Secure Information Hiding Technique using Text Steganography Followed by Image Steganography

Suthar Maulik Kumar[1] Mukesh Kumar Choudhary[2]
[1,2]Department of Computer Science and Engineering
[1,2]Rajasthan Institute of Engineering & Technology, Jaipur, India

Abstract— Steganography is a data encoding technique which prime aim to hide the information into a carrier or enveloped media. The word steganography came from Greek language, which means covert writing. Today each information is going in digital due to the fast communication of data through internet. Hence, today digital word demands secret communication. So, here is a need of sending information through cover media. There are many kinds of cover media are available among them images are preferred mainly. The secret and confidential data requires such data hiding technique to avoid the attack. The secure communication of data continuously demands to develop the secure steganography technique. Information system security is an authority or disciplines that aim is to provide Availability, Confidentiality, and Integrity. Today`s digital media is the way for fast communication. Each and every thing is presented in digital form over cloud or internet. In this way, there is a requirement for secure correspondence. Locale increasing obvious cryptography is utilized to cover numerous mystery levels in an unmarried picture. In n level spot increasing obvious cryptography conspire; photograph is partitioned in n regions. Every area incorporates one level certainty. For forcing unmistakable cryptography in n levels need to encode (n+1) stocks in such a way in this way, that any single offer isn't in a situation to uncover the records and by utilizing joining any two offers, first degree insights may be seen. After visible cryptography the photograph is embedded into the duvet photo and gets the steno photo. So, it is difficult to discover by using the steganalysis and it is appear like as a cowl photograph. In proposed set of rules, problem of pixel growth and negative evaluation has been re-moved and further it's far changed to generate the ranges automatically which is known as automatic vicinity incrementing visible cryptography.

Keywords: Steganalysis, Image, Security, Cryptography

I. INTRODUCTION

Steganography is a data encoding technique which prime aim to hide the information into a carrier or enveloped media. The word steganography came from Greek language, which means covert writing. Today each information is going in digital due to the fast communication of data through internet. Hence, today digital word demands secret communication. So, here is a need of sending information through cover media. There are many kinds of cover media are available among them images are preferred mainly. The secret and confidential data requires such data hiding technique to avoid the attack. The secure communication of data continuously demands to develop the secure steganography technique [1].Information system security is an authority or disciplines that aim is to provide Availability, Confidentiality, and Integrity. it is classified into three classes; these are as follow:

1) Cryptography,
2) Watermarking
3) Steganography

As the development in security techniques, attacker techniques are also designed. Steganalysis is a kind of attack in any kind of steganography technique which prime is to breech the security. The watermarking and steganography are something similar techniques but there aims are different. The watermarking is use as in copyright protection or authentication whereas the steganography is used secret communication. So, here we can say that it does not figure out where the actual message is [2][3]. One basic difference of both steganography and watermarking with the cryptography is that in cryptography the future is every time visible which may pay the attention of outsider that something is sending in encrypted form. So, the steganography techniques are helpful figure out where the message is [2][3].In some cases, sending encoded data may moreover draw the consideration of an eyewitness, while imperceptible certainties will now not. Watermarking is similar, anyway has an exceptionally stand-out reason. Watermarking is the system of installing records on the media. Putting a watermark in media record serves to end up mindful of the craftsman or author of the artistic creations for example its miles utilized for copyright security [4]. A watermark might be either unmistakable or imperceptible. The wide application territory of data covering up, security, encryption and watermarking can be classified as appeared in figure1.

A relation between various data hiding techniques and related parameters is illustrated below in table 1.

A. Scope of Steganography

With the improve in PC power, the net each and the entire parcel has long past in "advanced". Steganography has made a situation of organization watchfulness that has generated different intriguing projects appropriately, its proceeding with development is guaranteed. Probably the most punctual methodology to talk about virtual steganography is credited to Marvel [5] who proposed a way which takes after inserting into the 4 LSBs (least considerable bits). They inspected picture minimizing and contamination which is referred to now as photo based absolutely steganography. Digital wrongdoing is accepted to profit by this virtual unrest. Henceforth a prompt issue is to discover remarkable feasible ambushes to perform steganalysis, and simultaneously, vitality in present steganography methods against celebrated attacks.

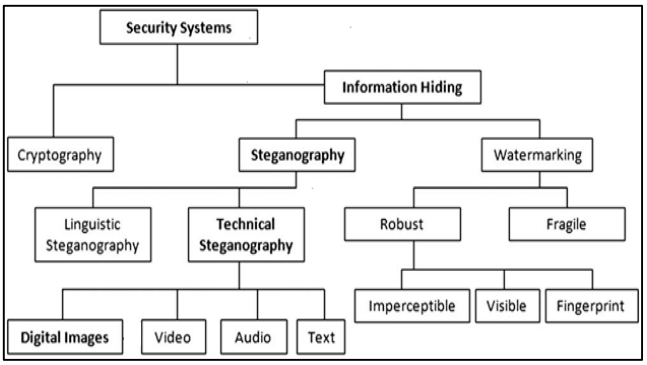


Fig. 1: Classification of different security system, for information hiding

Method → Parameter ↓	Steganography	Watermarking	Cryptography
Carrier	Any digital media	Mostly image/audio files	Usually text based, with some extensions to image files
Secret data	Payload	Watermark	Plain text
Input files	At least two	N/A	One
Detection	Blind	Usually informative	Blind
Result	Stego-file	Watermarked-file	Cipher-text

Table 1.1: Comparison of Steganography, Watermarking and Cryptography

B. Applications of Steganography

1) Steganography might be an answer which makes it suitable to deliver news and certainties without being edited and without the worry of the messages being blocked and followed again to us.
2) It is also possible to actually use steganography to store records on a place. For example, numerous information assets like non-public banking information, some navy secrets and techniques, can be stored in a cowl source. When it's far required to unhide the name of the game information inside the cover supply, banking statistics can be easily revealed and it is going to be not possible to prove the lifestyles of the navy secrets and techniques inner.
3) Steganography can also be used to enforce watermarking. The transportation of sensitive information is every other key use of steganography. A ability trouble with cryptography is that eavesdroppers understand they have got an encrypted message when they see one. Steganography lets in to transport of touchy records beyond eavesdroppers without them understanding any touchy information has handed them. The idea of using steganography in records transportation may be implemented to pretty much any statistics transportation approach, from E-Mail to photos on Internet websites.

C. Motivation

Steganography, forever, have modified the way people are sending and having access to the information. It allows the human beings to speak secretly. As an increasing number of fabric turns into available electronically. Much exclusive statistics become leaked to an adversary company. The utility of steganography is a critical motivation for feature choice. New steganography strategies are being developed and data hiding is turning into more advanced. The number one motivation for any steganography technique is to offer excessive high-quality steganography effects, robust towards statistical assaults [6], over a unexpectedly growing World Wide Web.

D. Problem Statement

Picture Steganography might be executed the utilization of some of techniques. There are popular plans utilized for photograph steganography: spatial zone and change space implanting. In spatial area inserting, the image handling is connected at the image pixel esteems right away. The advantage of these systems is effortlessness. By and large even the little adjustments coming about out data misfortune. Least Significant Bit Insertion strategies, strategy come underneath lay in this class.

In change region inserting, stage one is to change over the spread photograph into uncommon territory. At that point the changed coefficients are prepared to shroud the name of the game insights. These changed coefficients are changed once more into spatial area to get stego photo.

It has been located that maximum robust steganography systems recognized today virtually function in some shape of transform domain. Transform area methods conceal information in vast regions of the duvet picture which makes them more robust to the steganalysis attacks. Many remodel domain variations exist which include Fourier and cosine transforms, DCT and DWT. Here, in the proposed methodology, the discrete wavelet change is utilized.First the name of the game message is transformed into every other meaning full message with the assist of textual content-based steganography approach and generate a image from these textual content steganography message (say: secret image S). However, the trouble with this method is that there's still a opportunity of the stego message being without difficulty detected in steganalysis. So secondly the Discrete Wavelet Transform is applied on the quilt photo and mystery photo (S image). Then Alpha Blending or mixing is applied, which makes the detection of the name of the game photograph within the cover image impossible and sooner or later stego photo is obtained via making use of the Inverse discrete rework (IDWT).

E. Research Approach

The proposed method consists procedures- one is encoding technique and some other is deciphering technique. The encoding processed is combination of two steganography techniques.

1) Text based totally steganography
2) Image steganography

In image steganography alpha blending is used to addition of wavelet coefficients of respective sub-bands of cowl photo and secret image. After the Alpha Blending task,

Inverse Discrete Wavelet Transform (IDWT) is connected and the stego picture is gotten. The unraveling way is the turnaround of the encoding framework with one improves trademark dazzle identification.

II. LITERATURE SURVEY

A. Information Security

Security is the class to be free from hazard. A successful society should have mysterious security as objective, Communications and Network security.

Data security is assurance of data and its components that utilization to store and transmit that data. The PC can be either subject of an assault or the object of an assault, or both. At the point when a PC is the subject of an assault, it is utilized as a functioning. When it is the object of an assault, at that point it is treated as an individual being assaulted.

It is impossible to obtain great security; it is a process to achieve security in digital communication system. Security should be considered a balance between protection and availability of information.

Security is nothing new; the way that security has become a part of daily life today is unprecedented. The cryptography is used to encode political directives and other information. Steganography the art of hidden writing has also been used from last decades. But the connection of these existing techniques with the constant use of the Internet and communication skill makes this a restricted moment in record for concealed communication [9]. A covert communication system has to make use of unintended features of commonly used protocols, in a way that does not arise distrust, in order to unobservable transmitting messages between two users.

B. Cryptography

Cryptography encodes data so that no one can peruse scrambled data, aside from the planned beneficiary. Progressively advance cryptographic procedures guarantee that the data being transmitted has not been altered in the middle of travel. A comprehension of cryptography starts with a fundamental comprehension of some basic wording [10]:

Plain text refers to any type of information in its original form. It can be any word-processed document, an image file etc.

Cipher text refers to a message in its encrypted form, or corrupted information. The meaning of the information in cipher text is obscured. Encryption is the process of taking a plain text message and converting it into cipher text.

Decryption is the opposite of encryption [11],[12],[13]. Decryption takes a cipher text message and converts it to plain text. It's important to remember that there is a relationship between the encryption and decryption processes. A cryptanalyst is a person who tries to find weaknesses in encryption schemes [14],[15].

The key is use to provide protection in information, a key is necessary to decode an encrypted information. A lot of people may use the similar encryption algorithm, but as long as they use different-different security keys, information is being protected. To provide security the key should be protected and nobody guess the actual value of key.

Types of Cryptographic Algorithm

On the basis of public and private key cryptographic algorithm have two types.

1) Symmetric key
2) Asymmetric key

Cryptanalysis: Techniques utilized for decoding a message with no learning of enciphering subtleties fall into the region of Cryptanalysis. Cryptanalysis is the thing that the layman calls 'Breaking the Code '.

Cryptology: The territories of cryptography and cryptanalysis together are called Cryptology. [1]Goals of Cryptography

The main goals of cryptography are

1) Confidentially or privacy
2) Data integrity
3) Authentication
4) Non-repudiation

C. Characteristics of a Cryptographic Algorithm

The main characteristics of cryptographic algorithm are [2]

1) Level of Security

Typically the degree of security is characterized by an upper bound on the among of work important to overcome the goal. This is once in a while called 'Work Factor'. Work Factor could be characterized as the base measure of work required to contend the private key when given the open key, or on account of the symmetric key plan to decide the mystery key. A usefulness calculation should be joined to meet different data security destinations. Which calculation is best for the given goal, will be controlled by the essential properties of the calculation. The techniques for tasks calculation when connected in different ways and with different data sources will normally display various qualities. In this manner, one calculation could give altogether different usefulness relying upon its method of activity or utilization

2) Performance

Performance alludes to the effectiveness of a calculation in a specific Method of activity. For Example, the quantity of bits/secs at which it can scramble may rate an encryption calculation. [3]

Data is significant in our everyday life. Data gets more worth when imparted to other people. Because of advances in innovations identified with systems administration and correspondence, it is conceivable to share the data like sound, video and picture effectively. It might offer ascent to security related issues. Giving security to the computerized data partook in everyday life is a significant issue, all things considered.

D. Steganography versus Cryptography

The comparison and contrast between steganography and cryptography is illustrated from the following table 2.1.

S. No.	Context	Steganography	Cryptography
1.	Definition	Steganography is a art or science to hide the information in such a way that no one apart from the intendant receipent known	Cryptography is the art of hiding the contents of a message from an attacker, but future is always visible.

		the existence of hidden information.	
2	Cover Files	Imasge, Audio, Text, etc.	Manly Text Files
3	Hidden Files	Image, Audio, Text, etc.	Manly Text Files
4	Type of Attack	Steganalysis: Analysis which identify that the file is stego or not.	Cryptanalysis: Attempt to find out the decoding scheme.

Table 2.1: Comparisons between Steganography and Cryptography

E. Steganography Models

From last decades many steganographic technique have been developed to for concealed communication, and each of them will be designed to make steganalysis a difficult task by finding where the redundancies are within a cover work, and then modifying the redundant data such that it holds a secret message.

Steganography can be dividing into following main category:

1) Statistics-aware steganography
2) Model-based steganography

Each of these categories aims to preserve the qualities of the original cover work, with the logic that it will be hard to detect steganography in suspect work that is identical to an innocent work. Statistics-aware steganography considers the statistical techniques that steganalysis are known as the detector of steganography technique. With taking these approaches in mind, the steganographic technique is developed in such a way that none of these attacks will confirm the presence of information. In other words, the steganography that is produced after embedding a secret message will be statistically sound. Ingemar Cox [18] illustrates this by example when he suggests that an image can be "completely described" by its histogram (a graphical chart of pixel frequencies). If this is the case, histograms can be used to evaluate whether any unusual trends take place. A steganographic system that preserves the same histogram as the cover work would therefore be a prime example of a statistics-aware steganographic implementation.

III. PROPOSED STEGANOGRAPHY TECHNIQUE USING QR CODE

A. Proposed Technique

The proposed method is based on the sequence of two techniques-

1) Text based steganography method
2) Use image steganography technique to hide one share inside cover image

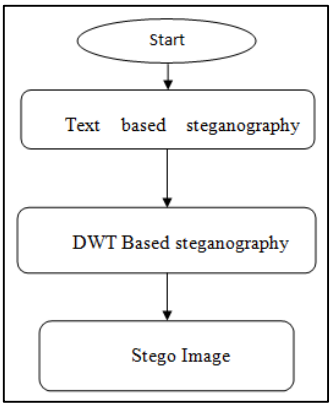


Fig. 2: Algorithmic flow chart for the development Technique

1) Text based steganography:

English alphabet-based text steganography is used in current work which has the fixed word order and it use the periphrases for date hiding without change the basic properties of a sentence. this is based on the Vedic Numeric Code it gives the flexibility to the user to form a sentence. The Vedic code is based on the idiom position and on the basis of it each letter is assigned a number. Table 2 shows the assignment of number for the letter these numbers are ranged in between 1 to 15.

The assignment of numbers are based on the frequencies, The number assigned on the basis on the following [25].

(N+0.99) % to (N+0.3) % and N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11.

It represents the frequency of integer in the form of number. Such kind of number assignment gives the flexibility to choose the letter for sentence assignment.

E	15		M	17
A	14		H	7
R	13		G	6
I	13		B	5
O	12		F	4
T	11		Y	4
N	11		W	3
S	10		K	3
L	10		V	3
C	9		X	2
U	8		Z	2
D	8		J	1
P	7		Q	0

Table 3.1: Letter to Number Assignment

2) Steps for Encoding:

1) Represent every letter in to the form of secret message by using its equivalent code in ASCII.
2) Convert the ASCII code into its equivalent 8-bit binary number.
3) Divide these 8 bits into two parts of 4 bit.
4) Select the appropriate letter from the given table 3.1 equivalents to the group of 4 bit.
5) Construct the Meaningful sentence by using the letters taken as the original letters of appropriate or proper words.
6) The formation of articles or sentence is free to use Pronoun, proposition, adverbs, is/am/are, was/were,

shall/will, should/would has/have/had in sentence construction.

3) Steps for Decoding:

1) Pick each word from cover message in which starting letter was represented by the 4-bit number in the time of encoding.
2) Combined these two 4-bit numbers and get number of size 8 bit.
3) Obtain corresponding ASCII code from generated 8-bit binary numbers.
4) Recover the Original message from these ASCII code.

4) DWT Based steganography:

Create image from text-based steganography message. This image is treated as the secret image and it is embedded inside the cover image and get stego image as output. Apply Haar Discrete Wavelet Transform (DWT) on the secret image and cover image. The alpha mixing matrix is acquired by the addition of wavelet coefficients of respective sub-bands of cowl picture and secret photo [15 abhis]. Alpha aspect increases the embedding strength issue. After the Alpha Blending operation, the Haar Inverse Discrete Wavelet Transform (IDWT) is applied and get the stego picture. The decoding procedure is reverse of the encoding system. The Algorithmic steps of encoding manner are shown below:

1) Step 1: Obtain the cover image and the secret image.
2) Step 2: Apply a 1-level 2-D Haar DWT on the image cover image.
3) Step 3: Apply a 2-level 2-D Haar DWT on the Secret image.
4) Step 4: Apply Alpha Blending operation on cover image and secret image which is obtained from step 2 and step 3. At last perform 2-D Haar IDWT to obtain the stego image.

B. Alpha Blending

Alpha Blending is the technique of mixing of two images together to form a desired output image. According to the alpha blending, the final image is given by following equation.

$$FI = I_1 + \alpha * I_2 \qquad (1)$$

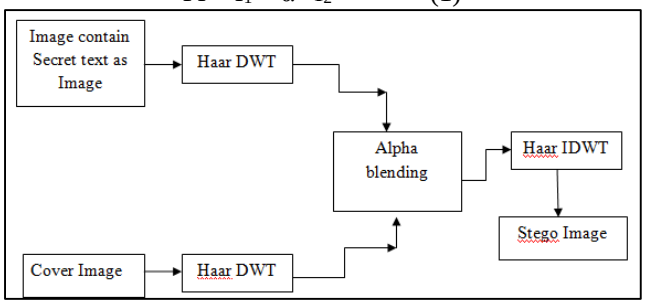


Fig. 3: Image Encoding Process of proposed technique.

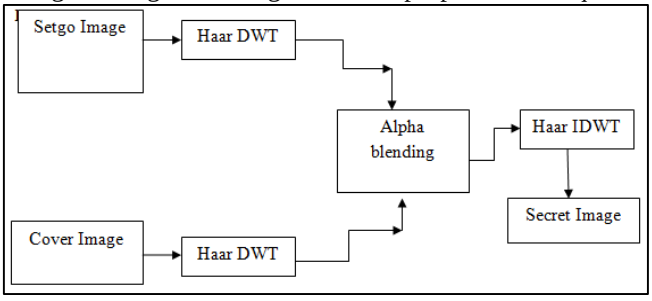


Fig. 4: Decoding Process of proposed technique

Here the value of α is in between 0 < α >1, FI - Final Image, and I1 and I2 is the First Image and Second Image respectively. The value of alpha is varying in between the 0 and one. The 0 indicate low value of embedding and it move towards to one but the extracted resultant image have the better visual quality at the value at the middle level of the embedding parameter.

The QR code-based embedding is used because text-based steganography the output message length is very high as compare to the original message. Here QR code has the grater embedding capacity in it and easy to embed inside the image or treated as the secret image.

IV. EXPERIMENTAL RESULTS OF THE ALGORITHM

A. Introduction to Mat Lab

The call MATLAB stands for Matrix Laboratory. MATLAB is a software package for excessive-performance numerical computation and visualization. It gives interactive surroundings with integrated functions for technical computation, graphics and animation. It has its very own excessive-level programming language [18]. MATLAB's built-in features provide wonderful guide for linear algebra computations, sign processing, facts evaluation, and numerical solution of everyday differential equations, optimization, quadrature and plenty of other varieties of clinical computations.

The matrix is the fundamental building block of MATLAB. The basic records shape is the array, an ordered set of real or complex elements. This object is obviously proper to the illustration of picture, actual-valued, ordered units of color or intensity information. (MATLAB does no longer support complex-valued photographs). Vectors, scalars, actual matrices and complicated matrices are all routinely treated as special instances of the primary information kind. Several non-obligatory "toolboxes" also are to be had in MATLAB. These toolboxes are units of capabilities written for unique programs together with photograph processing, neural networks, control device design, statistics and symbolic computation. The listing of toolboxes is persevering with to develop with time. Now, greater than 50 such toolboxes are to be had [18].

B. Image Processing in Mat Lab and it's Toolbox

When working with photos in MATLAB, there are many matters to cope with inclusive of loading an image, the usage of the proper format, saving the records as different data kinds, the way to display a photograph, conversion among exclusive image formats, and so on. MATLAB affords commands for these operations. These instructions require the Image Processing Toolbox to be hooked up with MATLAB. The Image Processing Toolbox is a collection of capabilities

C. Key Features

1) Standard wavelet families, including Daubechies wavelet filters, complex Morlet and Gaussian, real reverse biorthogonal, and discrete Meyer
2) Wavelet and signal processing utilities, including a function to convert scale to frequency

D. Experimental Results and Performance Analysis

The performance of the proposed method is evaluated by implementing it using MATLAB R2013a. By taking "Tex" secret message peppers.tiff as the cover image, the corresponding experimental results are as shown in figures below.

Example: suppose the secret message is "tex". To implement above steganography, here is need to convert "tex" into the binary number.

S. No.	Character	Decimal value	ASCII Representation
1	t	116	01110100
2	E	103	01100101
3	X	120	01111000

tex= 011101000110010101111000

Table 4.1: Shows the Binary Equivalents to These Letters
The Result of the overall encoding steps is shown in Fig. 5

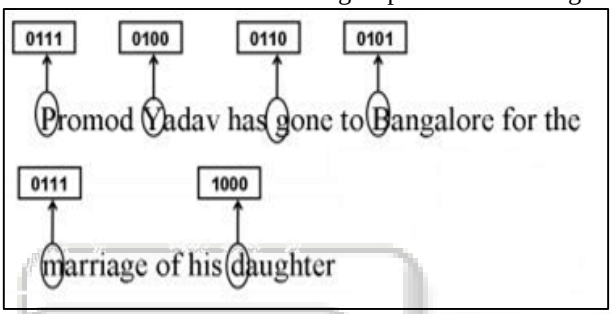


Fig. 5: Encoding process for steganography technique based on text

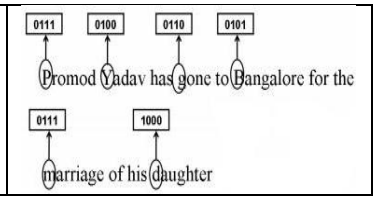
Performance of the proposed approach is analyzed by way of comparing the duvet picture and the stego picture in phrases of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE). PSNR degree the distortion between the original cover picture and the stego image. It is defined as comply with:

$$PSNR = 10 \log \frac{255^2}{MSE} DB$$

where MSE is the mean square error representing the difference between the original cover image x (sized M x N) and the stego image x' (sized M x N) [12]. If $xj_{,k}$ and $x'_{j,k}$ is the pixel located at the j^{th} row and k^{th} column of images x and x' respectively, then it is defined as follow

$$MSE = \frac{1}{N}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})^2$$

A large PSNR value indicates that the higher image quality (which means there is only little difference between the cover image and the stego image). On the contrary, a small PSNR value indicates that there is great distortion between the cover image and the stego image. It is tough for the human eyes to differentiate among the unique cowl picture and the stego photo whilst the PSNR cost is bigger than 30db [12]. Also, the cost of MSE need to be as less as feasible.

tex= 011101000110010101111000 a). Original secret message "tex" and its Binary representation	

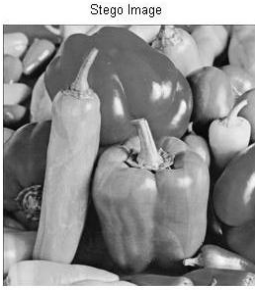
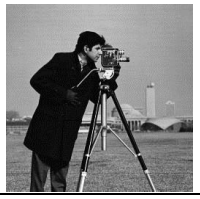
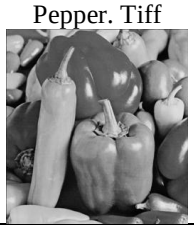
	b). Text based steganography containing "tex" as secret message
 c). Secret Image	 d). Cover image
 e). Stego image	 f). Extracted secret Image

Fig. 6: Experimental results of proposed technique

The proposed approach is tested for the extraordinary cover photos and secret pictures for the diverse values of Fine tuning the embedding power thing alpha improves the pleasant degree of stego photograph and the extracted secret photograph. The photo first-class measurements for some of the examined pix were illustrated in Table 4.Four. The results show excessive PSNR and occasional MSE values which indicate the effectiveness and accuracy of our proposed technique.

Cover Image	Message Image		
	Pramod message image	House	Lenna
Camera man 	34.6133	37.0950	39.6486
Gold hill 	34.3886	36.8532	39.4040
Pepper. Tiff 	33.8467	36.3113	36.3113

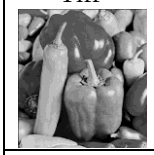
Cover Image	Secret Image	PSNR	MSE	NC
Pepper. Tiff 		33.8467	1.4673e+06	0.9698
cameraman  godhill		34.6133	5.8924e+06	0.9707
Godhill	Pramod	34.3886	1.4673e+06	0.9671

Table. 4.2:
Picture Quality Measurements of Proposed Technique, for Some of the Cover Images and Secret Images of Text Message

Image size and 256 X 256 cover image alpha=.02

Secret images (128X128)		Cover image (256 X 256)			
		Peppers.tiff	Goldhill.jpg	Cameraman.jpg	Barbara.jpg
Homi Bhaba.jpg	Existing Tech. [18]	25.11	25.58	26.65	24.54
	Proposed Tech.	43.33	43.87	44.11	43.80
Airplane.png	Existing Tech. [18]	27.72	28.43	27.40	27.92
	Proposed Tech.	46.15	46.69	46.11	46.62
Redfort.jpg	Existing Tech. [18]	30.79	30.91	29.76	30.34
	Proposed Tech.	44.20	44.74	44.99	44.67
Bird.png	Existing Tech. [18]	30.36	30.20	28.61	30.13
		47.01	47.54	47.78	47.11

Table 4.3: Comparison of Proposed Technique's PSNR with the Existing Technique

It can be concluded from the above table that proposed techniques results better as compared to the existing one [18]. The proposed technique provides good PSNR, observed ranged is 43 db to 47 db. Which indicates that the proposed technique results good quality stego image. The steganography based double encoding techniques introduced excellent security in secret data.

V. Conclusion and Future Scope

Highly secure hybrid image steganography technique has been proposed using two types of data hiding (i.e. text steganography followed by DWT steganography). The security of information is more agreeable then the previously existing technique. It can be clearly seen in the results section that the proposed technique's results are much better than the previously existing technique. Proposed technique provides the more security then other existing technique because it uses two time steganography data encoding so security of secret information is more reliable than other existing technique.

The PSNR value in our proposed work is good as compared to previously existing technique.

The Excellent NCC value is obtained in proposed technique as compared to previously existing technique.

On the basis of obtained results we can conclude that the proposed technique is robust then other existing technique.

The future work will focus other kinds of steganography techniques like; firefly image steganography, Particle Swarm Optimization Algorithm and other wavelet based steganography technique etc.

The future work will also focus more secure hybrid steganography using different approaches.

References

[1] BablooSaha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, vol. 62(1), pp. 11-18, 2012

[2] Palak Mahajan, Heena Gupta, "Improvisation of security in image steganography using DWT, Huffman Encoding & RC4 based LSB embedding", IEEE International Conference on Computing for Sustainable Global Development (INDIA Com), pp. 523-529, 2016

[3] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An overview of image steganography", Proceedings of the Fifth Annual Information Security South Africa Conference, June 2015

[4] J. Fridrich, R. Du, and L. Meng, "Steganalysis of LSB Encoding in Color Images", Proc.IEEE Int'l Conf. Multimedia and Expo, IEEE Press, Piscataway, N.J., vol.3pp. 1279-1282, 2000

[5] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. pp. 26-34, Jun. 2011.

[6] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. Vol. 5(1), pp. 41-52, 2011.

[7] Shaddad, J. Condell, K. Curran, and P. Mckevtt. "Biometric inspired digital image steganography." In Proc. of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008. Pp. 159-168.

[8] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE, pp. 1019-1022, 2001.
[9] GurmeetKaur and Aarti Kochhar "Transform Domain Analysis of Image Steganography" International Journal for Science and Emerging Technologies with Latest Trends" Vol. 6(1): 29-37, 2013.
[10] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, The Information Security Reading Room, SANS Institute 2002.
[11] F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in proceeding of IEEE , pp. 1062-1078, July 1999.
[12] Y.K. Lee and L.H. Chen, "A Secure Robust Image Steganographic Model", in Tenth National Conference on Information Security, Hualien, Taiwan, pp. 275-284, May 5- 6, 2000.
[13] R. Chandramouli, "Data hiding capacity in the presence of an imperfectly known channel," SPIE Proceedings of Security and Watermarking of Multimedia Contents II, vol. 4314, pp. 517–522, 2001. 22.
[14] N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in David Aucsmith (Eds.): Information Hiding, LNCS 1525, Springer-Verlag Berlin Heidelberg., pp. 32–47, 1998.
[15] D. Upham, "Jpeg-jsteg," ftp://ftp.funet.fi/pub/crypt/steganography/jpegjsteg-v4.diff.gz
[16] Y. Wang and P. Moulin, "Steganalysis of block-dct image steganography," IEEE Workshop On Statistical Signal Processing, 2003.
[17] Avcibas, N. Memon, and B. sankur, "Steganalysis using image quality metrics." Security and Watermarking of Multimedia Contents, San Jose, Ca., Feruary 2001.
[18] Burges, "A tutorial on support vector machines for pattern recognition," Data Mining and Knowledge Discovery., pp. 2:121–167, 1998
[19] R. Zamir, S. Shamai, and U. Erez, "Nested lattice/linear for structured multiterminal binning," IEEE Transactions on Information Theory, 2002.
[20] J. Chou, S. S. Pradhan, L. E. Ghaoui, and K. Ramchandran, "A robust optimization solution to the data hiding problem using distributed source coding principles," Proceedings SPIE: Image and Video Communications and Processing, vol. 3974, 2000.
[21] R. Chandramouli, "Data hiding capacity in the presence of an imperfectly known channel," SPIE Proceedings of Security and Watermarking of Multimedia Contents II, vol. 4314, pp. 517–522, 2001.
[22] P. Moulin and J. Sullivan, "Information theoretic analysis of information hiding," To appear in IEEE Transactions on Information Theory, 2003
[23] M. Ramkumar and A. Akansu, "Information theoretic bounds for data hiding in compressed images," IEEE 2nd Workshop on Multimedia Signal Processing, pp. 267–272, Dec. 1998.
[24] M. Ramkumar and A. Akansu, "Information theoretic bounds for data hiding in compressed images," IEEE 2nd Workshop on Multimedia Signal Processing, pp. 267–272, Dec. 1998.
[25] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.

