image is obtained.

Step8: Then we are applying DWT technique to embed this stego image into another cover image to obtain a secure stego image.

Step 9: At last press enter for recover the secret message.

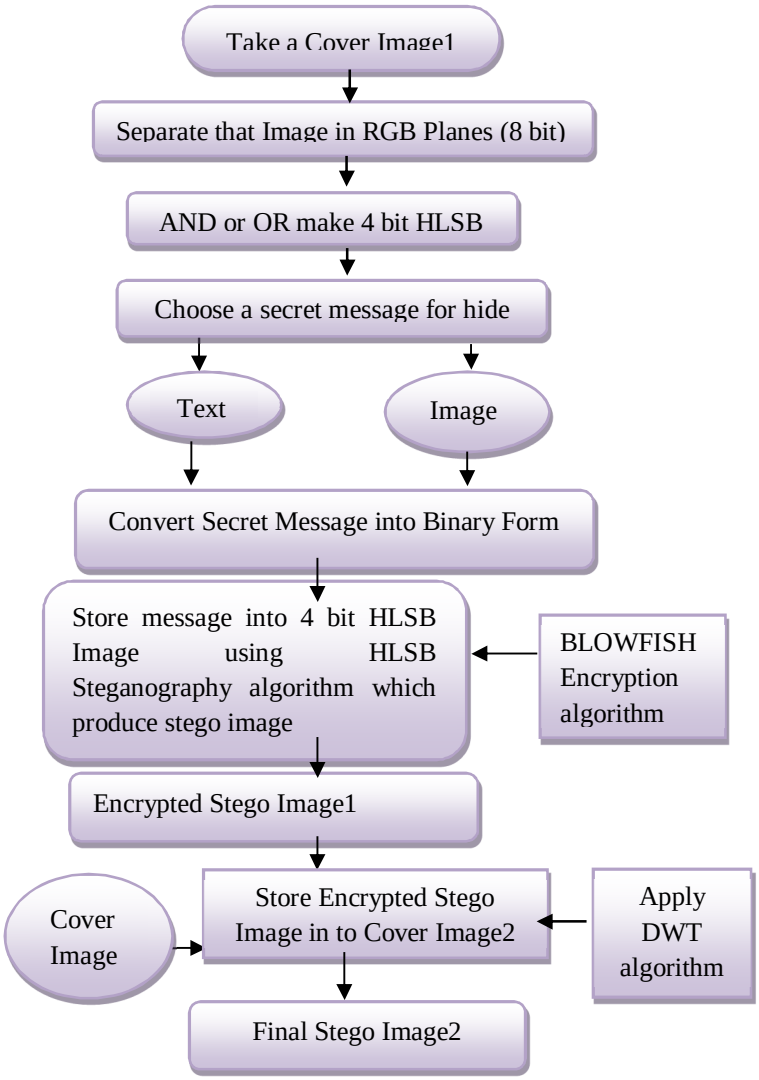


Fig 4. Flow Chart Of Proposed System

B. Extraction Process

Step 1: Press enter for extraction process.
Step 2: Apply idwt extraction process to extract the stego image1 from the "secure stego image".
Step 3: Get secret data or image from the R, G and B pixels of the stego image1.
Step 4: After that recover data or recover image is decode by using blowfish algorithm.

VI. PERFORMANCE ANALYSIS AND RESULTS

This work is implemented in MATLAB with an objective of better security and lesser detectability. It is capable of hiding an encrypted text message (by BLOWFISH Algorithm) within an image using Hash-LSB technique. Then the stego image is successfully hidden behind another cover image using DWT technique.

Firstly taken a cover image of Flower.JPG and then chooses a option for secret data which may be text or image that is encrypted with blowfish algorithm. After that encrypted message is hide in in cover image. Then the image of Flower.JPG with message encrypted within it is hidden behind another cover image of Mandrill.jpg which results in secure stego image. Following results of the figures shows the above process in more details.

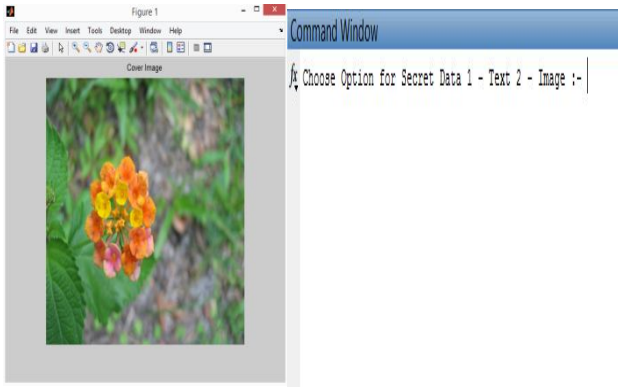


Fig.5 Original Image Fig.6 Choose option for secret data

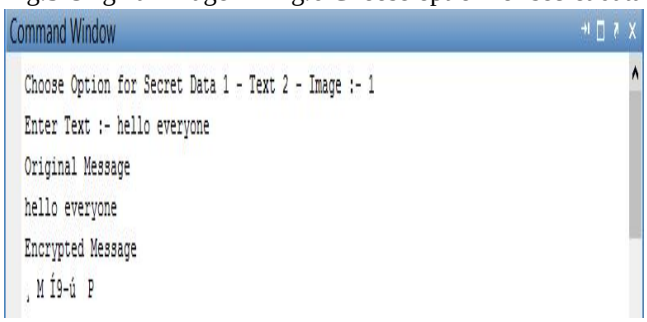


Fig.7 Encrypted form of text

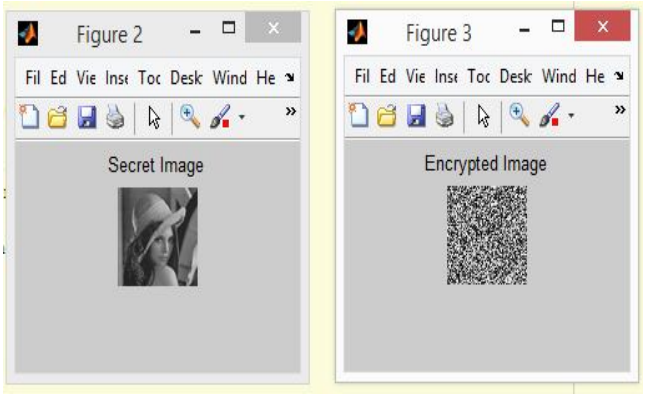


Fig.8 Secret image and its encrypted form

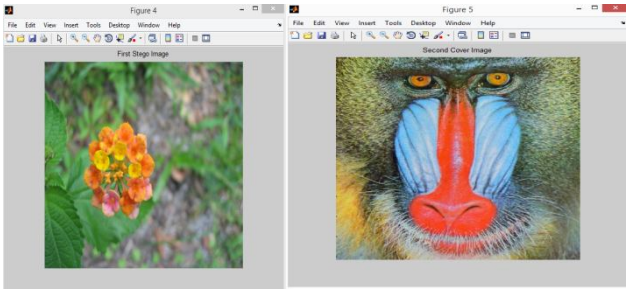
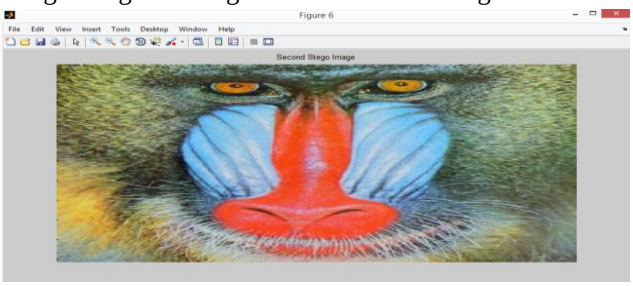


Fig.9 First Stego Image Fig.10 Second Cover Image With hidden message



After obtaining the final steganography image using DWT technique we can decode that secure stego image. Following images shows the decoding process.

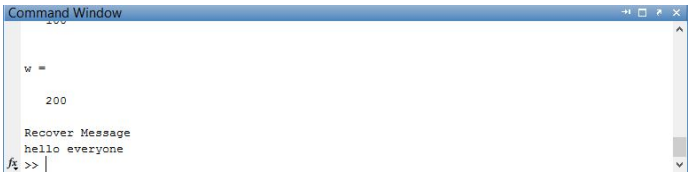


Fig.12 recover secret message

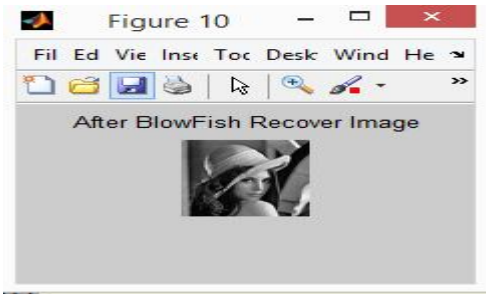


Fig.13 Recover secret Image

The quality of results obtained are depicted by

A. PSNR (Peak Signal to Noise Ratio)

The Peak Signal to Noise Ratio (PSNR) measures the estimates of the quality of stego image compared with an original image and is a standard way to measure image reliability or conformity.

B. MSE (Mean Square Error

The mean of pixel values of the image and by averaging the sum of squares of the error between two images.

PSNR = 10 log (peak) 2/MSE

And

MSE = 1/MN ((S-C) 2)

Where MSE is mean-square-error,

Peak = 255,

M and N are the dimensions of the image,S is the resultant stego-image, and C is the cover image.

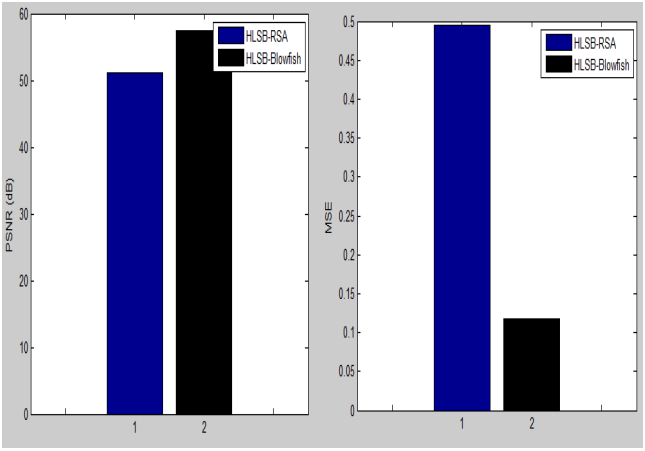


Fig.14 PSNR value Fig.15 MSE Value

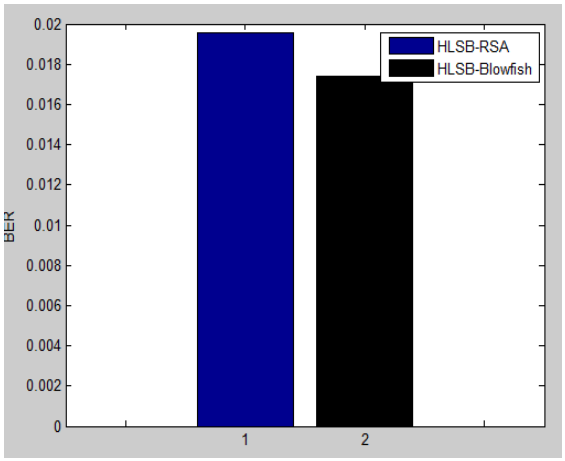


Fig.16 BER Value

Technique used	PSNR Value	MSE Value
Hash-LSB with RSA algorithm and DWT technique	51.18	0.4955
Hash-LSB with BLOWFISH algorithm and DWT technique	57.41	0.1178

Table 1: Comparison of our result with RSA Algorithm

The above result shows that PSNR value obtained from our work is 57.41 which is much more than PSNR obtained from Hash-LSB with RSA algorithm technique and the MSE obtained from our work is much less than the MSE value obtained from Hah-LSB with RSA technique. Thus we obtained larger PSNR value and lesser MSE value.

VII. CONCLUSION

When Hash –LSB with BLOWFISH and DWT techniques are combined, chances of security in terms of lesser detectability, and lesser distortion in an image would be more because here the message is encrypted first before embedding into an image. When the stego image is achieved it will be again embedded into another cover image so that if in case if intruder is successful in obtaining the image within the cover image, he/she cannot get any idea that there is the message embedded in the image. If at worst case the

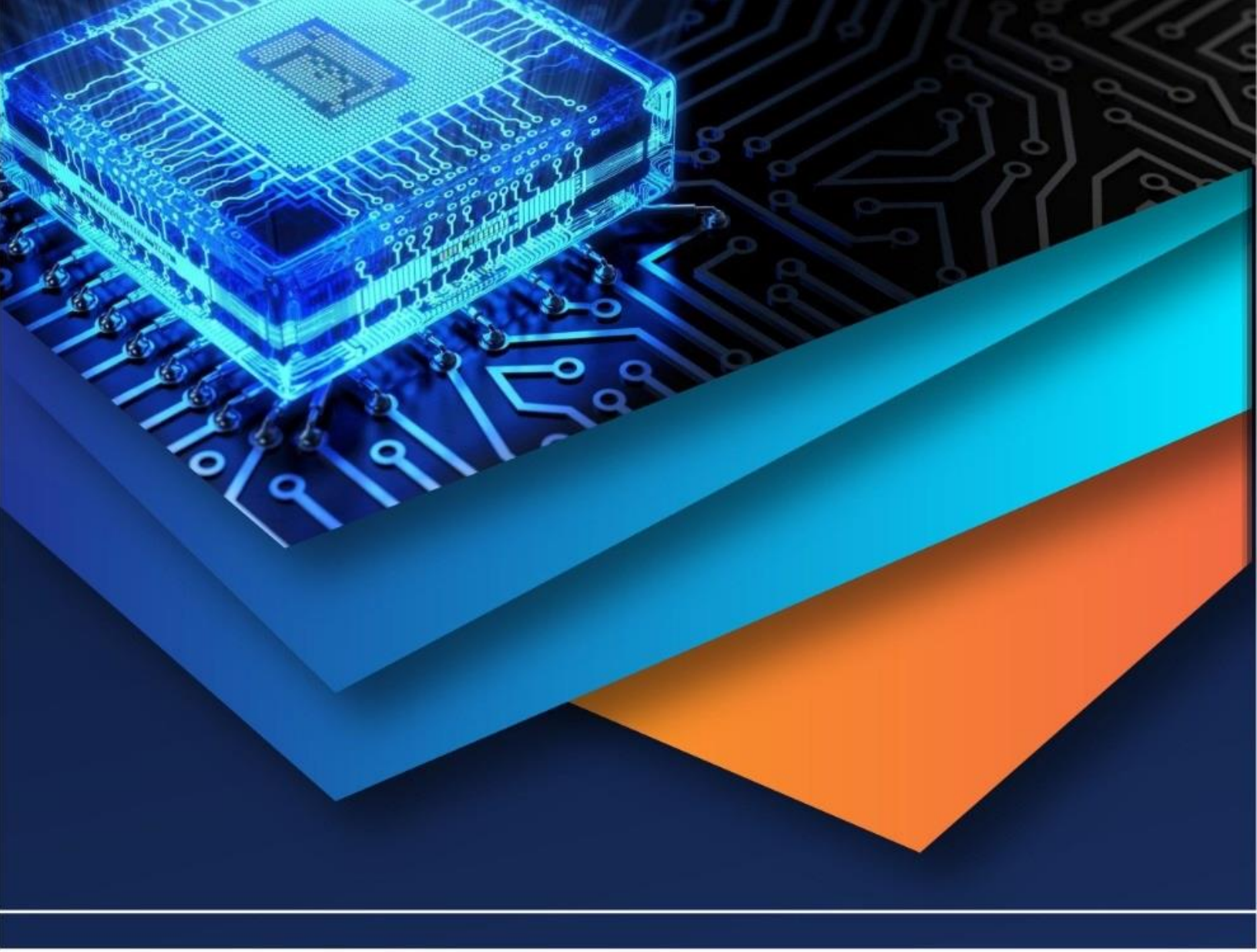
intruder is successful in obtaining the message in the image he/she cannot revealed the message because it is in encrypted form. We are successful in achieving the above mentioned objectives. We are successful in hiding an encrypted message into an image using Hash-LSB Technique and that stego image is successfully hidden behind another cover image using DWT Technique which results in more secure stego image. One more benefit of this system is hide the secret data may be in text or image form. This work results better PSNR value (57.41) than the PSNR value(51.18) obtained from LSB technique and lesser MSE value(0.1178) than the MSE value(0.49) obtained from Hash- LSB technique with RSA Algorithm. So this work gives better results in terms of security, confidentiality and detectability. This work is successfully implemented in MATLAB.

VIII. ACKNOWLEDGMENTS

I express my sincere and deep gratitude to my guide Mrs Gurjeet Kaur, Assistant Professor, Department of Computer Science and engineering, Sant Baba Bhag Singh University for the invaluable guidance, support and encouragement. She provided me all resource and guidance for this work.

REFERENCES

[1] Md. Khalid Imam Rahmani and Kamiya Arora, Naina Pal, "A Crypto-Steganography: A Survey in" in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014
[2] Jitha Raj.T, E.T Sivadasan, "Secure Transmission of Data by Splitting Image in" in IEEE, Dec. 16-19, 2015.
[3] Dipanwita Debnath, Suman Deb, Nirmalya Kar, "An Advanced Image Encryption Standard Providing Dual Security: encryption using Hill Cipher & RGB image steganography" in IEEE International Conference on Computational Intelligence & Networks, 2015
[4] Pooja Rani , Apoorva Arora, "Image Security System using Encryption and Steganography" in IJIRSET International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015.
[5] S.M. Masud Karim et. Al, "A New Approch for LSB based image steganography using secret key"in proceeding of 14th international conference on computer and information technology(ICCIT 2011) 22-24 December,2011
[6] Kamal and Lavnesh Bansal, "Enhancement Key Of Cryptography And Steganography Using RSA And Neural Network" in IJARCET International Journal of Advanced Research in Computer Engineering & Technology Volume 3 Issue 5, May 2014
[7] P. Selvigrija and E. Ramya,"Dual Steganography for Hiding Text in Video by Linked List Method" in IEEE International Conference on Engineering and Technology (ICETECH), 20th March 2015, Coimbatore, TN, India
[8] Vijay Kumar and Dinesh Kumar, "Digital Image Steganography Based on Combination of DCT and DWT" in Springer-Verlag Berlin Heidelberg 2010, pp. 596–60
[9] Nikita Sharma, Meha Khera , "A Novel Approach to Image Steganography Using Hash-LSB and DWT Technique" International Journal of Advanced Research in Computer Science and Software Engineering 5(6), June- 2015, pp. 1448-1454, (2015
[10] Prof Ms. Ashwini B. Akkawar, Prof. Komal B. Bijwe, "Review And Comparative Study Of Dual Stegnography Techniques For Embedding Text In Cover Images" in IJSER 2016 , Volume 7, Issue 2, February-2016 ISSN 2229-551
[11] Rohit.K. Kawade#1, Pranyati.P. Shinde#2, Devendra.D. Jagtap#3, Prof.Mohsin Mulla#4, "A SECRET WATERMARK HIDING USING LSB STEGANOGRAPHY AND BLOWFISH ALGORITHM" in PISER 2015, Vol.03, ISSN 2347-6680 (E)
[12] Atallah M (2012), "A New Method in Image Steganography with Improved Image Quality "Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 391
[13] Jasleen Kour(2014), "Steganography Techniques –A Review Paper" International Journal of Emerging Research in Management &Technology ,Volume-3, Issue-5, pp 132-135



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY