ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

SURVIVAL OF STEGANOGRAPHY AGAINST STEGANALYSIS

M. G. Gouthamanaath* & Dr. A. Kangaiammal**

* Full Time Research Scholar, Department of Computer Applications, Government Arts College (Autonomous), Salem, Tamilnadu

** Assistant Professor, Department of Computer Applications, Government Arts College (Autonomous), Salem, Tamilnadu

Cite This Article: M. G. Gouthamanaath & Dr. A. Kangaiammal, "Survival of Steganography Against Steganalysis", International Journal of Computational Research and Development, Special Issue, January, Page Number 55-61, 2017.

Abstract:

Steganalysis is to identify the stego-image with various algorithms and methods associated with that. This paper is a clear exhaustive survey of the survival of steganography methods against steganalysis that is explained with various kinds of steganalysis methods. Based on the properties of steganalysis methods, categorization as well as the problem associated with each of the category is summarized. It is intended to narrate the strength of steganalysis, improvements required to improve it against vast number of steganography techniques.

1. Introduction:

Steganography is an art of hiding the existence of secret information in any digital media. Secret communication techniques lead to breach in national cyber laws [1]. To overcome this issue steganalysis was introduced to find the existence of the secret information in the images. Even though lot of steganalysis methods developed in short span of time, there are lot of new techniques required to make a full-fledged system to find the existence as well as retrieval of secret information in it. Today most of the digital data are transferred through internet. It is tedious to find the existence of the secret information through general image analysis [5]. There are several image steganography methods, generally classified as spatial as well as transform domain depicted in Figure 1. The pixel values are modified and the secret information is stored according to the modification on the basis of spatial domain, whereas in transform domain pixel values are converted to transform coefficients and then the modification made among the transform coefficients and it is again converted to pixel values with less modification depicted in Figure 2 and 3. Most of the spatial domain methods are changing the Least Significant Bit of pixel values and in extraction phase it is identified by the other algorithm. Discrete Cosine Transform and Discrete Wavelet Transform are the most common steganography methods in transform domain [33]. Most of the steganalysis methods have a percentage wise detection among stego-image which trails different kinds of techniques [32].

2. Steganography Methods:

There are number of image steganography methods, generally classified as spatial and transform domain presented in Figure 1.

2.1 Spatial Domain Methods: The pixel values are directly modified in spatial domain methods. Recovery of secret message depends on the modification among the cover image. Two kinds of spatial domain methods available as per recovery of secret information. Recovering the data by comparing the stego-image with cover image is the first kind. Another kind of methods that recover information without having the original cover in destination. Spatial domain methods are known for its capability to hide high quantity of secret information.

2.1.1 LSB and MSB Embedding Method: Embedding the secret data in the LSB of pixel with some relevant techniques to retrieve the data in destination. It is most common and easy to implement it in images with simple algorithms. LSB embedding methods implemented with single and multiple biplanes [3]. A bitmap image is used as cover image for embedding the secret message bits with AES cryptography and also for filtering noise, it uses Most Significant Bit method [23]. To avoid the changes made among sensitive pixels leads to suspicion by steganalysis, LSB++ method was introduced instead of LSB+ [16].LSB embedding steganography methods are applied in basic level steganography applications. This method becomes powerful when the imperceptibility of the secret information is maintained.

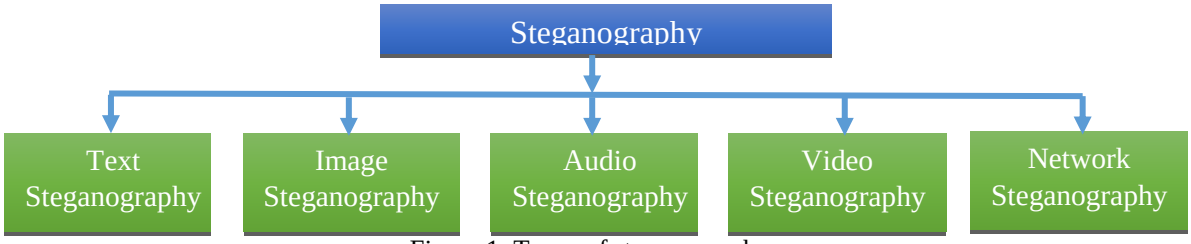

Figure 1: Types of steganography

2.1.2 LSB Inversion Technique: Secret message is converted as binary bits. The binary bits are embedded by inverting the binary values of the image in random manner [24]. Two schemes have been carried out to hide the secret bits. In first scheme LSB embedding in random manner. In second scheme cover image bits are inverted to create identification for the secret bits [25]. LSB inversion techniques are applied in binary image steganography. One pixel can hold one bit of secret message. It is easy to implement and tedious to reveal.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

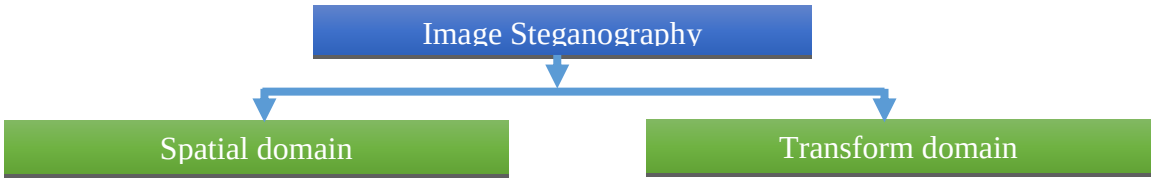

Figure 2: Types of Image Steganography

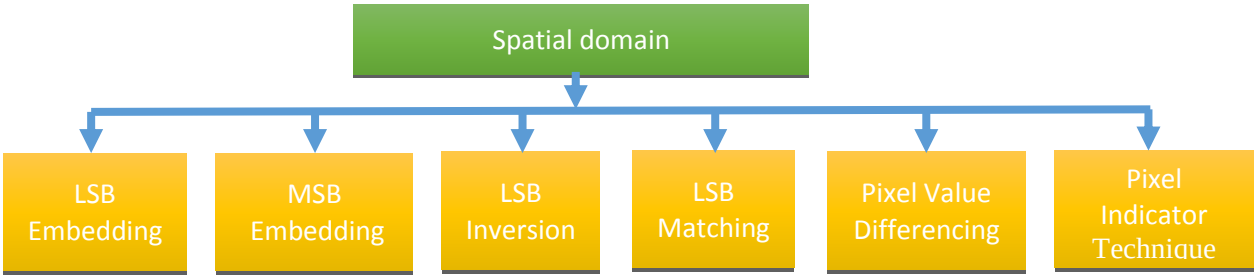

Figure 3: Types of Spatial Domain Steganography

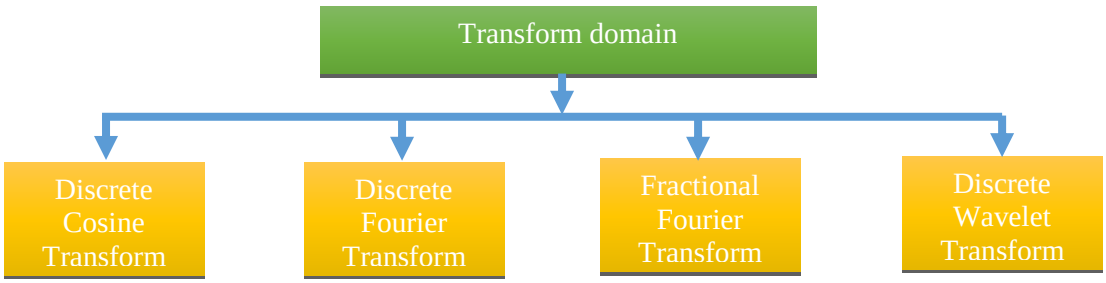

Figure 4: Types of Transform Domain Steganography

2.1.2 LSB Matching Method: By changing the values of LSB while embedding and based upon the changes made among it, the secret information is retrieved in destination by comparing original image with stego-image. LSB matching is one of the strongest algorithms known for its strength against steganalysis as well as cryptanalysis [22].To hide a binary image in a grayscale image, values of binary images are inverted to reduce the number of binary 1's and it is shuffled through a customized pseudo random number generation algorithm [21]. LSB matching is applied for achieving imperceptibility, improved embedding capacity and high security in steganography systems.

2.1.3 Plus or Minus Method: Increasing and decreasing the values of LSB or the pixel value by one or more will change the original image into stego-image. Comparison of stego-image with original image, the secret information is retrieved from it [14].Plus or Minus methods are implemented to achieve less variations in difference between original and modified pixel values. The system implemented with Plus or Minus method is simple and easy to implement.

2.1.4 Pixel Value Differencing (PVD) Method: Two are more pixels selected as a block, based on the difference between those pixels in which the secret bits are embedded in the pixel values. Sharper areas of image have higher difference between the pixels. Those pixels are used in PVD method instead of soft areas of the image which have the similar valued pixels as well. Such changes made among are visible to histogram attacks [8].Pixel value differencing and pixel indicator technique is combined together with a pseudo random number generator for hiding secret message in a cover image was proposed for obtaining higher Peak Signal Noise Ratio(PSNR) and security [20]. Steganography systems implemented with PVD methods are less exposed to steganalysis methods. It is tedious to identify the natural correlation between the pixel values of stego-image.

2.1.5 Pixel Indicator Techniques: In the three channels of the color image, any of the channel is used as an indicator channel to identify where the secret information is residing in other channels. It is easy to implement and resistance against statistical attacks [17].To increase the accuracy of secret message retrieval, pixel indicator technique is proposed along with pixel value differencing [20]. Pixel Indicator Technique is a simple and unique method to implement. It is easy to combine pixel indicator technique with other spatial domain steganography systems to increase the complexity of recovery of secret message.

2.2 Transform Domain Methods: Physical properties of image are converted in to transform coefficients. Secret message bits are embedded among those transform coefficient values and it is converted back as an image. Transform domain steganography is known for its complex algorithms which made the intruder, hard to recover the secret information from stego-image [11]. It is tedious to recover the information hidden through transform domain methods. Transform domain methods are applied in steganography system to increase the security of the secret message to be hidden.

2.2.1 Discrete Fourier Transform (DFT) Method: DFT is implemented with set of harmonically-related complex exponential function for the decomposition of a finite-length and discrete-time vector into a sum of scaled-shifted basis functions. Physical properties converted with functions resulted as transform coefficients and literally known as frequencies. Secret messages are

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

embedded in DFT coefficients. Image enhancement and correction implemented with DFT to achieve better security [12]. Generalizingthe ordinary Fourier transform with a power or angle parameter α, which controls the rotation of signals by Fractional Fourier transform applied to hide the secret information in an image [4]. DFT is applied in steganography system with harmonically-related complex exponential functions to avoid direct recovery of secret information by steganalysis methods.

2.2.2 Discrete Cosine Transform (DCT) Method: DCT is similar to DFT method. The only as well as powerful change is, DCT uses cosine functions insteadof harmonically-related complex exponential functions. Cosine functions in DCT are easily implementable than exponential functions in DFT. One dimensional DCT is implemented as well as coefficients of transform domain are used to embed the secret bits [11].Lossy compression techniques are implemented in steganography system by DCT methods.

2.2.3 Discrete Wavelet Transform (DWT) Method: The image is transformed to discrete wavelets and the secret bits are embedded among wavelets by modifying its values. Again, the wavelets are grouped together and converted to pixel values to form the stego-image. Sub-band of low-frequency of discrete wavelets which is processed to embed the secret data bits [27]. Secret messages are partitioned into small message blocks and it is embedded into the discrete wavelets. Wavelet based steganography is implemented for getting high level compression ratio in images.

3. Steganaysis Methods:

Steganalysis methods find out the existence of secret information in a suspicious image. Steganalysis is a process of revealing secret information hidden by steganography systems. Feature selection, classification and extraction algorithms carried out in steganalysis. The type of steganalysis is depends on the necessity created to reveal the stego-image by steganalyzer. Types of steganalysis are presented in Figure 5.

3.1 JPEG & DCT Specific Steganalysis Methods: To improve over-fitting problem as well as increase in detection accuracy against the Gaussian noises or Salt-Pepper noise which is proven against other JPEG steganalysis methods. Sparse representation plays the major role to detect the image with DCT coefficients [44]. Single classifier is used to find the secret bits in multi-directional detection algorithms in DCT coefficients. Processing of multi-dimensional DCT consumes more computation time than single-dimensional DCT which is easy to implement as well as can be processed with less consumption of time. To decrease the time taken by multi-directional DCT and increase in detection rate, a new method isproposed with multi-direction transition probability matrices [14]. Performance of detection is highly related with errors which occur during computation of image models. To reduce the model errors in proposed work, by spread out of the detection in all scales in JPEG images. Neighborhood classifiers that select a block of DCT coefficients to find the correlation between those values thereby to identify the relationship between all them [22]. JPEG & DCT specific steganalysis methods focusing on transform coefficients with lossy data compression techniques. It is hard to find out the correlation between transform coefficients after embedding secret messages in it. Natural correlation between the pixel values are safeguarded in DCT & JPEG steganography which leads to revealing steganalysis process as a tedious one.

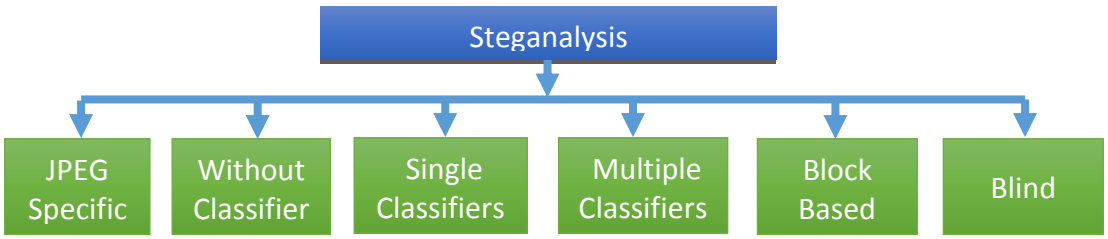

Figure 5: Types of Steganalysis

3.2 Only JPEG Specific Steganalysis Methods: Lempel-Ziv characteristics of complexity that leads to the large consumption of physical properties as well as less in embedding rate. To achieve higher embedding rate using Lempel-Ziv characteristics of evaluating steganalysis algorithm before applying to any image for performance appraisal as well as to achieve optimum probability rate in achieving higher success rate [10]. Large number of features counted to 810 were used in their proposed work to make the detection accurate. However, the work consumes computational time for testing its most of the features to succeed against suspected images. This work is good against targeted attacks [39]. Several steganalysis methods are combined together to increase the detection of stego-images against various steganography techniques. Probability Density Function(PDF) and characteristic functions are used to find out the way other steganalysis methods intended to detect secret information [3]. JPEG image format is most common and widely used. It is necessary to implement a steganalysis system with a JPEG specific module of steganalysis to quickly reveal the secret message.

3.3 Multiple Methods Without Classifiers: Steganalysis is an art todiscover the survival of secret information in the cover media. Image histogram, closest color pair, feature extraction, de-correlation of wavelet transform and characteristic function methods are used to find the existence of secret information [12]. The new steganalysis methods are targeted and it becomes weaker in spite of most of other steganography methods due to specific attacks [42]. There is no necessity of classifier if few features are targeted in steganalysis. The narrowed targeted steganalysis doesn't require a classifier and the secret message is revealed through features and patterns.

3.4 Steganalysis with Single Classifier: Random forest employing Huffman code statistics which uses simple classifier for steganalysis. This method is applied on image database to process 30,000 images. Advantage of this method is stronger in

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

detection and it is only applied to the specific channels [38]. Steganalysis with single classifier is required when more number of features have to extracted through steganalysis.

3.5 Steganalysis with Multiple Classifiers: Neural networks and super vector machine are the two classifiers with Bhattacharyya distance method to extract the secret information from the stego-image. After classification of datasets, redundant features were removed by the feature selection procedure [29] Selected number of features with three classifiers are used to detect the content of stego-image gray level sub-occurrences with histogram methods as global confined leads to better steganalysis [6]. Single classifier methods are known for its weakness due to less number of features. Multiple classifiers are required when more number of features to be compared and detect the existence of secret information in it.

3.6 Block-based Steganalysis: Single classifier methods are weaker and detection rate is very less, comparatively with more than one classifier. Instead of using a whole image to find the correlation, the pixel block-based detection has an advantage of computational efficiency. In order to achieve higher detection rate and better computational efficiency, a method is proposed with decomposition of image into blocks and the selected blocks are intended to find the secret bits. Tree Structured Vector Quantization (TSVQ) method is to quantize the coefficients with minimal values which also solves over-fitting problem [28]. When feature size is higher than the computation complexity of the block-type steganalysis methods leads to higher time complexity, which is not affordable. The methods are tested against uncompressed image database and the results are average, but preferably better thanthe existing steganalysis methods [30,31]. To reduce time taken for computation steganalysis implemented as block-based systems. It is necessary to implement block-based steganalysis methods when large amount of steganography methods have to be tested by steganalysis methods for finding the existence of secret information.

3.7 Blind Steganalysis: The feature selection plays the major part to avoid higher computational complexity. A Localized Generalization Error Mode l(LGEM) is proposed with optimized list of features as well as accuracy in selection of features against variety of stego-images [43]. Various sub-bands of frequencies in distribution of statistical parameters and variety of feature selection techniques are used to detect the secret information. The proposed works are to spot the existence, instead of concentrating on computational complexity. There are no parameters given to predict the time complexity. Increase in detection rate is higher than other composite methods which uses optimum feature selection from a list of successful feature detection algorithms [40]. Statistical parameters are analyzed instead of testing the physical properties of the image with cross-validation techniques which leads to higher detection efficiency [39]. Evidential K-Nearest Neighbors algorithm was proposed with steganalysis to increase the performance of secret message identification comparably higher than existing ensemble classifier steganalysis algorithm [26].

3.8 Other Steganalysis Methods: Increase in the risk of cloud computing as well as neural networks, steganalysis methods are implemented by optimizing the cloud computing architecture as per the requirements of steganalysis algorithms. Fisher linear discriminator, neural network and support vector machines are the three classifiers that propagate the detection operation among network environment [9]. Dependencies in spatial domain is detection by processing inter-pixel values and its correlation. Spread-spectrum techniques will lead to numerical difference between the pixel values which consumes less computational time than other models implemented to increase the chance of detection [17].A universal method for the introduction of heterogenous algorithm to find out the existence secret message instego-image. Large number of image databases were connected to carried out most of the steganalysis algorithms in combined manner [7]. Requirement of independent steganalysis leads to blind steganalysis which have statistical measures to improve the sensitivity of the steganalysis system.

4. Application of Image Steganography and Steganalysis Methods:

Steganography system depends on the characteristics security, embedding capacity, imperceptibility and reliability. It is not necessary to achieve all of them in every method. Steganography methods with its application criteria is presented in the table 1.

Table 1: Steganography Methods with Application Criteria

Types	Methods	Application Criteria
Spatial Domain Methods	LSB&MSB Embedding method	• Basic level steganography method • Good imperceptibility • Security is less against detection methods
	LSB inversion method	• Binary bits are inverted to hide secret message • Security depends on randomness • Easy to implement and hard to detect the secret message existence.
	LSB Matching method	• Original image is necessary for secret message retrieval • Highly secured steganography method. • Imperceptibility is increased by deliberate randomness
	Plus or Minus method	• It is easy to implement the steganography system by this method. • Extra variation in histogram • Effective when the value to be modified is less.
	Pixel Value Differencing	• Retrieval of secret message is done without original image. • Difference value of consecutive pixel is modified to hide secret message. • Less variation in histogram. • Natural Correlation between the pixels affected by this method. • Achieves high security for the content hidden.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

	Pixel Indicator Technique	• Original image not necessary for secret information retrieval. • Moderate level of security • Less complex implementation
Transform Domain Methods	Discrete Fourier Transform	• Conversion of pixel values to coefficients increases computing time • Harmonically-related complex exponential function achieves high security for secret message • Embedding capacity is less
	Discrete Cosine Transform	• Preferred method of implementing steganography in transform domain due to its ease of implementation • Computation Time is higher than other methods • Compression techniques in DCT leads to moderate embedding capacity
	Discrete Wavelet Transform	• Splitting of secret information into high and low frequency components leads to high security • Statistically undetectable method • Less amount of data is hidden in a cover image than other methods.

Steganalysis methods are dependent to computation time, number of features, number of classifiers and the level of implementation. These characteristics were the base for the creation of various steganalysis methods described in table 2.

Table 2: Steganalysis Methods with Application Criteria

Steganalysis Methods	Application Criteria
DCT & JPEG Steganalysis	• Powerful method againstlossy compression based steganography • Feature extraction is applied through multi directional search leads to a quick detection • Detection possibility is higher than other methods.
JPEG specific Steganalysis	• Detection rate on JPEG image is high • Large number of features defined to increases the possibility of detection in JPEG stego-image
Methods with no Classifier	• Strong in feature specific detection method • Weak against other steganography methods
Methods with Single Classifier	• Number of features under a single classifier is an effective method for specific detection on image database. • Applied only for specific channels leads to a narrowed search.
Methods with Multiple Classifiers	• Possible feature extraction procedures are incorporated with multiple classifiers leads to high detection ratio. • Computation time is extensively high because of more number of classifiers and features.
Block based steganalysis	• Detection methods on random blocks reduce computation time of steganalysis system. • Accuracy in block based detection is lesser than detecting an image as a whole.
Blind steganalysis	• Unpredicted steganography methods are handled by blind steganalysis. • Detection ratio is lesser than other steganalysis methods.

5. Survival of Steganography:

From [18, 19, 34, 35, 36, 37], it is observed that huge number of images are transferred through internet every minute as given in Table 3. This survey results include six different widely used social network applications taken from four different references. It is tedious to implement a steganalysis system which is capable of handling all types of images with all types of steganography methods. Even though an integrated system is implemented for finding the secret message in existence, there are number of problems associated with such steganalysis system. Qmee, Go-Globe, Excelacom and DOMO are the organizations who had surveyed regarding internet in 60 seconds.Second-to-second internet data transfer is being measured and updated in two of the websites [18,19].In Go-Globe survey 4,86,000 images are transferred through whatsapp in a minute of time(Go-Globe 2016). For instance, if a steganalysis system focusing on whatsapp images that spends at least 10 seconds to find the existence of secret information for each image, then it will take 56 days and 6 hours as a processing time for 4,86,000 images transferred in a minute of time. Even though the computational time is reduced to Nano seconds, it has a less contribution to the system processing speed. It is impossible to queue the images through the security system because the number of images are vast in numbers. Accessing servers using steganalysis systems for detection leads to reduced server performance. Creating virtual server space is also an expensive idea. Most of the steganography methods are unpublished which leads to less clue for a steganalyzer to implement the steganalysis system and therefore steganalysis systems are not always considered to be complete. Some of the pitfalls in steganalysis as indicated above leads to the survival of steganography methods predominantly.

ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 4.775, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

Table 3: Image Transfer in 60 Seconds

Applications Considered	Survey Results(Images per 60-second)			
	Qmee 2013	Go-Globe 2016	Excelacom 2016	Giphy 2016
Instagram	3,600	56,000	38,194	24,30,555
Snap chat	1,04,000	2,80,000	5,27,760	No data
Tumbler	20,000	No data	No data	No data
Whatsapp	No data	4,86,000	No data	No data
Facebook	No data	No data	No data	2,16,302
Giphy	No data	No data	No data	24,30,555

6. Conclusion:

Intention of this paper is to have an exhaustive survey on how steganography is surviving against steganalysis methods. From the above literature survey, it is observed that eventhough steganalysis methods are closer enough to detect the existence of secret information on stego-images, most of the steganalysis algorithms are bigger in terms of collection of feature selection algorithm and make use of several classifiers as well as features and consumes plenty of time for a single image as well. Every day crores and crores of images are transferred through internet with different kinds of purposes; however, there is no filter mechanism implemented to assess the image transfer. Existing targeted steganalysis algorithms are only used on specific images. Even blind steganalysis methods detect the stego-image in specific channels. Very less possibility for creating an integrated mechanism in detecting media files have a hidden content. Digital laws protect those media files and allow steganalysis to act as the targeted analysis. Speed of data processing and transfer of data is necessary which will not go under invigilation of an integrated system that causes considerable amount of waiting time in communication. Research works in most of the steganography methods were unpublished; if they were published those methods could be revealed for steganalysis.Steganalysis methods are to be implemented with futuristic approach such that reduced computation timeto make it easier to increase the detection rate. In future, steganalysis implemented with withstanding ability will be on the rise; while it is implemented with multi-level of classification techniques as well as enhanced feature selection methods for the purpose of achieving higher probability detection rates.

7. References:

1. Abbas cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, Elsevier, 2013. pp. 727-752.
2. Alondra Gabriela Hernandez Chamorro and Mariko Nakano Miyatake, “A New Methodology of Image Steganalysis including for JPEG Steganography”, IEEE 2010, pp. 434-438.
3. Arijit Sur, Piyush Goel and Jayanta Mukhopadhyay, “A Spatial Domain Steganographic Scheme for Reducing Embedding Noise”, IEEE, 2008, pp. 1024-1028.
4. Ashish Soni, Jitendra Jain and Rakesh Roshan, “Image Steganography using Discrete Fractional Fourier Transform”, IEEE 2013, pp. 97-100.
5. Ashraf M. Emam and Mahmoud M. Ouf, “Performance Evaluation of Different Universal Steganalysis Techniques in JPG Files,”Annales UMCS, Informatica. Volume 12, Issue 3, February 2013, pp. 121–139.
6. Ashu, Rita Rana Chhikara and Deepika Bansal, “GLCM Based Features for Steganalysis”, IEEE 2014, pp. 385-390.
7. Chen xu, Tao zhang and XiaodanHou, “Unsupervised Universal Steganaysis Combining Image Retrieval and Outlier Detection”, IEEE 2016, pp. 1047-1050.
8. Chung Ming Wang and Nan-I Wu, "A High Quality Steganographic method with pixel value differencing and modulus function", International Journal of System and Software, 2007, pp. 247-252.
9. Dai Zhonghua, Xiong Qi, Peng Yong and Gao Haihui “Research on the Large-Scale Image Steganalysis Technology Based on Cloud Computing and BP Neutral Network”, IEEE 2010, pp. 415-419.
10. G. S. Raman and R. T. Subhalakshmi, “Active Steganalysis based on Adapted Lempel-Ziv complexity and Approximate Entropy Estimation”, IEEE 2013, pp. 917-922.
11. Hardik Patel and Preeti Dave, “Steganography Technique Based on DCT Coefficients”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp. 713-717.
12. Hernandez-Chamorro, A. Espejel-Trujillo, J. Lopez-Hernandez, M. Nakano-Miyatake and H. Perez-Meana, “A Methodology of Steganalysis for Images”, IEEE 2009, pp. 102-106.
13. Inderjit Singh, Sunil Khullar and Dr. S. C. Laroiya, “DFT Based Image Enhancement and Steganography”, International Journal of Computer Science and Communication Engineering, Vol. 2 Issue 1, February 2013, pp. 5-7.
14. Jarno Mielikainen, “LSB matching Revisited”, IEEE Vol.13, No.5, 2006, pp. 285-287.
15. Jun Xiao, Bin Qin, Yusheng Sun and Xiao Xu, “Research OF Multi-Direction Transition Probability Matrices Algorithm for JPEG Steganalysis”, IEEE 2012, pp. 3907-3912.
16. KazemQazanfari and Reza Safabakhsh, “A new steganography method which preserves histogram: Generalization of LSB++”, Elsevier, Information sciences 2014, pp. 90-101.
17. Kenneth Sullivan, Upamanyu Madhow, Shivkumar Chandrasekaran, and B. S. Manjunath, “Steganalysis for Markov Cover Data with Applications to Images”, IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, june2006, pp. 275-287.

18. Live status of internet is accessed from: http://onesecond.designly.com/ accessed on 27/01/2017.
19. Live status of internet is accessed from: http://www.internetlivestats.com/one-second/ accessed on 27/01/2017.
20. M. G. Gouthamanaath and Dr. A. Kangaiammal, "Color Image Steganography using Combined Pixel Value Differencing and Pixel Indicator Technique in Spatial Domain", International Journal of Computer Applications (0975 – 8887), pp. 20-23.
21. M. G. Gouthamanaath and Dr. A. Kangaiammal, "Hiding binary image in a grayscale image using pixel matching and randomization technique", Journal of Advances in Image Processing Technique, Vol. 3 No.2, pp. 9-13.
22. M. G. Gouthamanaath and Dr. A. Kangaiammal, "Multilayered Pixel Matching Steganography using a novel PRNG Algorithm and Character Indexing Method", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.85 (2015), pp. 301-307.
23. Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An Efficient Filtering based Approach Improving LSB Image Steganography using status Bit along with AES Cryptography", IEEE 2014, pp. 1-6.
24. Nadeem Akhtar, PragatiJohri and Shahbaaz Khan, "Enhanced the Security and Quality of LSB based Image Steganography", IEEE 2013, pp. 385-390.
25. Nadeem Akhtar, Shahbaaz Khan, PragatiJohri, "An Improved Inverted LSB Image Steganography", IEEE 2014, pp. 749-755.
26. NadjibGuettari, Anne Sophie Capelle-Laize and Philippe Carre," Blind image steganalysis based on evidential k-nearest neighbors", IEEE 2016, pp. 2742-2746.
27. Pham Hai Dang Le and Matthias O. Franz, "Single Band Statistics and Steganalysis Performance", IEEE 2010, pp. 188-191.
28. Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering,2006, pp. 275-290.
29. Rita Rana Chhikara and MeenaKumari, "Significance of Feature Selection for Image Steganalysis, IEEE 2016, pp. 75-79.
30. Seongho Cho, Jingwei Wang, C.C. Jay Kuo and Byung-Ho Cha, "Block-Based image steganalysis foramulti-Classifier",IEEE 2010, pp. 1457-1462.
31. Seongho Cho, Martin Gawecki, and C.-C. Jay Kuo, "Content-Dependent Feature Selection for Block-Based Image Steganalysis",IEEE 2013, pp. 1416-1419.
32. Shunquan Tan and Bin Li, "Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting", IEEE 2012, pp. 336-339.
33. SumathiC.P, SantanamT .and Umamaheswari G, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013. pp. 9-25.
34. Survey of internet in a minute of time by DOMO in the year of 2016 and accessed from: https://www.domo.com /learn/data-never-sleeps-4-0 .
35. Survey of internet in a minute of time by Excelacom in the year of 2016 and accessed from: http://www. marketwatch.com/story/one-chart-shows-everything-that-happens-on-the-internet-in-just-one-minute-2016-04-26.
36. Survey of internet in a minute of time by Go-Globe in the year of 2016 and accessed from:http://www.go-globe.com/blog/60-seconds/accessedon 27/01/2017.
37. Survey of internet in a minute of time done by Qmee in the year of 2013 and accessed from: http://blog.qmee.com/qmee-online-in-60-seconds/ accessed on 27/01/2017.
38. Veena H Bhat, Krishna S and P Deepa Shenoy, "SURF: Steganalysis Using Random Forests", IEEE 2010, pp. 373-378.
39. Veenu Bhasinand Punam Bedi, "Steganalysis for JPEG Images Using Extreme Learning Machine", IEEE 2013, pp. 1361-1366.
40. VladimírBánoci, Gabriel Bugár, Martin Broda and Dušan Levický, "Multi-classification Model for Image Steganalysis", IEEE 2013, pp. 37-40.
41. Xiangyang Luo, Fenlin Liu, Shiguo Lian, Chunfang Yang, and Stefanos Gritzalis, "On the Typical Statistic Features for Image Blind Steganalysis", IEEE journal on selected areas in communications, vol. 29, no. 7, august 2011, pp. 1404-1422.
42. Yam bern Jina Chanu, Themrichon Tuithung and Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", IEEE 2012, pp. 1-4.
43. Zhi-min he, wing w.y. Ng, patrickp.k.chan and daniel s. Yeung, "Feature Selection For Blind Steganalysis Using Localized Generalization Error Model", IEEE 2010, pp. 500-505.
44. Zhuang Zhang, Donghui Hu, Yang Yang and Bin su, "A Universal Digital Image Steganalysis Method based on Sparse Representation", IEEE 2013, pp. 437-441.