National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 446-452

Improved study and literature review on image steganography: A survey

[1] Swati Bhargava, [2] Manish Mukhija

[1] M.Tech Scholor, CSE Dept. Modern Institute of Technology and Research Centre, Alwar, Rajasthan, India

[2] Asst. Prof, CSE Dep. Modern Institute of Technology and Research Centre, Alwar, Rajasthan, India

Abstract

Steganography is the sciences that involve communicate covert data in a suitable multimedia carrier, for e.g., image, audio, and video files. It comes beneath the assumption so as to if feature is visible, point of assault is obvious, thus aim here is for all time to hide the extremely existence of embedded data. Steganography has a variety of use applications. Though, like any other science it be able to used for the ill intentions. It has been propelled to front of present security techniques by remarkable development in computational power, increase in safety awareness by, e.g., individuals, groups, agency, and government and all the way through intellectual detection. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. This paper introduces two new methods where in cryptography and steganography are combined to encrypt the data as well as to hide the data in another medium through image processing. This Report securing the image by encryption is done by DES algorithm using the key image. The encrypted image can be hiding in another image by using RSA techniques, so that the secret's very existence is concealed. The decryption can be done by the same key image using DES algorithm.

Keywords: component, formatting, style, styling, insert

1. Introduction

In this modern era, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first technique of cryptography was invented to send secret messages over places. In cryptography the message was encoded in another message in a covered way such that only the sender and receiver knew the way to decrypt it [1]. A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that other person came to know that the message had a hidden text in it and so the probability of message being decoded by other person increased. To overcome this limitation the technique of steganography was introduced. The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing". The first of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data. The technique of steganography was far better than cryptography as in it the data was hidden in image. The image was then sent over internet. It had advantage over cryptography as now the middle person does not come to know whether data is hidden in the image ors not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now no other person could change the sent data.

1.1 Steganography

This word is taken from Greek words Steganós (enclosed), and Graptos (script) which exactly signifies "enclosed script" [2]. Normally it is recognized as "invisible" communication. It denotes hide messages present in a different medium (video, picture, sound files communication). Today's these schemes utilize multimedia (image, sound file, video etc.) as enclose media because people over and over again broadcast digital pictures over message or distribute them through other communication application. It is different from protecting the real substance of a message. In simple words it would be like that, conceal data into other information.

Means of Steganography is not to modify the arrangement of covert message, but conceal it within a cover- object. Later then hiding procedure stego-object (moving concealed information) and cover object are comparable. So, cryptography (shielding information) and steganography (concealing information) are completely different to each other. Because of concealed factor it is hard to improve information with no identified process in steganography. Detecting procedure of steganography known as Steganalysis.

It is the method of thrashing covert information in any media. It is often baffled with cryptography for the reason that two are comparable in the manner that they together are utilized to defend secret information. The dissimilarity between the two is in the form in the executed output; the outcome of steganography procedure is not actually visible other than in cryptography the outcome is scrambled in order that it may represent attention. Steganlysis is procedure to detect of presence of steganography. Many steganography schemes use pictures a stego-medium.

1.2 Steganography Model

Generally a steganographic system has a coverage file that is used to cover the original message and the steganography algorithm to carry out the required object as shown in Fig. 1. The result is a file called stego-file which has the message inside it, hidden. This stego file is then sent to the receiver where the receiver retrieves the message by applying the de-steganography. The goal of modern steganography is to keep the message undetectable [3].

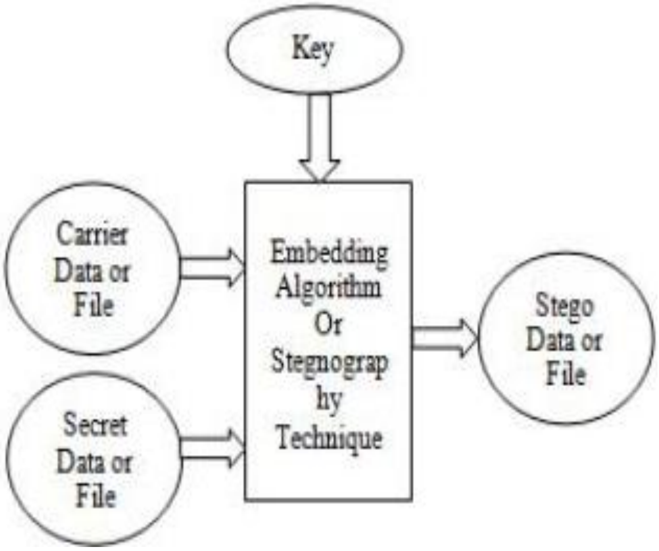

Fig 1: Basic Steganography Model

2. Steganography System

Steganography is the art of hiding the information in some other host object. It has been used since ancient time by the people. In ancient time, secret information is hidden in the back of the wax, the scalp of the slaves, in rabbits, etc. With passage of time, the application of steganography and its area has become widened. With the introduction digitization era, digital steganography has emerged as the new tool to hide the information secretly. Text, digital image, digital audio and digital video have become the host object for data hiding. Below are some of the common term which is necessary to understand any steganography system [4].

Cover Media- It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data

Stego- Media- It is medium obtained after embedding the secret information.

Secret data- The data or information to be hidden in cover media.

Steganalysis- The process of detecting, presence of secret data in cover media.

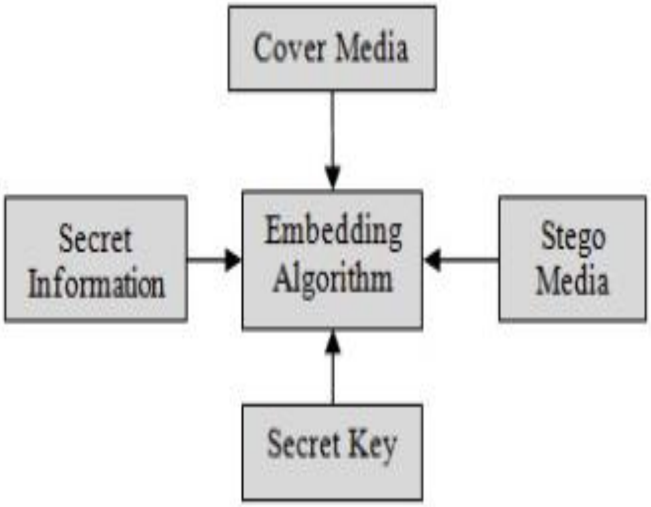

Fig 2: Steganography Process

2.1 Steganography in Digital Mediums

Based on the sort of cover object there are numerous appropriate steganographic schemes that are pursued so as to achieve protection.

i) Image Steganography

In steganography taking the cover object as picture is recognized as image steganography. Generally, in this system pixel intensity is utilized to conceal the information.

ii) Network Steganography

Once getting cover object like network protocol, for instance IP, ICMP, UDP TCP, *etc.*, where protocols are utilized as transporter, is recognized as network steganography. In the OSI model secret channels are present where steganography may be obtained in idle header bits of TCP/IP model [5].

iii) Video Steganography

It is a process to cover up any type of information into digital video form. Video is utilized as transporter for concealed information. Traditionally DCT regulate values (8.667 to 9) that is utilized to conceal the information in every image within video that is not visible through eye. This steganography uses AVI, MPEG, Mp4, H.264, or other video formats.

iv) Audio Steganography

Once getting audio as a transporter for concealing information it is named audio steganography. It has turn into extremely essential medium owing to voice over IP (VOIP). It uses audio formats for example MPEG, WAVE, AVI or MIDI *etc.*

v) Text Steganography

Universal scheme in this steganography, for instance capital letters, numeral tabs, white spaces, as Morse code [6] *etc.* are utilized to get concealed information.

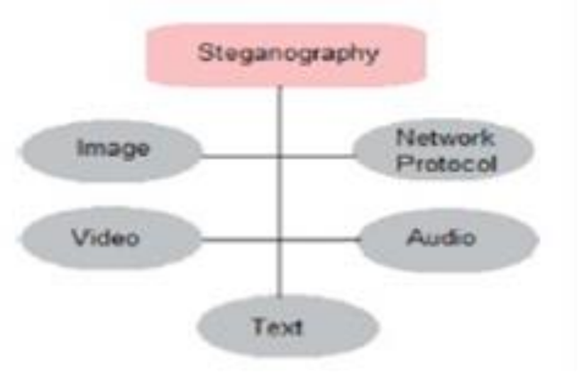

Fig 3: Digital Medium to achieve Steganography

2.2 Image Steganography Terminologies

These are as follows

- **Cover-Image**: Actual picture which is utilized as transporter for concealed information.
- **Message**: real information that is utilized to conceal into pictures. Message can be a simple text or some other image.
- **Stego-Image:** later than embedding messages into cover images is identified as stego-image.
- **Stego-Key:** key is utilized for extracting or embedding the message from cover and stego image.

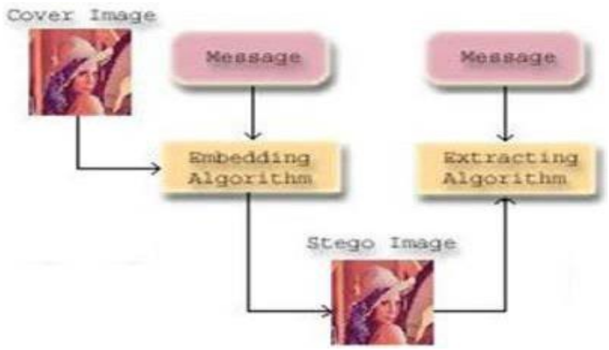

Fig 4: Image Steganography

Usually image steganography is technique of concealing information into cover-image and produces a stego-image. This stego-image forwarded to the other party by well-known medium, where the intermediary does not know that stego-image has concealed message. Hidden message can basically take out with or without stego-key (based on embedding algorithm) through the receivers. Basic graph of image steganography is illustrated in Figure 2 without stego-key, where embedding algorithm needed cover image with message for embedding process. Stego-image is the outcome of embedding algorithm which basically sends to extracting algorithm, where this algorithm unhides messages from stego-images.

2.3 Image Steganography Classifications

Usually this steganography is classified in following [7].

a. **High Capacity**: Maximum size of information can be inserted into image.

b. **Perceptual Transparency**: Later than concealing procedure into cover image, this feature will be tainted into stego-image as contrast to cover-image.

c. **Robustness**: Once embedding, data must reside unharmed if stego-image departs into an amount of transformations for example filtering, scaling, cropping and accumulation of noise.

d. **Tamper Resistance***:* It must be hard to change the message formerly it has been embedded into stego- image.

e. **Computation Complexity**: How much exclusive it is calculation for extracting and embedding a concealed message?

2.4 Cryptography

Cryptography comes as of a Greek word which means concealed or secret script for secure communication in attendance of 3rd parties or the Un-authorized persons. Cryptography actually hides the information from illegal sources. Earlier forms of secret writing are classic cryptography, cipher texts. Cipher machine was also introduced by French but with the development of latest computers much more complex ciphers were developed and they encrypt data of any kind, whether it's binary format, plaintext or the hexadecimal data. Modern cryptography is mixture of arithmetical theory and CS. In today's era, technology has entered into new world of advancements and with this change modern applications of cryptography were also introduced; these are ATM cards, computer passwords, and the electronic commerce.

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is an art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information.

Two basic terms used in cryptography are encryption and decryption; encryption is the process of converting plain text into cipher text and decryption is the reverse process of encryption. Plain text is the text having the actual message or data which is not encrypted and cipher text is the text after encryption of message or data which is ready to be shared [8]. A key is needed for both encryption and decryption of the message.

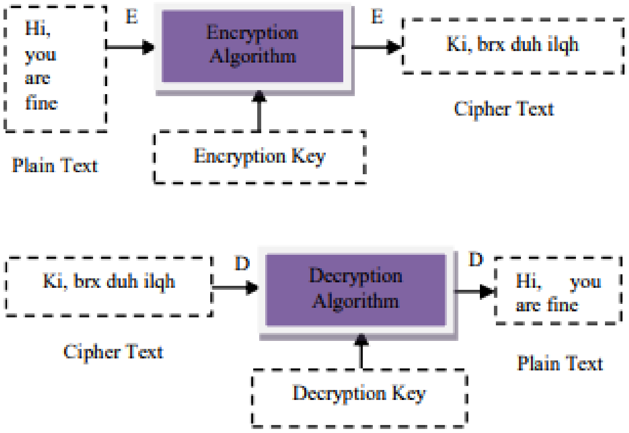

Fig 5: Basic Model of Cryptography

3. Applications

Few applications of the steganography are [9]:

- Defense Organizations: Security from enemies
- Intelligence Agencies: Security of person's private information
- Government Agencies: Store critical data like criminal record
- Smart Identity Cards: Personal information is embedded into photo
- Medical: Patient's details are embedded within image

4. Steganography Technique

1. Spatial Domain Methods: In this approach the secret data are embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories:
   1) Least significant bit (LSB)
   2) Pixel value differencing (PVD)
   3) Edges based data embedding method (EBE)
   4) Random pixel embedding method(RPE)
   5) Mapping pixel to have hidden data method
   6) Labelling or connectivity method
   7) Pixel intensity based.
      a) LSB: this method is most commonly used for hiding data. The image received after embedding is almost the same as the original image because the change in the LSB of image pixel does not bring too much differences in the image.
      b) BPCP: In this part of the image are used by measuring its complex difficulty. Complex difficulty is used to decide the noisy block.
      c) PVD: In this method, two consecutive pixels are selected for embedding the data. The payload is decided by checking difference between two pixels and it serves as a basis for identifying whether the two pixels belongs to an edge area or smooth area.
2. Spread Spectrum Technique: Spread spectrum concept is used in this method. In this technique the private data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it's become difficult to findout the present of data. Even if parts of the data are seperate from several bands, there would be still enough information is available in other bands to recover the data. Thus, it is difficult to remove the data completely without entirely destroying the cover. It is a very robust technique mostly used in military communication.
3. Statistical Technique: In this approach information is embedded through changing various cover image properties. It concludes the cover image splitting into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one, otherwise no modification is required.
4. Transform Domain Technique: Different algorithms and transformations are used on image to secrete information in it.
5. Distortion approach: In this approach secret information is stored through signal distorting. A modification sequence is using to cover through encoder. The decoder calculates varies between the original cover and distorted cover to detect the sequence of the modifications and as a result recover the secret message.
6. Masking and Filtering: These techniques hide the message by marking an image. Steganography only hides the message where as watermarks become a potion of the image. These techniques fix the information in the more significant areas rather than hiding it into the noise level. Watermarking method can using without the image destruction fear because of lossy compression as they are additional integrated into image. This approach is basically used for 24-bit and gray scale images [10].

5. Literature Survey

Rupesh Gupta and Tanu Preet Singh [11] presents about Since the rise of usage of internet in the world security is becoming the major concern all over. So making this thing clear in mind developers are continuously working to make internet a safe environment for all the users. numerous algorithm or techniques are proposed and they work but as intruders be the stage smartly to hack the information developers are too supposed to discover new techniques to stop hacker's intentions. As per basic knowledge extra is PSNR value and smaller is MSE results are improved so, here in this thesis we are proposing a new technique by combing 3 major safety techniques so as to is cryptography, stegnography and watermarking so as to will not only conceal the information but create better outcome for MSE. PSNR and the Embedding ability still following sound attack. The purpose this paper is to provide a new technique that will provide better security for hiding data in an image and watermarked video.

Souvik Roy and P.Venkateswaran [12] presents about A rapid increase in E-Commerce marketplace is seen in new time all the way through world. With forever increasing popularity of the online shopping, Debit or the Credit card fraud and the personal information safety are main concerns for customers, and banks specifically in case of CNP known to be (Card Not Present). This presents a novel approach for provided that limited information merely that is necessary for fund remove throughout online shopping in that way safeguarding customer data and the increasing customer confidence and prevent individuality theft. The way uses joint application of steganography and the visual cryptography for this reason.

Ramadhan J. Mstafa *et al.* [13] Over the past few decades, the art ofzz secretly embedding and communicating digital data has gained enormous attention because of the technological development in both digital contents and communication. The imperceptibility, hiding capacity, and toughness next to attacks are 3 main necessities that some video steganography way should get into thought. In this, a tough and protected video steganographic algo inside the DWT and DCT domain names is to be based on Multiple Object Tracking known as MOT algo and Error Correcting Codes this is called (ECC) is being proposed. Primarily, motion-based MOT algorithm be implemented resting on host videos to differentiate the regions of attention in moving objects. After that, the process of data hiding is being performed by concealing top secret message into DWT and DCT coefficients of each and every motion regions in video depending on center masks. Our experimental outcome exemplify that suggested algo not only improves capacity of embedding and imperceptibility although it also enhances its safety and robustness by encoding the secret message and withstanding against various attacks.

Alavi Kunhu *et al.* [14] In this paper, we recommend a new blind color video watermarking way for copyright safety of multimedia color films through the use of index mapping concept. The inventiveness in obtainable approach consists in crafty a hybrid Discrete Wavelet Transform (DWT) and Discrete Cosine Transform also recognized as (DCT) based distortion caused all the way through watermarking be assess by way of peak signal to sound ratio (PSNR) along with correspondence structure index measure (SSIM) and robustness within antagonism to different types of attacks have been assessed using StirMark. The proposed video watermarking algo provide improved imperceptibility within harmony by way of human visual system and offers advanced toughness in opposition to signal processing attacks.

Ch.Sathi Raju *et al.* [15] Compression is serious trouble in applications of capsule endoscopy. In this paper hybrid DCT compression method and DWT compression method is being employed to capitalize advantages of together techniques. The approach entails in generating shade statistics of the white band and slender band pictures in an intermediate layout and then generating the decompressed image. The quality of decompressed image is being evaluated in conditions of mean square error (MSE), signal to noise ratio known as (SNR) and PSNR.

N.V.Lalitha *et al.* [16] steganography is method of embedding information into signal in a technique that is complex to remove here, a dynamic capacity of audio watermarking system is used to establish data and take away them via singular value decomposition also known as (SVD). With help of SVD based algor and by income of lifting wavelet transform recognized as (LWT), discrete cosine transform (DCT) and DWT. DCT-SVD, DWT-SVD, DWT-DCT-SVD, LWT-DCTSVD methods are developed. It be observed so as to by growing the quantization levels signal-to-noise ratio (SNR) value decreases exponentially which leads to deformation in the original signal. It is moreover observed with the aim of robustness is also greater than before by applying dissimilar malicious attacks like resampling, echo addition, cropping, additive white gaussian noise (AWGN), and signal subtraction to enclosed signal with the aim of doesn’t perturb novel signal and mine image.

Ammad Ul Isla *et al.* [17] in this paper the rapid development of data communication in modern era demands secure exchange of information. Steganography is recognized way intended for hiding information as of unauthorised access. Invisibility, capacity of payload, and PSNR security and toughness are key challenges to steganography. In this, an original image stegnography way based on majority significant bits (MSB) of pixels is proposed. Bit No. 5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. Five and 6 is dissimilar from mystery facts bit then the fee of bit no. Five is modified. The consequences state that the proposed technique ensures sizable enhancements in sign to noise ratio. Usually, hackers focus on the LSB bits for top secret data mining but proposed method utilizes MSB bits that create it more protected from illegal access. Furthermore, the offered approach is not simplest relaxed, however computationally green as properly.

Vidhya P.M, *et al.* [18] encrypted in Malayalam text with custom UNICODE values generated for the Malayalam text. The comparative proposed technique study against an existing approach revealed that, proposed steganography methods are more precise in the encoding process and in the decoding process. The method achieved a precision rate of .95 and the decoding rate of .81.

Milia Habib *et al.* [19] DCT steganography technique is proposed. It is permitting hiding a secret image in another image randomly using Chaos. The chaotic generator Peace Wise Linear Chaotic Map PWLCM with perturbation was selected; it has good chaotic properties and simply execution. It enhances the LSB-DCT technique with threshold.

Yugeshwari Kakde *et al.* [20] Working on audiovideo steganography, which is combination of Image and Audio steganography, in this the author is applying computer forensics approach for authentication purpose. In this paper main focus is to hide secret data behind audio and image of a video file. As we know that video is the combination of many still frames of images and audio.

Kamaldeep Joshi, *et al.* [21] Steganography and cryptography are used to the hide messages and its meaning respectively. Message (encrypted) is embedded inside an image applying new image steganography approach i.e. LSB with Shifting (LSB-S).

Sayantari Ghosh, *et al.* [22] a Hilbert curve based technique to embed information in an image using the neuro psychological behavior of the human vision system which is robust to different attacks like cropping, scratching, additive noise etc.

Avinash Tyagi *et al.* [23] The proposed algorithm hides secret information in cover image by manipulating the difference or sum of the non-overlapping blocks of two consecutive pixels. This approach is an enhancement over Wu and Tsai’s PVD technique that is totally based on pixel value differencing

In Ifra Bilal, *et al.* [24] a survey on latest audio steganographic technique is carried out along with their strength and weakness. Also, comparison between numerous steganographic technique based on robustness is carried out. Another contribution of this paper is evaluation of performance of various reviewed steganography techniques.

6. Propose Methodology

DES-RSA hybrid cryptography is used alongside LSB photograph steganography. The proposed scheme is implemented in MATLAB platform the use of preferred cryptography and steganography set of regulations. Select an genuine photograph. Apply canny aspect detection on unique photo. Encrypt and cover textual content rub down using RSA and DES. Open encrypted massage. Decrypt textual content using RSA & DES. Calculate PSNR and MSE. Figure 6. Shows the working of proposed statistics protection scheme.

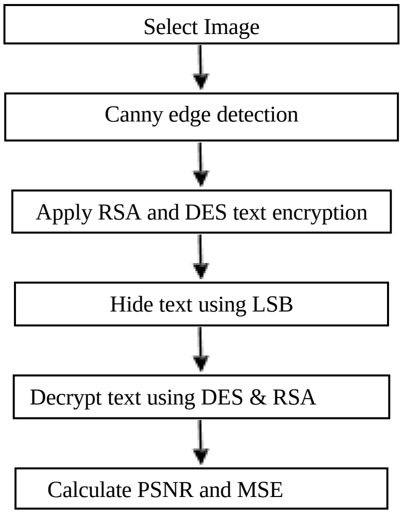

Fig 6: Flowchart on Propose Methodology

Table 1: Comparison of Steganography Technique [25]

Image Steganography Techniques	Description	Advantage
Extensionof LSB (Least significant bit)	Compression algorithm is used to maximize storage capacity	Robust and efficient for hiding text and works efficiently for bmp images.
Hash-LSB	Uses a hash function to generate a pattern for hiding data bits in LSB.	Hash-LSB with RSA increases the security of secret message
LSB and DCT (Discrete Cosine Transform)	Comparative Analysis of two techniques based on security, PSNR	Peak signal to noise ratio is improved using LSB but security wise DCT is best
Modified LSB	Hides the secret message based on searching about identical bits.	More efficient, simple, Appropriate and accurate.
Combinations of LSB	Hiding the data in LSB bit pairs of pixels and comparison between two bit pairs.	Less visible to human eye that is quality of image is better.
LSB with compression technique	Preprocess data is embedded into the LSBs of the pixels.	High image embedding capacity, sufficient payload and high security
IWT(Integer Wavelet Transform)	Hide multiple secret images and keys in cover image.	High quality of the stego image and having high PSNR values.

7. Conclusion

image steganography is a technique designed to secure a via hiding that message inside every other item so that it can be saved secret from all and sundry except the intended recipient. Seganography is the process of hiding or embedding an imperceptible signal (data) into the given signal (data). In the proposed method the strength of DES-RSA hybrid increase the level of security as compared to the existing technique where only DES is used. With the fast growth of digital era and internet, steganography has incredibly advanced masses in a beyond few years. Steganography, mainly shared with the cryptography is a stronger tool which permits replacing records secretly. It will take a look at the information of the attacker about every cryptography and steganography.

8. References

1. Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth. Review Paper on Image Steganography International Journal of Advanced Research in Computer Science and Software Engineering. 2016, 6(6). ISSN: 2277-128X.
2. Mehdi Hussain, Mureed Hussain. A Survey of Image Steganography Techniques. International Journal of Advanced Science and Technology, 2013.
3. Hemang A, Prajapati1, Dr. Nehal G Chitaliya. Secured and Robust Dual Image Steganography: A Survey, International Journal of Innovative Research in Computer and Communication Engineering, 2015.
4. Kedar Nath Choudry, Aakash Wanjari. A Survey Paper on Video Steganography, (IJCSIT), 2015.
5. Handel T, Sandford M. Hiding data in the OSI network model, Proceedings of the 1st International Workshop on Information Hiding, 1996.
6. Johnson N, Jajodia S. Exploring steganography: seeing the unseen, IEEE Computer, 1998, 26-34.
7. Lin E, Delp E. A Review of Data Hiding in Digital Images. Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference (PICS'99), Savannah, Georgia, 199, 25-28.
8. Md. Khalid Imam Rahmani, Kamiya Arora2, Naina Pal, A Crypto- Steganography: A Survey. (IJACSA) International Journal of Advanced Computer Science and Applications, 2014; 5(7).
9. Hemang A Prajapati, Dr. Nehal G Chitaliya. Secured and Robust Dual Image Steganography: A Survey. IJIRCCE, 2015, 3.
10. Hui Tian, Jie Qin, Yongfeng Huang, Yonghong Chen, Tian Wang, Jin Liu, *et al*. Optimal matrix embedding for Voice-over-IP steganography College of Computer

Science and Technology, National Huaqiao University, ELSEVIER, 2015.

11. Himani Trivedi, Arpit Rana. A Study Paper on Video Based Steganography, IJARIIT © 2017 All Rights Reserved. [12] Ammad UI Islam *et al*, An Improved Image Steganography Technique based on MSB using Bit Differencing, 978-1-5090-2000-3/16/$31.00 IEEE © 2016.
12. Ramadhan J, Mstafa1, Khaled M. Elleithy1 and Eman Abdelfattah2, A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC, 2169-3536(c)2016 IEEE.
13. Alavi Kunhu, Nisi K, Sadeena Sabnam, Majida A, Saeed AL-Mansoori. Index Mapping based Hybrid DWT-DCT Watermarking Technique for Copyright Protection of Videos Files, 978-1-5090-4556-3/16/$31.00©2016 IEEE.
14. Ch. Sathi Raju, DV Rama Koti Reddy. On Compression Characteristics of White Band and Narrow Band Images Using Hybrid DCT and DWT, 978-1-4788-7225-8/15/$31.00©2015 IEEE.
15. NV Lalitha, Vara Prasad P, UmaMaheshwar Rao S, UmaMaheshwar Rao S. Performance Analysis of DCT and DWT Audio Watermarking based on SVD, 978-1-5090-1277-0/16/$31.00 ©2016 IEEE
16. Ammad Ul Islam1, Faiza Khalid2, Mohsin Shah2, Zakir Khan2, Toqeer Mahmood3, Adnan Khan2, Usman Ali2, Muhammad Naeem4. An Improved Image Steganography Technique based on MSB using Bit Differencing, 978-1-5090-2000-3/16/$31.00 ©2016 IEEE.
17. Vidhya PM, Varghese Paulb. A Method for Text Steganography Using Malayalam Text, 2014; 28.
18. Milia Habib, Bassem Bakhache, Dalia Battikh, Safwan El Assad. Enhancement using chaos of a Steganography method in DCT domain, IEEE, 2015.
19. Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale. Audio-Video steganography IEEE, 2015.
20. Kamaldeep Joshi, Rajkumar Yadav. A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication IEEE, 2015.
21. Sayantari Ghosh, Saumik Bhattacharya Amity University, Kolkata WB, India Hilbert Curve Based Steganographic Scheme for Large Data Hiding, IEEE, 2015.
22. Avinash Tyagi, Ratnakirti Roy, Suvamoy Changder, High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum IEEE, 2015.
23. Soon-Nyean Cheong, Huo-Chong Ling, Pei-Lee The. Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system ELSEVIER, 2014.
24. Divyanshu Triapthi1, Yash Kumar Singh2, Rohit Singh. A Review on Digital Image Steganography with its Techniques and Model. IJSART. 2016; 2(4).ISSN [ONLINE]: 2395-1052.