ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Dual Steganography Technique Using Status LSB and DWT Algorithms

Manisha[#1], Deepkiran Munjal[*2]

M Tech Scholar, Dept. of Computer Science & Engineering, BSAITM, M.D.U. Rohtak, Faridabad, India[#1]

Assistant Professor, Dept. of Computer Science & Engineering, BSAITM, M.D.U. Rohtak, Faridabad, India[*2]

ABTRACT: There has been an increasing demand for information security and secure communication with continuous growth of internet users. Out of various available security mechanisms the most widely used security mechanism is Dual Steganography. Dual Steganography combines two security mechanisms steganography and cryptography both together. This mechanism has advantages of providing high security, low time complexity but this mechanism does not enhance capacity, robustness, and image quality. In this paper we have used a new version of Dual Steganography using status Least Significant Bit (LSB) algorithm and 2-D Haar-Discrete Wavelet Transform (DWT) algorithm both together. This new mechanism has advantages of both algorithms status Least Significant Bit (LSB) and 2-D Haar-Discrete Wavelet Transform (DWT). The main objective of this new security mechanism is to achieve high security, payload capacity, high Peak Signal to Noise Ratio (PSNR) value, low Mean Square Error (MSE) value, good imperceptibility and robustness.

KEYWORDS: Steganography; Cryptography; Dual steganography; DWT; LSB; PSNR; MSE.

I. INTRODUCTION

Today, in this new era of internet Information Security is becoming a big problem for the world due to the fast growth of internet users day by day. If an internet user wanted to share his personal information with other internet user by using the social applications, then hackers can attacked on these social applications and they can hack all the personal information about the internet user. Therefore to protect all the personal information from an unauthorized person we need security mechanisms. “Steganography” is a Greek word which means “hiding writing”. Steganography word is the combination of two parts: Steganos which means “secret” and Graphic which means “writing. Steganography is a security mechanism of hiding sensitive information among the bits of a cover file such as an image, text, an audio file and video file in such a way that only sender and receiver know about the hidden message inside the cover file. Cryptography comes from a Greek word meaning hidden or secret writing for secure Communication in the presence of an unauthorized person. Cryptography includes encryption and decryption process of a message. Cryptography is the art of protecting sensitive information by encrypting it into an unreadable format called cipher text .The person who has a secret key can decrypt the message in to Plain text. In cryptography the message is converted into encrypted form with the help of encryption key which is known to sender and receiver only. However, the transmission of encrypted message is not safe because the encrypted message may easily arouse attacker‘s suspicion and may be intercepted or attacked easily.

Dual steganography is the security mechanism in which steganography and cryptography are used together. In dual steganography secret message to be transmitted is first encrypted using encryption algorithm. Then the encrypted message (cipher text) is hidden into a cover file using steganographic technique. The cover file is then sent to the receiver. Even if a hacker suspects the presence of data into the cover file and recovers the cipher text he will still need decryption algorithm to understand the message. So using the dual steganography is much more secure than using cryptography or steganography alone.

A new version of dual steganography is the security mechanism which uses steganography within steganography. In this secret data is embedded in a cover image using the status Least Significant Bit (LSB) embedding algorithm to generate a stego-image. Then stego-image is considered as secret data and it is again embedded in other cover image using the 2-D Haar-Discrete Wavelet Transform (DWT) embedding algorithm which creates a final stego–image. Dual steganography is the process of transmitting two or more images simultaneously in a single channel which is achieved

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

by merging the images. In order to achieve enhanced security, two images can be merged (i.e. one image is hidden in other) so that when an intruder tries to intercept the secret data, it is not knowledgeable to him. In this technique at the sender side, sender uses a secret message and two cover mediums 1 and 2. Out of which secret message and cover medium 1 are private and cover medium 2 is public.

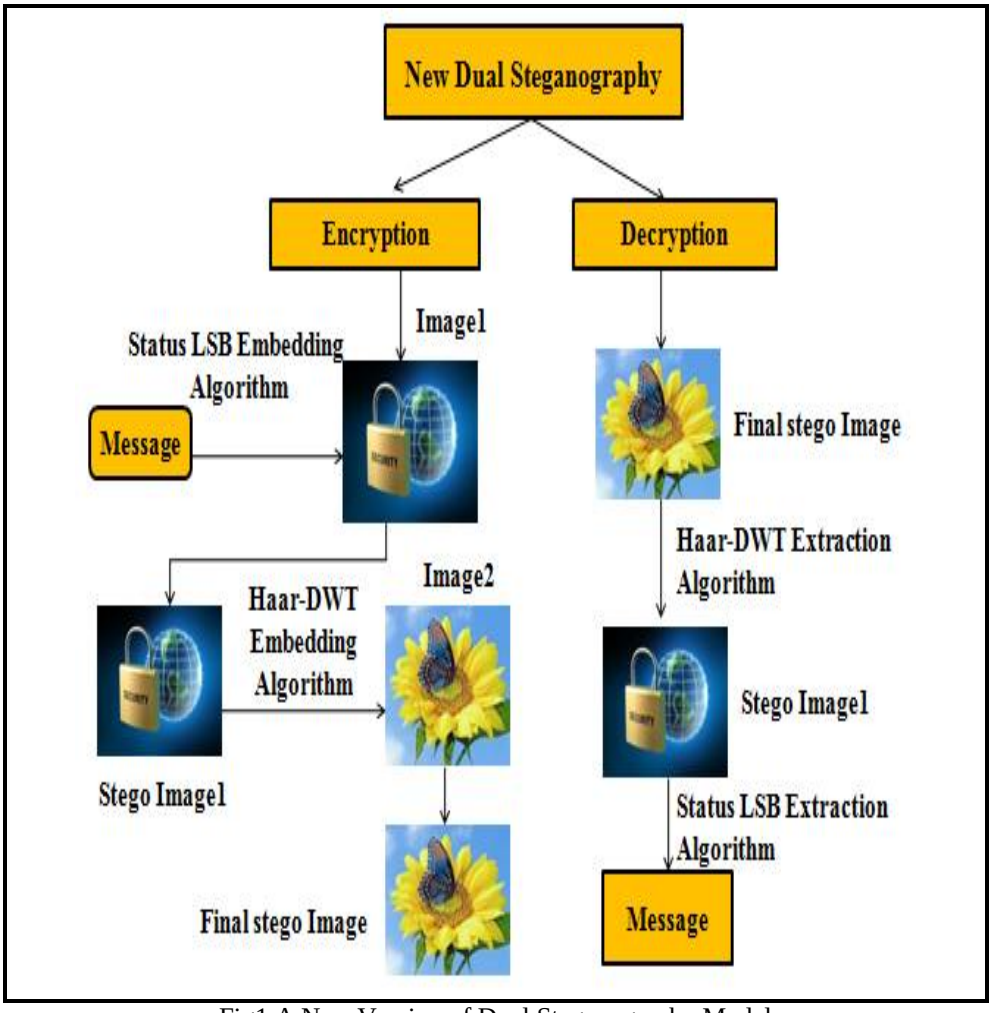

Fig1.A New Version of Dual Steganography Model

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II. COMPARISON BETWEEN DUAL STEGANOGRAPHY AND A NEW VERSION OF DUAL STEGANOGRAPHY

Table1: Comparison between Dual Steganography and A New Version of Dual Steganography.

S NO.	CONTEXT	DUAL STEGANOGRAPHY	NEW VERSION OF DUAL STEGANOGRAPHY
1.	Definition	It is the process of secret transmission data hiding in which steganography and cryptography are used together.	It is the process of secret transmission data hiding in which two steganographies are used together.
2.	Objective	The main objective of this technique is embedding data in such a way that it can increase security and decrease time complexity.	The objective of this new dual technique is embedding data in such a way that it can increase security, payload capacity, PSNR value, good imperceptibility and robustness.
3.	Working	In this technique secret data is encrypted in cipher text by using secret key (cryptographic technique) to create encrypted message. Next this encrypted message is used as a secret message and hidden in any cover file by using LSB (steganography technique) to create a stego file.	In this technique secret data is embedded in a cover image by using Status LSB embedding algorithm to make stego image. Next this stego image is used as a secret message and hidden in a cover image by using 2-D Haar- DWT algorithm to create a final stego image.
4.	Security services Offered	Confidentiality, Identification, Authentication, Data Integrity, Non-repudiation.	Confidentiality, Identification, Authentication, Data Integrity, Non-repudiation.
5.	Advantages	It has advantages of high security and low time complexity.	It has advantages of high security, payload capacity, good imperceptibility PSNR value and robustness.
6.	Disadvantages	It has disadvantages of low payload capacity, low PSNR value and robustness.	It has disadvantage of a very few high time complexity.
7.	Applications	Confidential data communication and secret data storing, Protection of data alteration and Media database system.	Confidential data communication and secret data storing, Protection of data alteration, Intelligence Agencies, Smart Identity Cards, Medical, E-Commerce and Media database system.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. LITERATURE SURVEY

Table 2: Literature Survey of Dual Steganography Using Status LSB and Haar-DWT Algorithms.

Author Name	Title Name	Proposed work	Advantages	Disadvantages
Piyush Marwaha et al.	Visual Cryptographic Steganography in Images [1].	To combine LSB steganography with visual cryptography.	Less time complexity, more secure	Lower PSNR value
S. M. Masud Karim et. al.	A New Approach for LSB Based Image Steganography using Secret Key [2].	To combine cryptography with modified LSB steganographic technique.	Higher PSNR value and good security	Higher time complexity and not robust
Gokul M et. al.	Hybrid Steganography using Visual Cryptography and LSB Encryption Method [3].	To combine Visual cryptography with LSB substitution steganographic technique.	Low time complexity	Lower PSNR value
Shailender Gupta, et al.,	Information Hiding using Least Significant Bit Steganography and Cryptography [4].	To combine cryptographic techniques RSA and Diffie Hellman with steganographic technique LSB substitution.	High security	Higher time complexity
Mohammad et. al.	Public-Key Steganography Based on Matching Method [5].	To combine cryptographic techniques Diffie Hellman with LSB steganographic technique.	High security	Higher time complexity, limited embedding capacity and not robust
R. Nivedhita et. al.,	Image Security using Steganography and Cryptographic techniques [6].	To combine Cryptographic technique DES with the steganographic technique LSB.	High security	Low embedding capacity and high time complexity.
Ramakrishna Mathe et. al.	Securing Information: Cryptography and Steganography [7].	To combine the Cryptographic technique Diffie Hellman with the steganographic technique LSB.	High security	Higher time complexity, limited embedding capacity and not robust
Md. Rashedul Islam et al.	An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography [8].	To combine AES cryptography with Status bit LSB steganographic technique.	Higher PSNR value.	Higher time complexity and is not robust.
Pye Pye Aung et. al.	A Novel Secure Combination Technique of Steganography and Cryptography [9].	To combine the AES Cryptographic technique and the DCT steganographic technique.	High security and robustness.	Higher time complexity and limited embedding capacity.
Shingote Parshuram N. et. al	Advanced Security using Cryptography and LSB Matching Steganography [10].	To combine the AES Cryptographic technique and the LSB steganographic technique.	Higher PSNR value and good security.	Limited embedding capacity, higher time complexity and not robust.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. PROPOSED WORK

In the proposed scheme steganography is used two times. The main reason behind this if steganography is used only once then an unauthorized person can hack secret data from any multimedia cover medium over the internet. But if steganography is used two times, then even if an unauthorized person can hack the secret data from any cover medium at the first time then second time secret data will be secured inside any cover medium. Thus this proposed work is used to protect the secret data at two times. To achieve the goal of high security, embedding capacity, good imperceptibility and robustness use the new version of dual steganography using the two status Least Significant Bit (LSB) algorithm and 2-D Haar-Discrete Wavelet Transform(DWT) algorithm together. Section A and B presents the data hiding and data extraction process for the proposed scheme.

A. Data Embedding Process:

In data embedding process two cover images are used i.e. cover image1 and cover image2. The secret data is embedded inside the cover image1 with the help of status Least Significant Bit (LSB) embedding algorithm to generate a stego-image1. Next this stego-image1 is considered as the secret data and it is embedded inside other cover image2 by using the 2-D Haar Discrete Wavelet Transform (DWT) embedding algorithm which generates a final stego-image.

The Proposed algorithm works as follows at the sender side:

Step1: Get the original message.
Step2: Convert it into binary form.
Step3: Get the cover image1.
Step4: Collect the MSB bits from a pixel (Red, Green, Blue color component).
Step5: Check the pixel whether it is a lighter or darker pixel.
Step6: From the MSBs, for lighter image1 if it contains two bits 1 and for the darker image1 if it contains two bits 0, select this pixel for hiding message bit. Otherwise, skip this pixel.
Step7: Convert MSB into decimal number Pn.
Step8: If Pn=0 for the darker image1 only embed the message bit into the Blue color component of the pixel.
Step9: For lighter image1 or other value of Pn:

a. Check Pn bit position of the Blue color component with message bit.
b. If it matches then change the LSB of Blue color component with 1.
c. If it does not match then change the LSB of Blue color component with 0.

Step10: Get the cover image2 of the larger size.
Step11: Apply Haar-DWT transform on the cover image2 which creates four sub bands LL, LH, HL and HH.
Step12: Convert the stego-image1 obtained from the step 9 into a binary vector.
Step13: Embed this vector into the LL sub band pixels of transformed image2 by adding random values to that pixel value.
Step14: Apply inverse Haar-DWT transform to regenerate the final stego-image.
Step15: Transmit the final stego-image.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

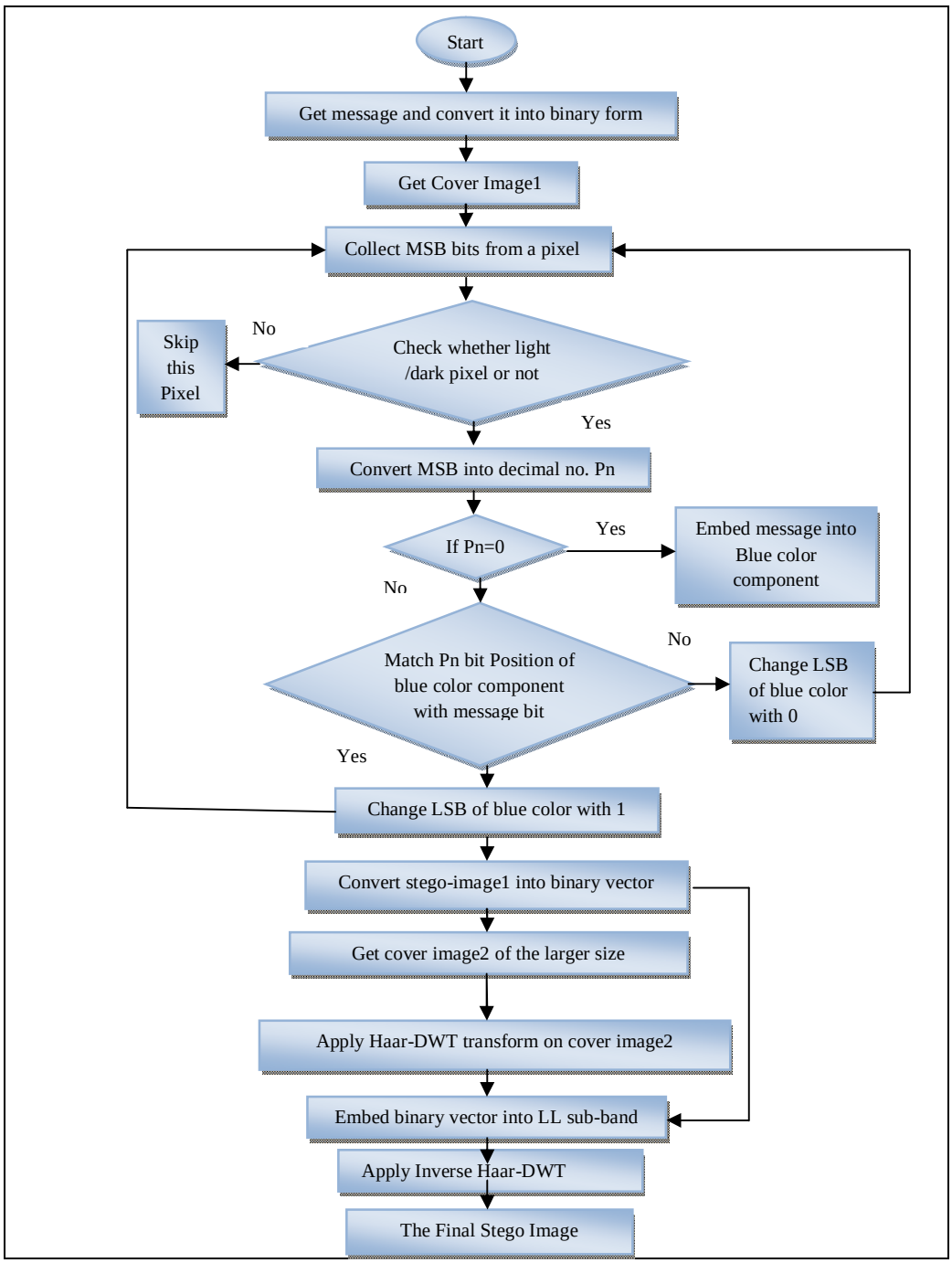

Fig2. Flowchart for data Embedding Process

B. Data Extraction Process:

In data extraction process stego-image1 is extracted from the final stego-image by using the Discrete Wavelet Transform (DWT) extraction algorithm. Next, secret data is extracted from stego-image1 by using the Least Significant Bit (LSB) extraction algorithm.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The Proposed algorithm works as follows at the receiver side:

Step1: Get the final stego-image.
Step2: Apply Haar-DWT transform on the final stego-image.
Step3: Extract the binary vector from LL sub band by comparing the pixel values i.e. if there is no match, then it contains vector bit else not.
Step4: Convert this binary vector into pixel values to form a stego-image1.
Step5: Collect the MSB bits from a pixel (Red, Green, Blue color component) from stego-image1 obtained from previous step.
Step6: Check the pixel whether it is a lighter or darker pixel.
Step7: From the MSBs, for lighter image1 if it contains two bits 1 and for the darker image1 if it contains two bits 0, select this pixel for extracting message bit. Otherwise, skip this pixel.
Step8: Convert MSB into decimal number Pn.

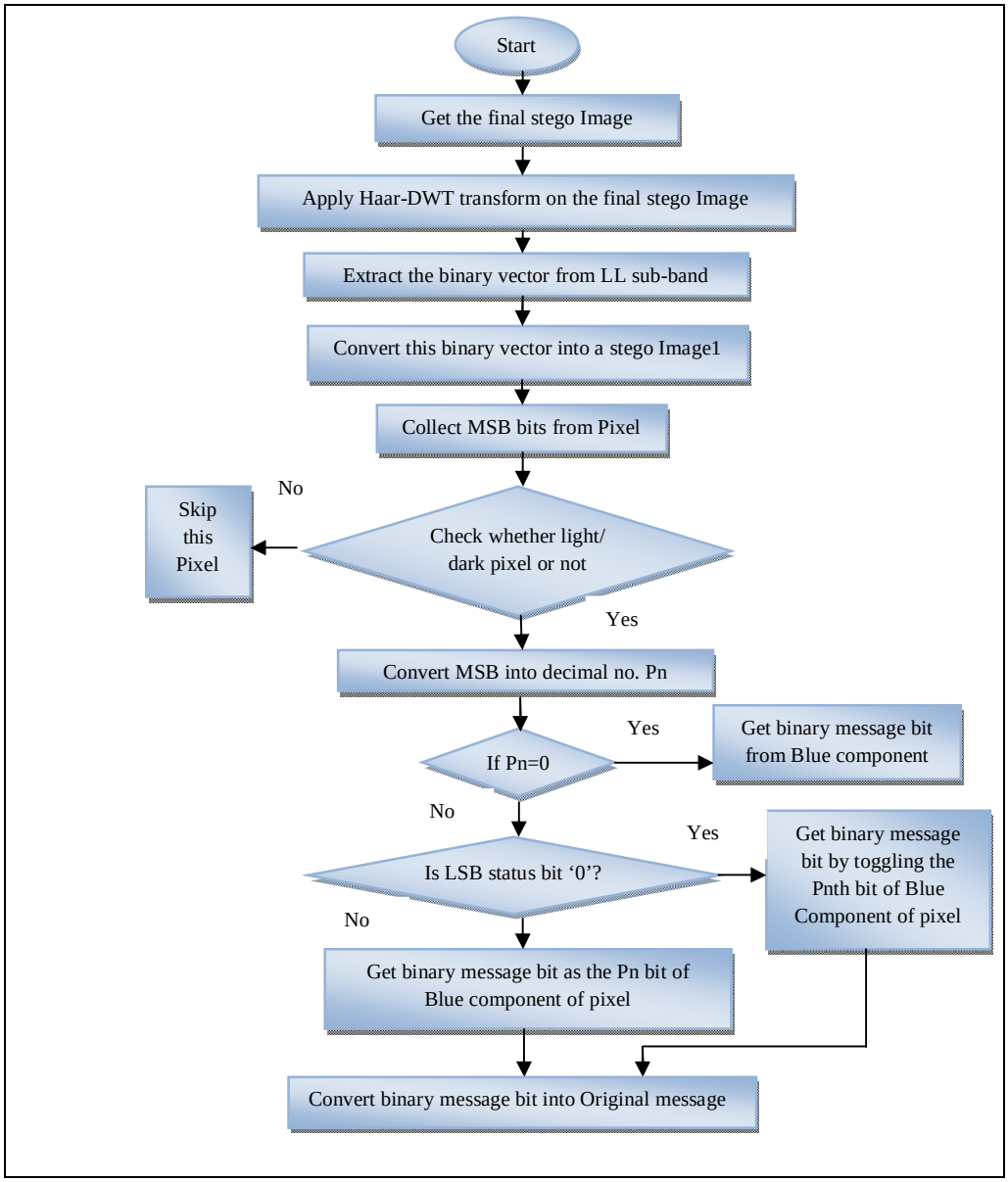

Fig3.Flowchart for Data Extraction Process

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Step9: If Pn=0 only get the binary message bit from Blue component of the pixel.
Step10: If Pn>0, check the LSB (Status bit) whether it is 0 or 1.

a. If the LSB equals to 0, then collect the binary message bit by toggling the Pn bit of the Blue component of the pixel.
b. If the LSB equals to 1, then collect the binary message bit as the Pn bit of the Blue component of the pixel.

Step11: Convert the binary message bits into its original form.

V. SIMULATION RESULTS

We performed simulation on two images of jpeg format using MATLAB 2010a, version 7.10, under the Windows 7 professional with dual Core i5 CPU and 4 GB RAM. Two cover images of different sizes and same format jpeg are used for simulation. From the simulation results, it is clear that the proposed scheme is ideal for secret data communication as it meets key requirements including highly security, high payload capacity, better perceptual Fidelity and robustness. In this proposed work Performance analysis is done based on parameters PSNR, MSE. Peak signal to noise ratio (PSNR) measures the quality of the Final stego-image with cover image. If PSNR value is higher, then the quality of an image will be better. Mean square error (MSE) can be computed by performing byte by byte comparison of the cover image and Final stego-image. The small value of MSE will represent more efficient image steganography technique. Below two graphs between previous and proposed techniques shows different PSNR and MSE values on different noise density values.

Table 3: PSNR Comparison between Previous and Proposed Techniques.

Noise Density	PSNR Values (Previous technique)	PSNR Values (Proposed technique)
0	94.0771	90.3973
.001	38.1991	84.6078
.005	34.3685	78.6433
.010	33.5587	75.7699
.050	32.5783	68.8761
.100	32.3719	65.9148
.250	32.1874	62.2873
.500	32.0952	60.2059
.750	32.0593	59.2932
1	32.0470	58.7893

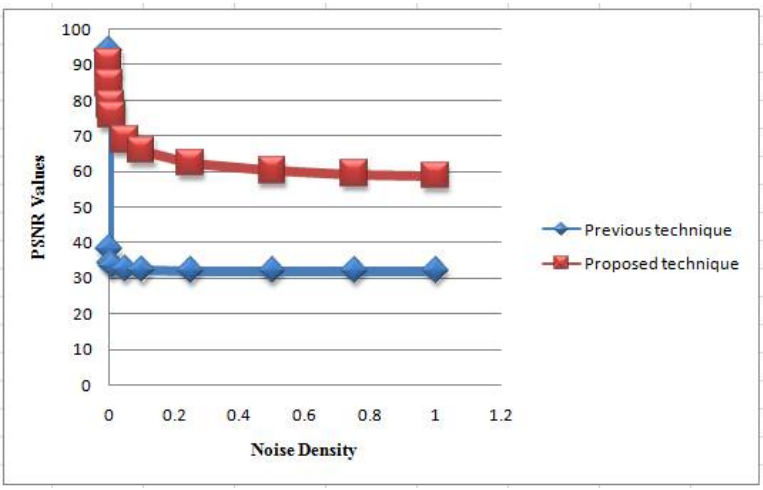

Fig4. PSNR Comparison between Previous and Proposed Techniques

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Table 4: MSE Comparison between Previous and Proposed Techniques.

Noise Density	MSE Values (Previous technique)	MSE Values (Proposed technique)
0	2.54E-05	5.93E-05
.001	9.8439	2.25E-04
.005	23.7809	8.89E-04
.010	28.6555	1.70E-03
.050	35.9128	8.40E-03
.100	37.661	1.67E-02
.250	39.2949	3.84E-02
.500	40.138	6.20E-02
.750	40.4719	7.65E-02
1	40.5863	8.59E-02

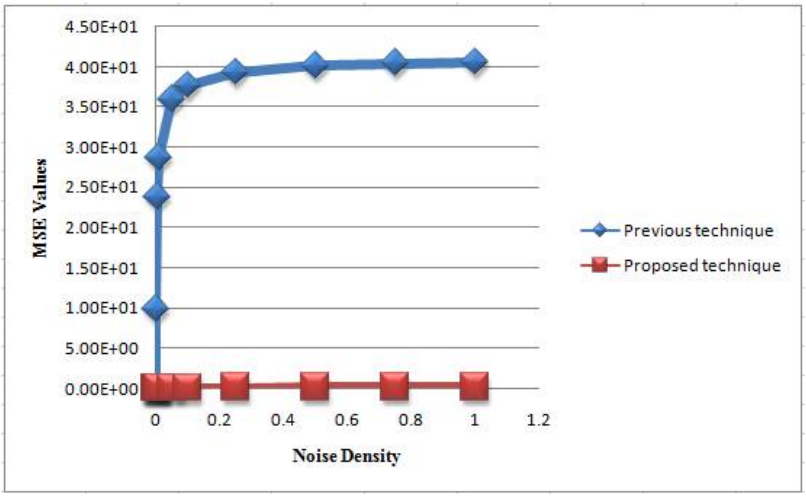

Fig5. MSE Comparison between Previous and Proposed Techniques

VI. CONCLUSION

During data transmission if data is intercepted then it can be used successfully by an unauthorized person over the internet. Therefore to provide more security to the information at the time of communication over unsecured channel a dual steganography advance technique for data security is needed. In this paper, proposed highly secured data hiding dual steganography scheme which is based on status LSB and 2-D Haar-DWT algorithms. A new dual steganography is a technique which combines steganography within steganography that offers an ideal system for secret data transmission with respect to stand-alone cryptographic and steganographic techniques. This technique hides the secret message in binary form in two cover images due to which double protection has been provided to confidential data. The Final Stego-image is looking perfectly intact and has high PSNR value and low MSE value. Hence, an unintended observer will not be aware of existence of the secret message inside the cover image. The extracted secret data is perceptually similar to the original secret data. This method is one of the safest forms of the digital data transmission and communication with the internet and other communication system in this digital world.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

[1] Piyush Marwaha, Paresh Marwaha ,"Visual Cryptographic Steganography in Images" in proceedings of Second International conference on Computing, Communication and Networking Technologies, pp 1-6, 20104.
[2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key" , in proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011), pp 22-24, 2011.
[3] Gokul M, Umeshbabu R, Shriram K Vasudevan, Deepak Karthik, "Hybrid Steganography using Visual Cryptography and LSB Encryption Method", in International Journal of Computer Applications, Vol. 59, pp 5-8, 2012.
[4] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding using Least Significant Bit Steganography and Cryptography" in I.J. Modern Education and Computer Science, Vol. 6, pp 27-34, 2012.
[5] Mohammad, A. A., and Abdel Fatah, "Public-Key Steganography Based on Matching Method" in European Journal of Scientific Research, pp 223-231, 2012.
[6] R. Nivedhita, Dr. T. Meyyappan, "Image Security using Steganography and Cryptographic Techniques", in International Journal of Engineering Trends and Technology, Vol. 3, pp 366-371, 2012.
[7] Ramakrishna Mathe, Veera Raghava Rao Atkuri, Dr. Srinivasan Kumar Devireddy, "Securing Information: Cryptography and Steganography", in International Journal of Computer Science and Information Technologies, Vol. 3, pp 4251-4255, 2012.
[8] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" in proceedings of 3rd International Conference On Informatics, Electronics & Vision, pp 1-6, 2014.
[9] Pye Pye Aung, Tun Min Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", in International Journal of Information Technology, /modelling and Computing (IJITMC), Vol. 2, pp 55-62, 2014.
[10] Shingote Parshuram N., Syed Akhter Hussain, Bhujpal Pallavi M., "Advanced Security using Cryptography and LSB Matching Steganography", in International Journal of Computer and Electronics Research, Vol. 3, pp 52-55, 2014.
[11] Divya Chaudhary, Shailender Gupta, Manju Kumari, "A Novel Hybid Security mechanism for Data Communication Networks" accepted for publication in Inderscience Journal, 2015.
[12] Yamini Jain, Gaurav Sharma, Gaurav Anand, Sangeeta Dhall, "A Hybrid Security Mechanism based on DCT and Visual Cryptography for Data Communication Networks" accepted for publication in CSI-2015 Journal.

BIOGRAPHY

Manisha (author) is an M-tech Scholar in the computer Science & Engineering Department, BSAITM college, M.D.U. Rohtak, Faridabad. I have received B.TECH degree in Computer Science and Engineering from Maharshi Dayanand University in 2013. My research interested areas are Computer Networks (wireless Networks), Secure Data communication and Image processing.

Deepkiran Munjal (co-author) is an Assistant Professor in the Computer Science & Engineering Department, BSAITM, M.D.U. Rohtak, Faridabad. She is working as an Assistant Professor in Computer Engineering department in B.S.A. Institute of Technology & Management, Faridabad. Her areas of interests are Software testing, Data mining and networking.