Evaluation of Best Steganography Tool using Image Features

Jensi Lakdawala[1], Jiya Rankawat[2]

[1,2]*Integrated M.Sc. (IT), UKA Tarsadia University, Bardoli, Gujarat, India*

Abstract—Steganography is technique of hiding a data under cover media using different steganography tools. Image steganography is hiding of data (Text/Image/Audio/Video) under a cover as Image. This review paper presents classification of image steganography and the comparison of various Image steganography tools using different image formats. The attainment of this study is to identify the reliable and best tool available in the market for Steganography. Analysing numerous tools on the basis of Image features and extracting the best one is the main goal of this paper..

Keywords—*Information hiding, Cryptography, Steganography, Steganography tools.*

I. INTRODUCTION

A. *Steganography*

In this modern era, where technology is growing rapidly with new developments, security has become the priority for every technology and individual. The data needs to be kept safe and secure so that only the authorised members/organisation could access it and any unauthorised members/organisation gain no access to that data. Every second thousands of data get transmitted on Internet from one place to another, which increases the amount of data sharing. The prime concern of sender is to protect the data sent in a correct and secret way that only the receiver should be able to understand the message received.

Till now the most essential techniques for data security are Cryptography and Steganography. Initially cryptography was developed to encrypt the message in another message in a hidden way such that only the sender and receiver knew the way to decrypt it. To decode the hidden message a cryptography key was used which only authorised person knew. One of the major drawbacks of cryptography was that even the person not involved in the exchange knows that the message contains some hidden information, which increases the probability of unauthorised decoding of secret message. Thus to overcome this limitation steganography technique was introduced.

The word "steganography" belongs to "Greek" language. In Greek the steganography stands for "covered writing". Steganography is basically the art of secretly hiding data or message in any cover medium such as an image, audio or video. Steganography has an advantage over cryptography, as now the third person does not come to know whether data is hidden or not. The authorised user could only decrypt the data, as no other person would come to know about the hidden message. The invention of steganography has improved data security and reliability of data transmission as no third person could change the data.

B. *History Of Steganography*

Steganographic techniques are one of the ancient techniques which has been widely used in historical times, especially before cryptographic systems were developed. The first known method of steganography is from the ancient Greek times, when mediator tattooed messages on their shaved heads and then let their hair grow so the message remained unseen. At that time, a wax table is also used as a cover source in which text was written on the wood and the message to be hiding was covered with a new wax layer.

During World War II invisible ink was used to hide information on pieces of paper, which appeared as a blank pieces of paper to the average person. Liquids such as urine, milk, vinegar and fruit juices were used, as when each one of these substances is heated they darken and become visible to the human eye.

"Ave Maria" cipher was another clever invention in Steganography. The book contains a series of tables, each of which has a list of words, one per letter. To code a message, the message letters are replaced by the corresponding words. If the tables are used in order, one table per letter, then the coded message will appear to be an innocent prayer.

All of these approaches to hide message with steganography technique have one thing in common: They hide the secret message in the physical object, which is the sent to the receiver of the data. The cover message is merely a distraction to a third person, and thus it could be anything in any form. Nevertheless, there are plenty of room to hide secret information, which seem to be not-so-secret message in original data.

C. *Application of Steganography*

Steganography is having various applications amongst them few are listed follow:

1. Feature Tagging
2. Copyright Protection
3. Medical
4. Secret Communication

5. Use by terrorists
6. Digital Watermarking

II. CLASSIFICATION OF STEGANOGRAPHY

Secret information can be hide and send inside all sorts of cover medium. The bellow formula provides a universal description of the pieces of the steganographic process:

Here, "Cover Medium" is used as a hidden file, which will hide the "Hidden Data" inside it. It may also be encrypted using the "Stego Key" for providing more security to the hidden data. And thus "Stego Medium" is the resultant files, which will be, send to the receiver.

There are four ways to implement steganography:

1. Using text.
2. Using images.

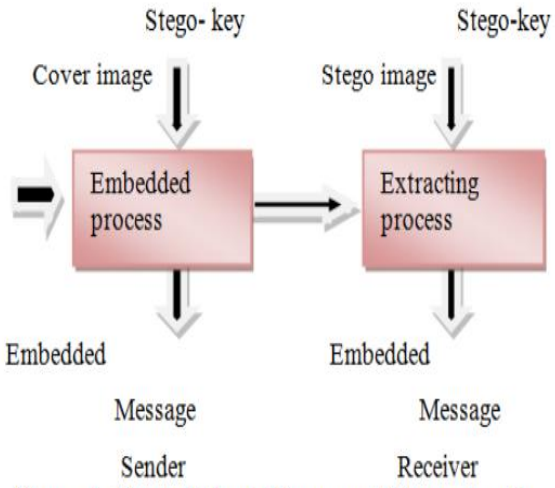

Figure 1: General Block Diagram of Steganography

3. Using audio files.
4. Using video files

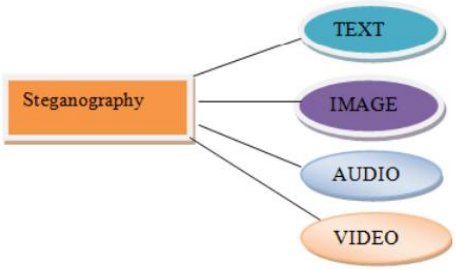

Figure 2: Steganographic Media

A. *Text Steganography*

Text steganography can be classified in three basic categories:

1. *Format Based*

- Hide Information in physical text formatting of text.
- *Modifies existing text in order to hide steganographic text.*
- *Formats like insertion of spaces, deliberate misspellings, resizing the fonts, etc. are used to hide information in text steganography.*
- *Only human eyes can detects those textual changes but it cannot trick to computer system easily.*

2. *Random and statistical generation*

- Generates cover text on the basics of statistical properties.
- Based on Character Sequences and Words Sequences.
- Information hidden based on character sequence will embedded it in to random sequence of characters which will appear random to third person who try to intercepts it.
- In order to create "words", Word sequence takes statistical properties of word-length and letter frequency, which will appear to have the same statistical properties as actual words in a given language.

3. *Linguistic method*

- Considers the linguistic properties of generated and modified text.
- Frequently uses linguistic structure as a place for hidden messages.
- Also, Steganographic data can be hidden within the syntactic structure itself.

B. *Image Steganography*

In Today's world, Image Steganography is the most widely used technique for hiding the secret messages into a digital image. Human visual system (HVS) cannot detect the variation in luminance of color vectors at collection of color pixels, thus Image steganography exploits the advantage of HVS. The optical higher frequency side of the visual spectrum represents individual pixels of an image. A picture can have features like brightness, contrast,

Chroma, pixel values, size of an image, etc. Each pixel of an image can be digitally valued in terms of 1s and 0s.

For example:

A 24-bit bitmap will have 8 bits, representing each of the three-color values (red, green, and blue) at each pixel. If we consider just the red color there will be n-no of different shades of red in an image. The difference between 11111111 and 11111110 in the value for red intensity is likely to be undetectable by the human eye. Hence, Least Significant Bit (LSB) can be used for something else other than color information when terminal recipient of the data is nothing but human visual system (HVS).

C. Audio Steganography

Audio steganography had taken the advantages of the psychoacoustic masking phenomenon of the human auditory system [HAS]. Psychoacoustic or auditory masking property renders a weak tone imperceptible which arises because of the low differential range of the HAS even though the dynamic range covers 80 dB below ambient level. Frequency masking occurs when human ear cannot perceive low power level frequencies, if they are present in the vicinity of tone- or noise-like frequencies at higher level.

Additionally, if the tone occurs within a critical band, a weak pure tone is masked by wide-band noise. This inaudibility of weaker sounds property is used in different ways for embedding information.

In audio steganography, digitized audio signal is used to embed secret message which result in slight altering of binary sequence of the corresponding audio file. The list of methods that are commonly used for audio steganography are listed and discussed below.

1. LSB coding
2. Spread spectrum
3. Parity coding
4. Echo hiding
5. Phase coding

D. Video Steganography

Video files are generally a collection of images and sounds, so the presented techniques, which apply on images and audio, can be applied on video files as well. Usually, the DCT (Discrete Cosine Transform) method is used for hiding information inside a video. DCT works by slightly changing each of the images in the video, which is rarely noticeable by the human eye. Precisely, DCT alters values of certain parts of the images, it usually rounds them up. For example, if part of an image has a value of 7.697 it will round it up to 8.

The major advantages of video steganography are that the large amount of data can be hidden inside in a moving stream of images and sounds. Therefore, continuous flow of information doesn't let human to notice the distortions.

III. IMAGE STEGANOGRAPHY(DOMAIN & ITS TECHNIQUES)

Images are the most popular files for hiding data. Image Steganography is the process of sharing secret or confidential data within an image. Secret message (payload) is set in the image and is passed to the sender. The sender can then extract the information from stego image using the key provided by the sender.

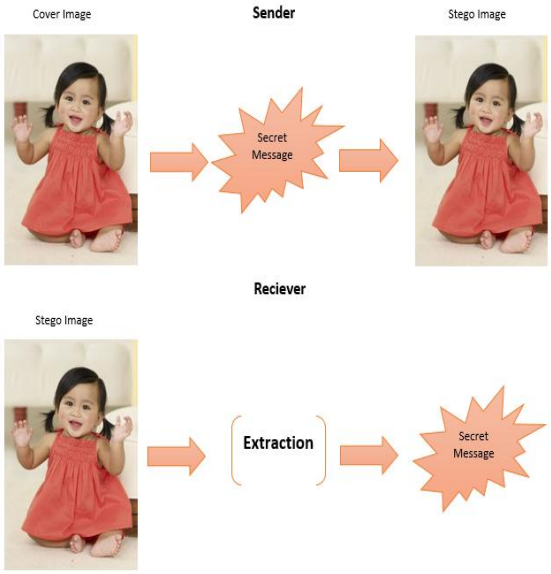

Figure 3: Image Steganography Process [28]

Image Steganography Domain and Its Technique are:

A. Spatial Domain
B. Frequency Domain
C. Masking and Filtering Domain

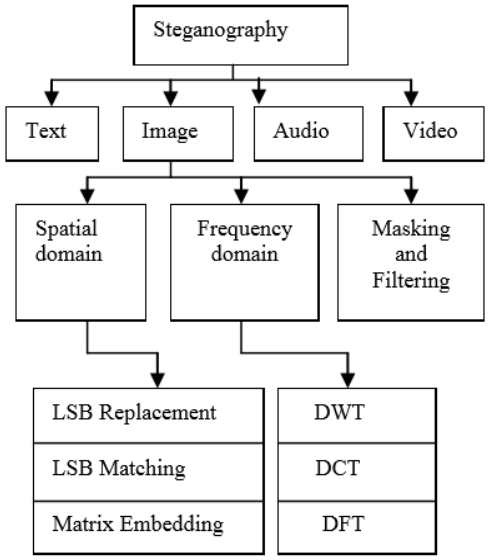

Figure 4: Classification of Image Steganography [28]

A. Spatial Domain Steganography

Spatial Domain Steganography uses Least Significant Bits for encoding the data. LSB insertion method is a frequently used method for embedding data into the original image. All the versions of this method alter some of the bits in the values of image pixels for hiding data. LSB dependent steganography hides confidential messages in the LSBs of some pixel values without any noticeable alterations. Human eye cannot be able to notice variations in the LSB. Embedding of data bits can be carried out either simply or randomly.

1. LSB Replacement

In this steganography, the cover pixel LSBs is substituted with a bit of the message that has to be embedded. The message is transformed into a sequence of bits before embedding, which are then inserted sequentially where the LSBs are located. This steganography is detectable even if there is low embedding rate.

Advantages of the LSB method are:

- Original image cannot be easily Degraded.
- Higher hiding capacity.

Disadvantages of LSB method are:

- Low robustness.
- Embedded data can be destroyed by simple attacks.

2. LSB Matching

LSB Matching is much improved over LSB replacement method. In this process pixel are randomly summed up or subtracted from the value of the cover pixel. As compared to LSB Replacement method it is hard to detect LSB matching.

3. Matrix Embedding

Matrix Embedding encodes the originalimage and the message by an error correction code. It alters the original image with respect to the result of coding. The possible message bits are embedded randomly, thus it helps in increasing embedding efficiency.

B. Frequency Domain Steganography

Frequency Domain Technique is one of the most complex ways of hiding information in an image. To hide the secret information within an image different algorithms and transformations are used. Transform domain is used as one of the strong steganographic system. Transform domain technique hides information in regions of the image that is less exposed to cropping, compression and image processing, whichbecome advantage over spatial domain. Some transform domain techniques may not be dependent on the image format and they may result in lossless and Lossy format conversions.

1. DWT (Discrete Wavelet Transformation)

DWT is the functions that are obtained over a fixed interval and have zero as an average value. DWT is used for signal investigation as well as image processing. It crumbles a signal into a number of constituents in frequency domain. Single Level Decomposition segments a cover image further into two major segments: approximate component and detailed component. Two Level Decomposition is used to segment a cover image into mainly four sub components: approximate component (LL), LH, HL, HH.

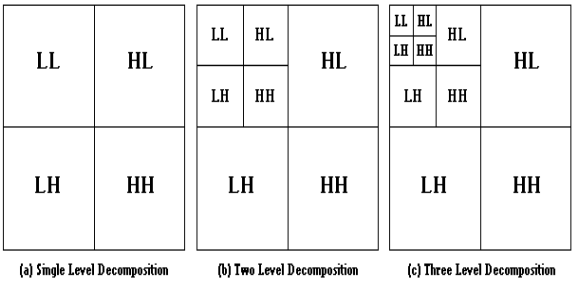

Figure 5: Discrete Wavelet Transformation Image Compression Level [28]

2. DCT (Discrete Cosine Transformation)

DCT separates an image into different parts of differing significance (which is associated with the image's quality). Fourier Transform Technique has been resembles, as it converts an image from its spatial domain into frequency domain. DCT technique the JPEG format of image makes use of cosine transform to convert consecutive pixel blocks of size 8 x 8 into a count of 64 cosine coefficients each for every color constituent.

3. DFT (Discrete Fourier Transformation)

DFT is important as it separates an image into mathematical values. It converts into the frequency-based information from space and time dependent information. DFT useful in numerous applications including image filtering and reconstruction and image compression. It does not include all frequencies that result to form an image but constitutes of only the set of those samples, which are sufficient to describe the original image.

C. Masking and Filtering

These techniques hide the information in the way of paper watermarking. These techniques not just hide the information into the noise level but also in more significant areas of image. The hidden message is more integral to the cover image. Watermarking

techniques can be applied without having the fear of image destruction due to Lossy compression.

Advantages of Masking and filtering Techniques:

- It is more robust than LSB replacement with respect to compression as the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:

- Techniques can be applied only to grey scale images.

IV. STEGANOGRAPHY TOOLS

Till now there are a number of tools available in the market, which are used for embedding of covert data within a cover medium. These tools can be open source, freeware and commercial tools. Bellow section identifies, discuss and compare open source or freeware steganography tools. Some of the tools also have steganalytic properties and functions; however, we discuss them only for data hiding aspects.

A. Silent-eye

- Open source.
- Cross-platform.
- Easy to use application.
- Embed data in images (bmp, jpeg) and audio files (wav).
- Tool offer different steganographic and cryptographic algorithms, which can be used owing to its plug-in support.

B. Image steganography

- Free software for hiding your information (Text, Files, Image) in image files.
- Encoded message will be hidden inside the image.
- You can even decode the hidden file or message from the stego image and obtain the original message out of it.

C. Hide 'N' Send

- It is like small utility, which offers steganography feature.
- Hides any kind of message behind a JPG image file.
- Hashing and Encryption is also supported which add an extra layer of security.

D. Hallucinate

- Small software application that hide sensitive files inside images.
- Deployed on Windows versions that have the Java working environment installed.

E. Quickstego

- Lightweight encryption tool that specifically help to protect sensitive data from unauthorized viewing of hiding text messages in images.
- Offers a clean and straightforward layout, which allows users to upload images easily and quickly.
- Support file formats: BMP, JPG, and GIF, and also lets you enter the text messages into a dedicated area.
- Even user can import data from plain text files.
- Stego images are saved to BMP file format only.

F. Steganofile

- System Utilities software that allow users to hide a file in one or many host files, so its main advantage over all tools stego image is it can not be easily seen by other persons.
- Basically, it attaches the original file to the end of the host file.
- If more than one host file is there to hide, the original file is spitted into the same number of host files.
- Advantage: Each host file size might not increase substantially, so it cannot rise any suspicious.
- More security is added to the file when password is provided to the hidden file, which would encrypt with a basic scheme.

V. BACKGROUND STUDY & LITERATURE REVIEW

The article [1] reviews about the different techniques used in digital steganography and also describing about the implementation of LSB method. It uses LSB insertion in order to encode data into a cover image. And an analysis of the performances is made using images ranging from 1:9 to 131 megapixels.

The paper [2] presents secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Discrete Wavelet Transform (DWT) technique of transform domain has been used to scramble the secret message. And the performance has been investigated by comparing various qualities of the stego image and cover image.

In review paper [3], data hiding is done under JPEG Image by using Quantization Error Table (QET) resulting from processing the DCT image with quantization and DE quantization used for

selecting the position for hiding secret bits in the image.

The stego tools and the comparison of different tools using the image as cover media for the performance measurement. It also introduces a robust and high payload steganographic algorithm mentioned in review paper [4].

The review paper [7] presents about the history steganography with its process comparing with cryptography. It also describes the communication system of these techniques. And also they improve the quality of image by using 12 bits instead of 8 bits.

The information about the Image steganography and the image used to hide the data using some software and analyzing on the metadata of images after data hiding was reviewed in paper [9].

The image Steganography and its detailed description about the techniques used for the same were mentioned in paper [15]. They have analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications.

The Review paper [16] presents the Image Steganography and its Current techniques for hiding the data considering the modern application for communication with the comparison of Steganography, Cryptography and Encryption.

The review paper [18] shows about image steganography, where edges in the cover image have been used to embed messages. It analysis that the more the amount of data to be embedded, larger the use of weaker edges for embedding.

In this paper [20] they provide a critical review of the steganalysis algorithms available to analyze the characteristics of an image, audio or video stego media and the corresponding cover media and understand the process of embedding the information and its detection. Also give a clear picture of the current trends in steganography so that we can develop and improvise appropriate steganalysis algorithms.

VI. COMPARISON OF STEGANOGRAPHY TOOLS

In Table 1, the Steganography tools, which are frequently used for hiding text under cover, image are compared. The information given in this table was thoroughly researched. The table has been listed alphabetically by tool names. The table describes the comparison of tools on the basis of image features like Image size, Dimension, Concealed File and Image Formats with its algorithm applied.

All steganography tools are run with same text (Text message is: ”Hello Friends! We love BMIIT. We believe in “Make it Happen Through Innovations and Values.“ ”) And made a stego image with the help of same image (Figure - 6). The difference between stego image and original image (Figure - 6) is shown in bellow diagram (Figure - 8).

Figure 6: Original Image

Figure - 7 describe about the comparison of original image (Figure – 6) with stego image on the basis of histogram values. The difference can be recognized by change in the frequency of histogram values. The below analysis bring us to the conclusion that “Hide ‘N’ Send” has the major value difference where as “Steganofile” has no visible difference.

Figure - 8 describe about the comparison of original image (Figure – 6) with stego image on the basis of pixel-by-pixel values. The difference can be recognized by the white pixels on the black area. The below analysis bring us to the conclusion that “Hallucinate” has the major pixel difference where as “Steganofile” has no visible difference.

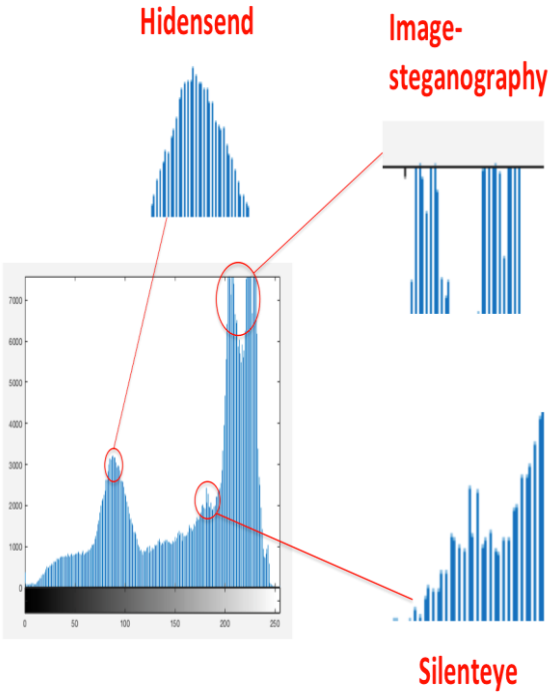

Figure 7: Histogram Differentiation of Original Image & Stego Image

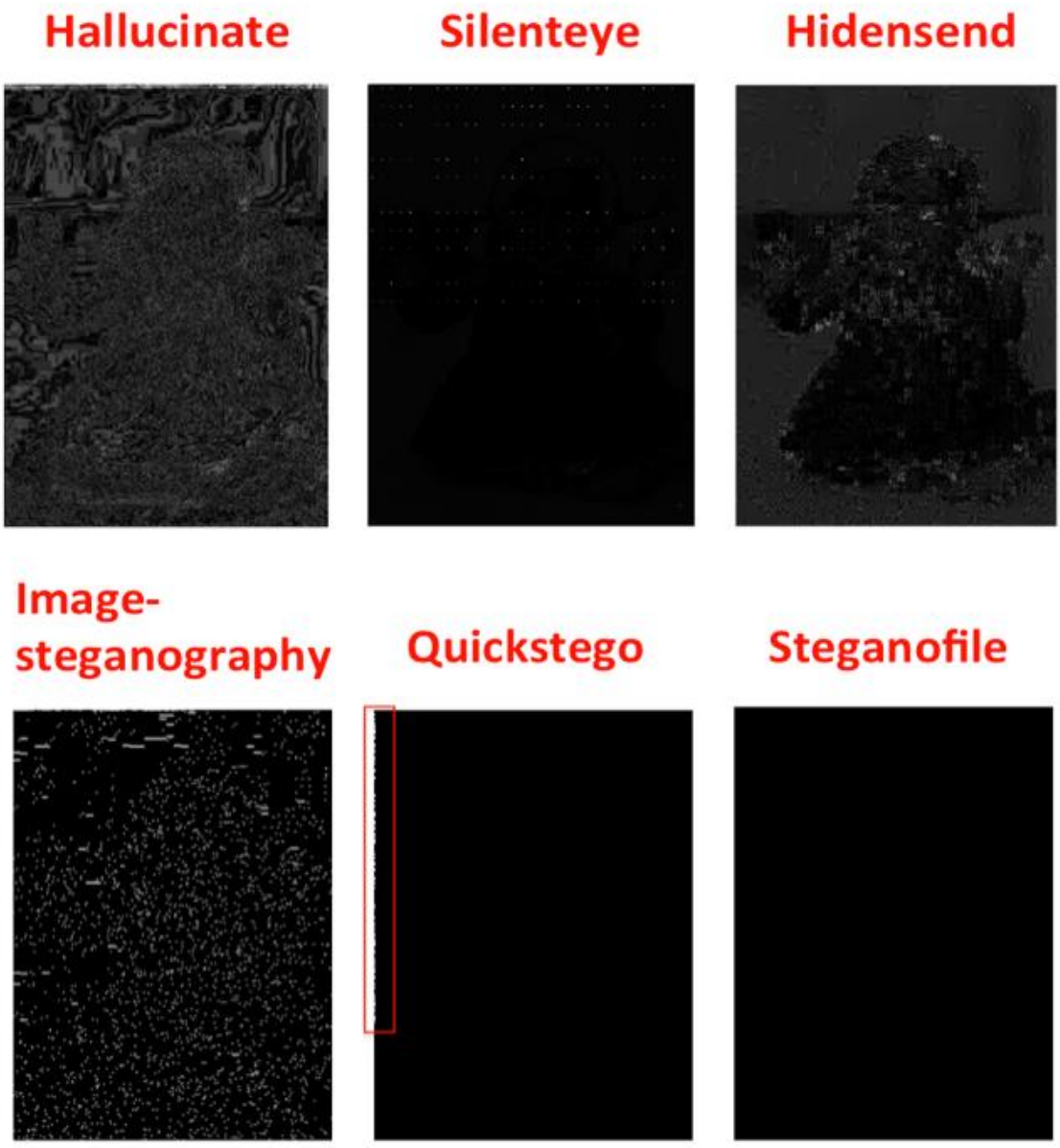

Figure 8: Pixel Value Differentiation of Original Image & Stego Image

Tool Name	Concealed Data Type	Stego Image properties				Additional Information
		Image Size (Increased by)	Dimension (Increased by)	Input Image Files	Output Image Files	
Hallucinate	Any File Type	3 Times	No change	Any	BMP, JPG	-
Hide 'N' Send	Any File Type	1 Times	Increased	Any	JPG	Algorithm used are LSB, FS, M-LSB, M-A and Password Protected
Image steganography	Any File Type	12 Times	No change	Any	PNG	-

Quickstego	Txt File	15 Times	No change	Any	BMP	-
Silenteye	Any File Type	5 times	No change	Any	BMP, JPEG	Algorithm used is LSB, Encryption, Password Protected, Adjustable Quality, Compression, Plugin support
Steganofile	Any	No Change	No change	Any	Any	Password Protected

Table 1: Steganography Tools Comparison

VII. CONCLUSIONS

This research presents a comparative study of some Steganography tools. The attainment of this study is to identify the reliable and best tool available in the market for Steganography. Some of the tools available in the market were selected based on the frequent use; these tools were tested using the same input on all of them. Specific text was embedded within all host images for each of the six Steganography tools selected. The results of the experiment reveal that all the six tools were relatively performing at the same level, though some software performs better than others. Out of all the above Stego tools used for comparison, "Steganofile" (tool) was considered to be the most efficient one. This conclusion of efficiency was based on the image features like size, dimensions, and pixel value and histogram differentiation.

Steganofile has the advantages over all the other tools that it supports all the image formats and does not change the image features as well as does not reflect the visible changes.

VIII. REFERENCES

[1] Monica Adriana Dagadita, Emil-Ioan Slusanschi, & Razvan Dobre, "Data Hiding Using Steganography ", IEEE 12th International Symposium in Parallel and Distributed Computing, pp. 159-166, 2013.

[2] G.Prabakaran & R.Bhavani, "A modified secure digital image steganography based on Discrete Wavelet Transform", IEEE International Conference In Computing, Electronics and Electrical Technologies (ICCEET), pp. 1096-1100, 2012.

[3] D.R. Denslin Brabin, Dr.V.Sadasivam, "QET Based Steganography Technique for JPEG Images", IEEE International Conference on Control, Automation, Communication and Energy Conservation, ISBN 978-1-4244-4789-3, 2009.

[4] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "A Comparative Analysis of Steganographic Tools", School of Computing and Intelligent Systems, Faculty of Engineering University of Ulster. Londonderry, Northern Ireland, United Kingdom.

[5] Ismail Karadogan, Resul Das," An Examination on Information Hiding Tools for Steganography", INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE Resul Das et al., Vol. 3, No.3.

[6] Hamad A. Al-Korbi1, Ali Al-Ataby2, Majid A. Al-Taee3 and Waleed Al-Nuaimy4, "HIGHLY EFFICIENT IMAGE STEGANOGRAPHY USING HAAR DWT FOR HIDING MISCELLANEOUS DATA", Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 2, No. 1, April 2016.

[7] Monika and Er. Mohinder Singh, "A survey on image based steganography framework to enhance quality of payload object", International Journal of Engineering Research and General Science Volume 4, Issue 2, March-April, 2016.

[8] L.Baby Victoria*, Dr.S.Sathappan, "A Study on Spatial Domain and Transform Domain Steganography Techniques used in Image Hiding", INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND CREATIVE ENGINEERING (ISSN: 2045-8711) ,VOL.5 NO.5 MAY 2015.

[9] Don Caeiro1, and Sanjana S2, "Detection of Steganography using Metadata in Jpeg Files", The International Journal of FORENSIC COMPUTER SCIENCE, IJoFCS (2015) 1, 23-28.

[10] D.Venkata Ramana, P.Nageswara Rao, "Steganography Algorithms for Image Security Using LSB Substitution Method", International Journal of Modern Embedded System (IJMES), Volume No.-4, Issue No.-1, February, 2016.

[11] Arnold, M. K., Schmucker, M., & Wolthusen, S.D. (2003). Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Norwood, Massachusetts.

[12] Joachim, J., Eggers, J. & Bernd, G. (2000). Robustness of a blind image watermarking scheme. ICIP 2000, Special Session on WM. Sep. 10–13. Canada.

[13] Stefan, W., Elisa, D. & Gelasca, T. (2002). Perceptual quality assessment for video watermarking. Proceedings of International Conference on Information Technology: Coding and Computing (ITCC). April 8-10. Las Vegas, NV.

[14] Wu, N. (2004). A Study on Data Hiding for Gray-Level and Binary Images. Master Thesis. Chaoyang University of Technology, Taiwan. [5] Bennour J. Dugelay J. L. & Matta, F. (2007). Watermarking Attack: BOWS contest. Proceedings of SPIE.

[15] Mehdi Hussain and Mureed Hussain, "A survey on Image steganography Techniques", International Journal of Advance Science and Technology Vol. 54, May, 2013.

[16] Sakshi Jindal, Navdeep Kaur, "DIGITAL IMAGE STEGANOGRAPHY SURVEY AND ANALYSIS OF CURRENT METHODS", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No3, May-June 2016.

[17] T. Morkel 1 , J.H.P. Eloff 2 , M.S. Olivier 3, "AN OVERVIEW OF IMAGE STEGANOGRAPHY", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science.

[18] Islam, S., Modi, M.R. & Gupta, P. , "Edge-based image steganography", EURASIP Journal on Information Security , December 2014, 2014:8.
[19] Taras Holotyak1, Jessica Fridrich1 , Sviatoslav Voloshynovskiy2, "Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics", Department of Electrical and Computer Engineering, State University of New York at Binghamton, Binghamton, NY, 13902-6000.
[20] Natarajan Meghanathan1 and Lopamudra Nayak2, "STEGANALYSIS ALGORITHMS FOR DETECTING THE HIDDEN INFORMATION IN IMAGE, AUDIO AND VIDEO COVER MEDIA", International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.
[21] Suhad shakir jaber, hilal adnan fadhil, zahereel i. Abdul khalib, rasim azeez kadhim, "SURVEY ON RECENT DIGITAL IMAGE STEGANOGRAPHY TECHNIQUES ", Journal of Theoretical and Applied Information Technology 31st August 2014. Vol. 66 No.3.
[22] Rajesh Kumar Tiwari and Gadadhar Sahoo, "Some New Methodologies for Image Hiding using Steganographic Techniques".
[23] Ms. Tejashree Shinde1, Ms. Ujwala Chaudhari2, Ms. Rushali Bodke3, "Image Steganalysis Based on Statistical Evidance by Using SVM", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014.
[24] Huan Dou, Zhipin Deng, Kebin Jia, "A Fast Macroblock Mode Decision Algorithm for MVC Based on SVM", Dept. of Electronic Information & Control Engineering, Beijing University of Technology, Beijing, Chin.
[25] Sunny Dagar, "Highly randomized image steganography using secret keys", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE) , pp. 1-5, 2014.
[26] K.A. Darabkh, I.F. Jafar, R.T. Al-Zubi, & M. Hawa, "An improved image least significant bit replacement method", IEEE 37th International Convention in Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp 11821186, 2014.
[27] Mohamed Amin, Hatem M. Abdullkader, Hani M. Ibrahem, and Ahmed S. Sakr. "A Steganographic Method Based on DCT and New Quantization Technique". International Journal of Network Security, Vol.16, No.3, PP.214-219, May 2014.
[28] Amandeep Kaur, Rupinder Kaur , Navdeep Kumar , " A Review on Image Steganography Techniques ", International Journal of Computer Applications (0975 – 8887) Volume 123 – No.4, August 2015.
[29] Reddy, H. S. M., & Raja, K. B. (2009). High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security (IJCSS), 3(6), 462-472.
[30] Amrita Khamruia , J K Mandal. "A Genetic Algorithm based Steganography using Discrete Cosine Transformation (GASDCT)". Procedia Technology 105 – 111.
[31] https://www.youtube.com/watch?v=7KSn_nekots
[32] https://www.slideshare.net/IJMER/en2646344638
[33] http://in.mathworks.com/help/images/ref/imshowpair.html
[34] https://www.slideshare.net/PrimaLCarnagE/dct-steg-o-group-1
[35] http://shodhganga.inflibnet.ac.in/bitstream/10603/8912/13/11_chapter%202.pdf
[36] http://www.codeforge.com/s/1/Image-steganography-using-DCT-algorithm-in-MATLAB
[37] http://en.pudn.com/downloads74/sourcecode/crypt/ca/detail267155_en.html
[38] http://read.pudn.com/downloads74/sourcecode/crypt/ca/267155/Steganography/
[39] http://en.pudn.com/downloads74/sourcecode/crypt/ca/detail267155_en.html
[40] https://in.mathworks.com/help/images/image-quality.html
[41] http://softasm.com/matlab-r2016-crack-full-windows-mac/
[42] https://www.searchenginejournal.com/7-similarity-based-image-search-engines/8265/
[43] https://www.searchenginejournal.com/google-neven-vision-image-recognition/3728/
[44] http://www.garykessler.net/library/ndaa_stego.html
[45] http://ws2.binghamton.edu/fridrich/Research/f5.pdf
[46] https://www.slideshare.net/WXavierP/computer-forensics-and-steganography
[47] http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/
[48] https://en.wikipedia.org/wiki/Steganography