Literature survey on steganography

In this chapter, the literature survey on the steganography and various network security mechanisms are described. Many existing algorithms for steganography since 1991 to 2009 are studied and presented in this literature survey. Numbers of web sites as well as research papers are referred on virtualization, ARP Spoofing, IDS Architectures. The description of the research papers referred pertaining to steganography and network security are given in the subsequent sections. The literature is presented in chronological order for these two areas separately.

2. 2 Literature survey on steganography

Bender et al. [6] in this paper, the authors describe the techniques of data hiding like low bit rate data hiding in detail.

Johnson, N. and Jajodia S. [34] This article explores the different methods of steganography such as LSB, Masking and Filtering and also explains about different software tools present in the market for Steganography, such as Stego Dos, White Noise Storm, S-tool etc.

Marvel et al. [38] It is proposed that (Spread Spectrum Image Steganography) SSIS is a blind scheme where the original image is not needed to extract the hidden information unless the receiver possesses the secret key to extract the secret message, otherwise it is virtually undetectable. Thus making this technique reliable and secure.

Jessica Fridrich et al.[32] This paper proposes a highly accurate steganalysis technique which can even estimate the length of secret message embedded in LSB method. In this method, the test image is divided into groups of n consecutive or disjoint pixels. This method exploits the modified pixel values to determine the content of secret message. A discriminating function is applied on the group of pixels. This discriminating function determines the regularity or smoothness of pixels. Then a permutation function called flipping is applied on the pixel groups. By using discriminating function and flipping, Pixels groups are classified in to three categories, i. e Regular groups, Singular groups and Unused Groups. For a given mask, fraction of Regular groups Rm and fraction of singular groups Sm are calculated. Presence of noise in the image causes Rm to be greater than Sm.

R. Chandramouli and N. Memon[49] It gives the analysis of various methods of LSB techniques for image steganography.

Tseng, Y. C et al. [63] This paper presents a secure steganographic scheme which makes sure that if any modified bit in the cover image should be adjacent to another bit that has the same value as the former’s new value. By this way the detection becomes extremely difficult. But for achieving this, data hiding space has to be reduced.

Da-Chun Wu, and Wen-Hsiang Tsai [23] proposed a differencing steganographic method that uses the difference between two consecutive pixels in the same block to determine the number of secret bits to be stuffed. In this method a range table is used which ranges from 0-255. The difference value is subsequently adjusted to the difference in the same range to embed the secret bits, and the difference between the original difference value and the new one is shared between the two pixels. Extraction scheme in this method is quite simple and it do not requires cover image.

Sorina Dumitrescu et al.[55] This paper proposes a new steganalysis technique to detect LSB steganography in digital signals such as image and audio. This technique is based on statistical analysis of sample pairs. By this technique the length of hidden message embedded via LSB steganography can be estimated with high precision.

C.-C. Chang and H.-W. Tseng [9] this paper proposes a novel steganographic technique, which modifies the pixel values. This method does not replace the LSBs of pixel value directly, but changes the pixel value into another similar value. In a word, this steganographic method provides a large embedding capacity with little perceptual distortion.

Mei-Yi Wu et al. [40] this paper presents a new iterative method of image steganography based on palette which reduces the Root Mean Square error between an original image and its corresponding stego-image. Based on a palette modification scheme, which can embed one message bit into each pixel in a palette-based image iteratively. The cost of removing an entry color in a palette and the profit of generating a new color to replace the old color are calculated. If the maximal profit exceeds the minimal cost, an entry color is replaced in iteration.

C.-K. Chan and L. M. Cheng [11] this paper proposes LSB technique in which the secrete data is embedded in the Least Significant bits of the image pixel.

Huaiqing wang and Shuozhong wang [29] Different techniques of steganography and steganalytic methods were discussed in detail in this paper. This paper focuses on LSB modification techniques, Masking techniques, Transformation domain techniques, Techniques incorporated in compression algorithms, and spread spectrum techniques. Then the important attributes of a steganographic system are presented, security, payload and robustness. This paper also presents various steganalytic methods such as, RS steganalysis, Chi-square test, Histogram analysis and universal blind detection.

Xinpeng Zhang and Shuozhong Wang [65] this paper proposes the steganalysis of PVD method proposed by Wu and Tsai. This steganalysis is based on Histogram analysis. The zigzag scan of the image pixels produces a vector called ‘ Image Vector’ and the difference of every pair of pixels in this vector produces another vector called ‘ Substitute vector’. An image from Substitute vector is built which is named as substitute image. Histogram of substitute image is constructed and analyzed.

Andrew D. Ker [4] Detecting LSB matching steganography is quiet difficult compared to the LSB replacement steganography. In this paper Histogram characteristic function (HCF) is used for the detection of steganography in color images, but it cannot be used for gray scale images.

Alvaro Martín et al. [3] Authors have experimentally investigated three different steganographic algorithms. steg, MHPDM, and one of the algorithm used in S-tools. Jsteg embeds a message in the least significant bit of JPEG DCT coefficients. The MHPDM (Modified Histogram preserving Data Mapping) algorithm, which is developed from HPDM (Histogram Preserving Data Mapping), works by altering the least significant bit of a subset of the JPEG DCT coefficients of an image.

Chin-Chen Chang et al. [15] this paper proposes two efficient steganographic methods for gray-level images by utilizing the run-length concept. The two methods embed bits of the secret data in each two-pixel block. In addition, the modular operation is applied in both methods to control image quality. The experimental results demonstrate that both methods in this study perform better than all previous methods, in terms of image quality and embedding capacity.

Chin-Chen Chang and Tzu-Chuen Lu [13] the method proposed in this paper exploit the difference in the expansion of the pixels to conceal large amount of message data in a digital image. The payload capacity of the proposed scheme is higher than Tian's scheme and Fridrich's scheme. In addition, the quality of the embedded image of the proposed scheme is even higher than those of the other schemes.

Chin-Chen Chang and Tzu-Chuen Lu [14] SMVQ (Side Match Vector Quantization) exploits the correlations between the neighbouring blocks to predict the index of an input block that improves not only the block effect of VQ, but also the compression performance of VQ. Owing to the good compression performance and image quality, more concerns are given to SMVQ.

Suk-Ling Li et al. [56] In this scheme, the best match cover-image block of the secret-image block is first selected based on the block difference. Then, the error-matrix, the normalized error- matrix, the difference-degree and the quantized-error matrix between the cover-image block and the secret-image block are computed. The block header information is embedded into the cover-image by the simple LSB substitution method.

Chin-Chen Chang et al. [17] this new scheme classifies the host image pixels into two groups of pixels according to the pixel values. For each group of pixels, the corresponding secret pixel values go through an optimal substitution process and are transformed into other pixel values by following the dynamic programming strategy. Then, embed the transformed pixel values in the host pixels by using the modulus functions and obtain the stego-image.

Hideki Noda et al. [27] The JPEG compression using the discrete cosine transform (DCT) is still the most common compression standard for still images. QIM(Quantization Index Modulation) is applied in DCT(Discrete Cosine Transformation) Domain. DCT based steganographic techniques are immune to Histogram based attacks. Two different quantizers are used with QIM, one for embedding ‘ 0’ and another for embedding ‘ 1’. Another method called HM-JPEG(Histogram Matching JPEG) Steganographic method is also presented along with QIM-JPEG Steganography. In these two methods embedding of secret message takes place during quantization of DCT coefficients only, not by modifying quantized DCT coefficients.

Chin-Chen Chang et al. [12] it presents a reversible data hiding scheme for compressed digital images based on side match vector quantization (SMVQ). In Vector Quantization or SideMatch Vector quantization based methods VQ and SMVQ Compression codes are damaged by the secret data embedded in the message. And they cannot be constructed completely after extracting the secret data. By using this method, the original Side Match Vector Quantization compression Codes can be completely reconstructed, after extracting the embedded secret data.

Ran-Zan Wang and Yeh-Shun Chen [51] this paper presents a new steganography method for images which use a two-way block-matching procedure to find for the maximum similarity block for each block of the image. The indexes which get along with some non matched blocks are noted in the least significant bits of the carrier image, using a hop scheme. This algorithm provides a high data payload capacity.

C.-C. Chang and W.-C. Wu [8] this paper provides a technique to improve the embedding capacity without reducing the quality of cover file. That technique is called an adaptive VQ-based data hiding scheme based on a codeword clustering technique. Adaptive embedding method is superior to the fixed embedding method in terms of embedding capacity and stego-image quality.

Xinpeng Zhang and Shuozhong Wang [64] a novel method of steganographic embedding in digital images is illustrated in this paper. In this method each secret digit in a (2n+1)-ary notational system is carried by n cover pixels, where n is a system parameter. This method offers a high embedding efficiency than that of previous other techniques.

Mehdi Kharrazi et al. [39] this paper gives the experimental evaluation of various steganographic and steganalytic techniques.

Chin-Chen Chang et al. [18] in this paper, a new watermarking based image authentication scheme is implemented. The feature extraction process of the proposed scheme is block-based, and the feature of a block is obtained by performing a cryptographic hash function. Then, the bit stream of the feature is folded and embedded into some least significant bits of the central pixel in the corresponding block.

Po-Yueh Chen and Hung-Ju Lin [48] this paper proposes a new image steganographic method based on frequency domain embedding. The frequency domain transform applied in this method is Haar-DWT. There are three regions i. e., low frequency region, middle frequency region and high frequency region. And embedding occurs in Middle frequencies.

Tse-Hua Lan and Ahmed H. Tewfik [61] the authors have proposed an algorithm which is based on the quantized projection embedding method. Quantized Projection (QP), combines elements from quantization that is QIM and spread-spectrum methods. It is based on quantizing a host signal diversity projection, encouraged in the statistic used for detection in spread-spectrum algorithms.

Yuan-Hui Yu a et al. [67] in this method, a color or a grayscale secret image is hided in a true color host image. Procedures to different secret image types are independent. There are three image-hiding types, which depend on the type of secret image. The second type is a palette- based 256-color secret image. The third type is a grayscale secret image.

Ran-ZanWang, and Yao-De Tsai [52] This paper presents an efficient image-hiding method that provides a high data hiding capacity that allows the embedded image to be larger than the cover image. In this method the image to be hidden is divided into a series of non-overlapping blocks. A block matching procedure is adapted for each block of the image to search for the best matching block from a pool of candidate blocks. This selection of best matching block is done by K-means clustering method. Then the indices of secret image are hidden in the LSBs of best matching block in the cover image.

Bibhas Chandra Dhara and Bhabatosh Chand [7] Block truncation coding and vector quantization are the two widely used spatial domain compression techniques. In the proposed method the inter-plane redundancy is reduced by converting RGB to a less correlated triplet. The spatial redundancy is reduced by block quantization using BTC-PF method and the code redundancy by entropy coding using Huffman code.

Nan-I Wu and Min-Shiang Hwang [41] this paper presents a survey of current methods of steganography in Gray scale images. The following methods are compared and analyzed in this paper.

1. The simple LSB method : Secret data is hidden in the Least Significant Bits of the Cover image. Quality of 3-bit LSB stego image is merely acceptable.

2. The optimal LSB methods: To improve the quality of stego image optimal procedure is adapted in LSB embedding. When data is hidden the nearest value is hidden in the cover image so that cover image distortion is minimized.

3. PVD method (Pixel Value Differencing): In this method the image is divided into non-overlapping blocks of two pixels in zig-zag manner. The amount of secret data to be embedded is determined by the difference in pixel values of two adjacent pixels. More amount of data can be hidden when the difference of pixel value is high, and less amount of data is hidden when the difference is low. In this method the cover image is not required for extraction of the secret message.

4. MBNS method (Multiple Based Notation System method): This method is based on Human vision sensitivity(HVS). The amount of secret data that can be hidden in a pixel is determined by a parameter called ‘ local variation’. Local variation depends on Human Vision Sensitivity, and it is determined by three surrounding pixel values. Greater the value of Local variation, more amount of data can be hidden in that pixel. And less amount of data can be hidden in pixel if local variation value is small.

When these methods are compared for low capacity hiding PVD and MBNS approaches produce better stego images than LSB based methods.

Zhe-ming-lu et al. [68] this paper proposes an image retrieval scheme based in BTC based Histograms. BTC (Block Truncation Coding) is simple and easy to implement image compression technique. To reduce the bit rate of each part of BTC coded triple data, Vector Quantization is applied.

Chin-Chen Chang et al. [19] this paper proposes a reversible data-hiding scheme for embedding secret data in VQ-compressed codes based on the de-clustering strategy and the similar property of adjacent areas in a natural image. This method has more flexibility and higher embedding capacity than other schemes.

H. Motameni et al. [25] the authors have proposed a novel technique for hiding text message in a grayscale image. In this method different colors in the cover image are labeled in order to identify dark regions in the image. Data embedding in the these darker regions results in high quality stego images. This method offers more security than other LSB techniques.

Zhensong Liao et al. [69] this paper summarizes the present techniques of data hiding capacity techniques. Various Communication channel models and host data models are discussed in this paper.

H. Arafat Ali [24] the author, proposes a spatial domain steganographic scheme for JPEG images. This technique is based on statistical analysis and called IVSP (Improving Visual Statistical Properties) Method. This proposed method enhances the statistical properties of the stego image and also reduces the quantization error, which creeps in with JPEG format. And this method is also more secure when compared to the other techniques which are in use presently.

Youngran et al. [66] this paper proposes a new method which is able to provide high quality stego image. According to pixel’s characteristics, number of bits can be embedded in stego image is varying and also providing the integrity of original data.

Andrew D. Ker [5] Batch steganography problem deals with spreading payload in multiple covers. Author has proved that the secure steganographic capacity is proportional to the square root of the total cover size.

Hong -juan zhang and Hong-jun tang [28], Proposed a novel method of image Steganography which can withstand for statistical analysis tests like RS and Chi-Square steganalysis techniques.

Kazuya Sasazaki et al. [35] this paper proposes scheme for hiding data that loss lessly stuffs a data bits into a carrier image using the two differences. In this scheme, a three-pixel block in an image contains two absolute differences-the difference between pixels one and two, and the difference between pixels two and three. Such a difference is called block difference.

Chung-Ming Wang et al. [21] this work is an improvement over Wu and Tsai scheme of pixel value differencing (2003). In this method the image is divided in to the blocks of two consecutive pixels and the number of bits that can be embedded is determined from the width of the range table. The reminder of sum of two pixel values with width of suitable range is calculated and modulus of pixel values is adjusted to the decimal value of binary string to be embedded in the block of two consecutive pixels. This method also addresses the falling-off boundary problem and produces high quality stego images than any other technique of spatial domain steganography. But the hiding capacity is low in this method when compared to other methods.

Chien-Ping Chang et al. [20] Authors have proposed a novel data hiding scheme that embeds a message into a cover image. This method uses Tri way pixel value differencing method. In this method blocks of four pixels are considered at a time. This four pixel block is divided into three pairs. And the

PVD method is applied separately to these three pairs. From the modified pairs on pair is chosen as a reference pair and other two are adjusted. By this method the hiding capacity enormously increases over Pixel Value Differencing Method. But the quality of stego image when expressed in terms of PSNR value decreases.

Adem Orsdemir et al. [1] this method is based on the Higher Order Statistics Steganalysis. Generally any steganographer focuses more on undetectability and payload but not about the statistical difference between the stego image and cover image. When the steganographer is well aware of the steganalysis methods HOS steganalyzer and by formulating statistical in distinguish ability requirement, visual quality requirement, and detect ability requirement the method of steganography can withstand the steganalysis methods based on statistical differences.

Chin-Chen Chang et al. [16] It is proposed in this method that digital images can be compressed using Block Truncation Coding (BTC). BTC is the most efficient spatial domain method with simple computations and acceptable compression rates.

Zhiyuan Zhang et al. [71] generally in two-description image coding the image are partitioned into two parts and each description is produced by alternatively concatenating a finely coded bit stream of the other part. Multi Description Coding is a reliable method for robust transmission over unreliable networks.

H. B. Kekre et al. [26] This paper proposes a new improved version of Least Significant Bit (LSB) method. Before embedding the data a 8 bit secret key used and XORed with all the bytes of the message to be embedded. Message is recovered by XOR operation, by the same key.

Depending on the MSBs the number of bits of LSB utilized for data embedding are calculated. This method is simple to implement and offers high payload than other methods like PVD.

Sathiamoorthy Manoharam [54] analyzes the steganalysis of LSB technique using the RS Steganalysis technique. The two classes of images- natural photographic images and synthetic images are taken as the cover medium.

Ahmad T. Al-Taani and Abdullah M. AL-Issa [2] the proposed method provides good quality and high embedding capacity of stego image. Here the carrier image is divided into blocks of equal sizes and then stuffs the original data bits in the edge of the block depending on the number of ones in left four bits of the pixel. Experimental results of this method are compared with Pixel Value Differencing method and Gray Level Modification Method.

P. Mouli and M. Mihcak [45] described the data hiding capacities of various image sources.

Hong -juan zhang and Hong-jun tang [28] Proposed a novel method of image Steganography which can withstand for statistical analysis tests like RS and Chi-Square steganalysis techniques.

2. 3 Literature survey on Network Security

John McHugh et al. [33] this paper describes the role of an IDS in an enterprise and also gives survey on mostly used intrusion detection techniques. This paper also describes the various representative systems from the commercial, public, and research areas.

Ray Spencer et al. [53] this paper, proposed a Flask micro kernel based operating system, security architecture which provides the solutions for the access rights sort of problems and it is suitable for many operating environments.

Clive Grace [22] it gives a detailed understanding of various types of attacks possible and also various types of intrusion detection systems and soft wares.

Nong Ye et al. [42] this work paper gives an investigation on a multivariate quality control technique. This method is finds a long-term profile of normal activities in the profiles in order to detect intrusions.

Tal Garfinkel and Mendel Rosenblum [59] it proposes the Intrusion detection architecture and also the results are demonstrated to detect the attacks using the IDS which are completely isolated from the monitored host.

Tal Garfinkel et al. [58] This architecture provides a tamper resistant trusted hardware platform where each and every application will be running on either the open platform that is general purpose platform or the closed platform that is general purpose platform with security and integrity properties.

P. Englund et al. [43] this paper describes the trusted platform which provides a strict control over the software and hardware platforms to withstand the various vulnerabilities.

Suresh N. Chari and Pau-Chen Cheng [57] Blue box, the host based IDS, is designed based on the system call introspection. They designed some set of fine grained rules for access control to the system resources.

M. Rosenblum and T. Garfinkel.[37] It describes the virtual machine monitor and also how the VMM is useful to provide security. It also looks after the various implementation issues and future directions for the VMM.

James E. Smith and Ravi Nair [30] in this paper various levels of abstractions of virtualization and also the architecture of virtual machines are described. Process and system virtual machines are also described over here.

Peyman Kabiri and Ali A. Ghorbani [47] it gives a review on current trends and technologies implemented by re- searchers and also elucidated the applications of honey pots to detect attacks.

Petar Cisar and Sanja Maravic Cisar [46] this paper describes a flow based algorithm combined with data mining techniques for intrusion detection.

Jenni Susan Reuben [31] this paper gives a literature survey on various security issues as well as threats which are common for all virtualization technologies.

Zhenwei Yu et al. [60] this paper gives an experimental result for an automatically tuning intrusion detection system which controls the number of alarms output to the system operator and according to the feedback mechanism provided by the system operator, tunes the detection model when false alarms are identified.

The Flask architecture of security enhanced Linux for red hat is described in detail in this website [81].

2. 4 CONCLUSION

This literature described the various methods and algorithms existing for the steganography and network security. Based on the existing algorithms, the conclusions are proposed to provide the efficient methods for the below

1. Data Security

2. Network Security

2. 4. 1 Data Security

For providing the data security, there are many cryptography and as well as steganography methods existing for the data to be transmitted on the channel. But for any algorithm, it is has its own disadvantages. In the case of Steganography, the basic algorithm is LSB algorithm and some variations on the spatial domain techniques. But at any point of instance, algorithm is public. Once the algorithm is known, attacker will be trying to get the secure data. In this thesis two algorithms are proposed to provide the data security, which were not presented so far, which are as follows:

Highly Secured, High Payload and Randomized Image Steganographic Algorithm using Robust Key:

In this proposed method, the algorithm used for steganography process is either the PVDM or LSB algorithms depending on the inter pixel difference value in order to increase the data stuffing capacity with out disturbing the quality of the stego image. The position of pixels where to stuff bits will be decided by the stego key which is randomly selected by the user and this key is transmitted to the other party in encrypted form. So the key is robust.

Highly Secured, High Quality, High Payload and Randomized Image Steganographic Algorithm using Robust key based on Tri way PVDM Method :

In this proposed method, the algorithm used for steganography process is the Tri – way PVD with Modulus which is an extension of Tri – way PVD [20] in order to increase the stego image quality. The position of pixels where to stuff bits will be decided by the stego key which is randomly selected by the user and transmitted to the other party in encrypted form. So the key is robust.

2. 4. 2 Network Security

For Providing the Network Security, There are many software and hardware devices available like firewalls, IDS etc.,. Generally an intrusion is detected by the IDS, immediately that can be patched by using the available techniques, meanwhile the applications are to be stopped temporarily, where as the proposed trusted architecture for providing network security will provide a self healing intrusion detection system without disturbing the actual state of the system, and trust can be taken back to the system by using the virtualization concepts.