A Review on the Various Recent Steganography Techniques

[1]Sandeep Singh, [2]Aman Singh

[1]Department of Computer Science Engineering, Lovely Professional University
Phagwara, Punjab, India

[2]Assistant Professor, Department of Computer Science Engineering, Lovely Professional University
Phagwara, Punjab, India

Abstract - Security of the secret information has been a challenge when the large amount of data is exchanged on the internet. A secure transfer of information can be very much achieved by steganography and Cryptography. Steganography is a tool for hiding information inside an image. Cryptography is a tool which provides encryption techniques for secure communication. This paper presents a survey on various steganograpgy techniques along with other techniques used in the literature from 2003-2013. Several different techniques are mentioned with their benefits, limitations, year of publication and their authors. 65 papers were selected after content filtering out of more than 150 papers. LSB (least significant bits) technique was mostly used, while MSB (most significant bits) technique was very less used. There were also several other techniques used such as SSHDT, RSTEG, DCT, DWT, LWT etc... in various papers. Combined techniques of steganography and cryptography were also used in some papers. The survey results show that the steganogarph has played a very beneficial role in various applications. It increased the level of information security with a wide use of its techniques. It would be very useful and provide a better platform for the beginners who want to work in steganography. By analyzing the existing techniques more new techniques can be developed.

Keywords *- Steganography, Cryptography, LSB, GLM, Distortion techniques, Visual Steganography, OPA*

1. Introduction

Information security is a major issue of concern while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of loosely network. It is not restricted by any geographical, national or international boundaries; it means anyone can access it from any part of the world. Although it is very useful for various purposes but there is a risk associated with security of the information which is transfer through the internet. Anyone can hack the information and then make misuse from that or corrupt it or we can say that anyone can destroy the information if it is not fully secured or protected. Steganography and Cryptography both plays a very important role in information security. Steganography is information security tool which stores the secret information in any media file in such way that no one else except the sender of the information and the intended receiver can only suspect the existence of any sort of information. Cryptography is also an information security tool which provides encryption techniques to hide the secret information. Aim of both steganography and cryptography is same but achieved by different ways. Good imperceptibility (difficult to detect hidden information) and sufficient data capacity (efficiency of hidden information) are two properties which should be possessed by all the steganography techniques.

This study includes the various papers on steganographic techniques from 2003 to 2013. Most possible techniques used within this period of time are reviewed. All the papers which are discussed in the literature review were taken from IEEE explore. The survey was conducted on various steganography techniques which are very helpful and useful for providing better information security along with some cryptography techniques and some other techniques such as LSB, LSBM, LSBMR, SSHDT, RSTEG, OPA, Genetic-X mean algorithm, VSS, SDSS, FDSS, BPCS, GLM algorithm, SDS, Transform domain techniques, Distortion techniques etc.

1.1 LSB (Least significant bits)

Simple method in which the least significant bits of the bytes in an image is replaced by bits of secret message. A large amount of data can be embedded by LSB without observable changes. Very effective, easy to implement, takes very less space but it has low imperceptibility.

1.2 BPCS (Bit plan complexity segmentation steganography)

It was invented by Eiji Kawaguchi and Richard O. Eason in 1997[66]. In this segmentation of image are used

by measuring its complexity. It replaces the noisy blocks of bit plan with the binary patterns mapped from a secret data. Noisy blocks are determined with help of complexity. It has Very large embedding capacity.

1.3 SDSS (Spatial-domain steganalytic system) and FDSS (Frequency-domain steganalytic system)

These are the two categories of the steganalytic system. In SDSS spatial domain statistic features are used for checking the lossless compressed images whereas in FDSS DCT (discrete cosine transformation) are analyzed for detecting JPEG segos images.

1.4 Transform Domain Techniques

It is more robust against various attacks such as cropping, compression, etc as it uses the significant region of the cover image to hide the secret information. There are number of transform domain techniques such as DCT, DWT, DKT etc. DCT (discreet cosine transforms) is the most widely used

1.5 Masking and Filtering

These techniques are applicable for 24-bit and a gray scale images. Masking is very useful for hiding data in such a way that the hidden data is more integral to the cover images than simply hiding the data. Filtering is used to remove noises form high level processing steps like embedding secret image can carry on the original data.

1.6 OPA (Optimal parity assignment)

Algorithm was proposed by Fridrich in 2000[51] similar to EZ_stego. It uses the shortest distance principle for selecting the RTD (Replacement transfer direction) for every index in Platte. Secured than EZ_stego and avoids the statistical artifacts.

1.7 GLM (Gray level modification)

Algorithm is for hiding information instead of image processing. Data is mapped within an image by using the concept of odd and even numbers. Only the binary format information is hidden. Effective algorithm and stores as many bits as size of image.

1.8 Distortion Techniques

In this the knowledge about the original cover should be known to the receiver so that receiver can reconstruct the modification made by sender by measuring the differences with the original cover.

The purpose of the paper is to bring out the current techniques of the steganography and establish a platform for the beginners it may help them to develop new techniques or improved the existing one. The remaining part of the paper is organized as follow: in section (2) a brief Literature review is discussed, in section (3) all the possible results with proper tables and figures are described and in section (4) the conclusion of the paper is mentioned.

2. Literature Survey

The main purpose of this paper is to present a survey on various steganography techniques used in recent years. Search was made on IEEE explore, about 150 papers are downloaded out of which only 65 papers left after content filtering. Table 1 presents an extensive literature survey in which all the papers are arranged in a descending order of their year of publication. Different techniques were used by different authors in different years were mentioned clearly along with their advantages and limitations. Keyword used to search were steganography techniques, steganography methods, steganography algorithms etc.

Table 1: Literature Survey

Author	Year of Publication	Steganography techniques and other technical details	Advantages	Limitations
Alam and Islam [1]	2013	SDS, ATMED, ATMAV, MED. Color Quantization: 256 colors, 240 blocks, RGB components- 3 bit R, 2 bit G and 3 bit B component.	To compare the accuracy of the transmitted data, safe and secure image data transformation and to authenticate the sender SDS is efficiently incorporated.	PSNR ratio performance is not very much good and not effective for standard datasets.

Geetha, *et al*.,[26]	2013	LSB: 262,144 bits, Edge Detection Method, Multiple Edge Detection Method:- Gaussian filter, 2-dimensional convolution filter, Multiple Error Replacement, Variable Embedding Ratio.	Good visual qualities and highest embedding capacity with high security.	
Jose and Abraham [7]	2013	Image Encryption, Chaotic sequence, Pseudorandom number.	Provide higher data hiding capacity.	
Kadam, *et al*., [9]	2013	AES:- 128 bit key,32-bit words,128-bit cipher key, LSB, Experimental design: Intel core i3 at 2.27GHz, 4GB RAM, 500GB hard disc capacity.	Prevent transformation of secrete file from third party access, Increased data security level and Keys of decryption process is protected from the hackers.	Memory required for implementation should be as small as possible.
Mahato, *et al*., [6]	2013	HTML attributes, Stegno-Crypto techniques.	Steganography is achieved easily by HTML as HTML is rich in code and very less chance to check its source code and easily communicated through internet.	Secrete message can't be extracted and High time complexity of the algorithm
Ramaiya, *et al*., [4]	2013	LSB:- 2-bit, DES:- 64-bit,16 rounds, S-Box: - 6-bit as input and 4- bit output, 4*16 definition tables,0-15 decimal values.	In presented paper, high level of security is provided and variation in two LSB of each pixel will not affect the cover image quality.	Small modification to an S-Box could significantly weaken DES.
Samidha and Agrawal [28]	2013	LSB, Raster Scan, Random Scan, Layout Management, Spatial Domain	Pixels can be used to hide data. Technique can be extended at any place in image using any dimension of any shape.	.
Thenmozhi and Chandrasekaran [3]	2013	DWT:- 2-D, M x N size cover image, Henon Map.	High capacity, good invisibility, secrete message cannot be extracted and Removes the outlines of the encrypted images completely.	
Chanu, *et al*.,[5]	2012	RS method, Spatial domain, Transform domain.	All strong and weak points are mentioned very clearly and by analyzing steganalysis techniques a better steganography techniques can be developed.	Not able to detect the secret message.

Danti and Manjula [27]	2012	DWT, HWT: combination of DCT and DKT, combination of DCT and Discrete Walsh Transform.	Increased capacity and hidden image size is twice or more than that the size of cover image. MSE, Entropy and Capacity is better with acceptable PSNR.	
Das, *et al*.,[21]	2012	LSB:- 32 bit secret key, Blind extraction, ASCII, HVS.	Through digital colour images hidden text passing is very efficiently done and embedded text is completely invisible in the encrypted images.	
Fridrich [23]	2012	Rich Models, Noise Residuals, High dimensional features.	Building Model Process can be independently viewed of the final classifier design and Interesting interplay is revealed between the embedding and detection.	
Manoharan [12]	2012	LSB, RS analysis, Low colour images.	Effective in all cases such as random embedding with LSB replacement and random embedding for sequential for LSB matching.	Technique only applies to synthetic images with a small number of distinct colours such as logos and flags and it is not effective for big sizes images.
Mare, *et al*.,[15]	2012	LSB:- 9 LSBs RGB images, Payload adaptation.	Stronger steganographic model. Size of jump table for extraction is reduces and leaves more space for secret data	Jump table cannot be store in nosy areas.
Motamedi and Jafari [18]	2012	DWT:- 2-D Wavelet Transform, Inverse DWT, Threshold Selection Based on Denoising Methods.	Robustness against the attack of steganalysis. Improved capacity and PSNR. Without referencing the original image data can be extracted from stego-image.	Level dependent denoising methods.
Pevny, *et al*.,[24]	2012	Linear least-square regression, Support vector regression, Quantitative steganalysis, LSB.	Able to construct quantitative steganalyzers for stegosystems for which no quantitative attacks existed.	Not provide high accuracy.

Premkumar and Narayanan [22]	2012	Visual Cryptography Schemes, LSB.	Decreased Image distortion, Dynamic capacity values can be estimated more precisely and Secret parameters can be extracted easily.	
Reddy, *et al*., [19]	2012	SSHDT, LWT:- Inverse LWT, DFBM.	Better PSNR and embedding capacity.	Limited amount of data can be used.
Sanchez, *et al*.,[29]	2012	LSB, MLA: GA and PR algorithm.	Sending the message and receiving the original message are treated equally.	Need to improve the safety of sending the X matrix.
Selvi, *et al*.,[30]	2012	LSB): LSBM and LSBMR, Edge Detection	Recovered sent message through noisy channels like binary symmetric channel.	
Talip, *et al*., [20]	2012	Uyghur text: - 32 letters, 32 phenomes,8 vowels and 24 consonants, Characteristic code mapping:- SKT for encryption, Crypto-Stegano techniques.	Communicating message is protected from being compromised for the local community.	The SKT and CCM tables need to be improved.
Yang and Zhong [13]	2012	KCCA, DCT, Markov reduced feature, 216-D DTC features, Feature fusion.	Better detection rate, improve the detection capability. Reasonable and Effective.	Fuses only two features.
Zheng, *et al*.,[11]	2012	LSB:- Replacement and Matching, Software identification, Steganography detection.	Variety of steganography software can reliably identify based on LSB steganography algorithm.	Difficult to find more steganography software's with fewer templates and difficult to transform a better form of intermediate code.
Zhou, *et al*.,[17]	2012	LSB, AES: 128-bit.	Provide significant benefits upon sequential distribution and more secure method.	Much costly.
Zhou, *et al*.,[14]	2012	L-GEM, RBFNN, Double JPEG compression: - DCT.	Influence steganalysis to a notable extent, It is of great use and good generalization capability.	Detection of double compression is not accurate and SVM perform a little bit worse than the RBFNN optimized by the L-GEM.
Bansod, *et al*.,[10]	2011	Hybrid cryptography:- DES: 64 bit, 56 bit key,	No need to send DES key secretly before communication by using	Limitation of matching the

		RSA. BPCS.	RSA algorithm. Encryption and decryption speed is same as DES.	data bits with image bits so maximum value is not successfully completed the steganography.
Mandal and Ghatak [25]	2011	LSB), (2,2) Visual cryptography, Visual steganography, SITMSVC.	Original and regenerated images are same as the evaluated pixel values is position wise same as the original pixel values of the original cover image.	Degrades the quality of the images.
Usha, *et al*.,[8]	2011	Reference matrix, Playfair square, AES, LSB, 3-D Matrix with RGB as the axes.	Provide higher level of security.	
Zhai, *et al*.,[16]	2011	RSTEG: TCP, IRSTEG algorithm.	Reduced resource consumption and overcome the shortcoming of retransmission probability comparison algorithm.	
Zin and Soe [2]	2011	LSB, RIPEMD-160 hash algorithms: 512-bit message blocks, sixteen 32-bit words. RC4 algorithm, BBS.	Integrity and confidentiality is enhanced.	Data can't be extracted if stego-image is transformed by any image processing software.
Afrakhteh and Ibrahim [33]	2010	LSB, Images distortion, 8-bit gray scale image.	MSP a new method. Robust against Chi-squared attack and stand for more surrounding pixels.	It is not a reliable
-Cheddad, *et al*.,[32]	2010	OOE, BRGC, DCT, 274-D merged Markov, DWT.	Enhance steganography in digital images for ongoing researches.	Payload available is limited and MB2 faces much more accurate targeted attacks.
Jankowski, *et al*.,[31]	2010	ARP, TCP, Frame padding, Etherleak.	Important method of identification in order to minimize the potential threat of inter-protocol steganography to public security and Crucial for the effective development of counter measures.	A universal and effective steganalysis method can't be developed by considering the complexity of network protocols using currently. For the new

				potential threat a security system must be adapted after each new steganographic method is identified.
Sun and Liu [34]	2010	LSB, Information hiding techniques, Image processing.	Secured by efficient cover selection method and to improve steganography security sender can choose a better cover.	No estimation regarding the effect of gap on the security of steganography and to detect LSB matching with SSIS is very difficult.
Almohammad, et al.,[37]	2009	16 x16 quantized DCT) block, 2-LSBs.	Provide higher information hiding capacity and better quality of stego-images.	
QI Ke, et al.,[36]	2009	3D models, Spatial domain, MQIM, Adaptive embedding estimation.	Suitable for 3D mesh models. Secure, Simple, Low distortion high capacity and robust against affine transformations and vertex reordering attacks.	
Safy, *et al*.,[38]	2009	IWT, DWT, Spatial domain, Adaptive algorithm, OPA algorithm, Extraction algorithm.	Increased hiding capacity of the system and Secret data is embedded in random order using secret key known by only sender and receiver.	Not good robust against attacks like histogram equalization and JPEG compression. PSNR ratio is needed to be improved with the obtained hiding capacity.
Szczypiorski [35]	2009	HICCUPS, CSMA/CA, WLAN.	WLAN efficiency and cost of system usage included to focus on the performance features of the HICCUPS.	A versatile Assessment of HICCUPS security is needed to cover.
Chen, *et al*.,[40]	2008	8 x 8 DCT matrix, RBFNN, PCA.	Reduced training dimensionality. Potential bias is avoided and allows data to reside in same dynamic range.	Accuracy cannot be improved by feature extractions.
Geetha, *et al*.,[39]	2008	IQMs, Genetic –X-mean algorithm, DCT, DWT, LSB.	Improve the classification precision.	Difficult method to prove C0X.
Wang and Moulin [42]	2008	Watermarking. DMC, Reliability function, Universal codes, Binning code, Steganographic codes,	MPMI decoder and stacked-binning codes achieve a random-coding exponent. Perfectly secure steganography.	

		Timing channels.		
Bohme and Keiler [43]	2007	Public key steganography, Security analysis, Embedding function, Mapping function.	A secure alternative system can easily be constructed from standard primitives.	PKS-CE is not secured and operable and Both embedding and asymmetric trap –door function are weak.
Deng, *et al*.,[45]	2007	LSB, ANOVA, ML detector.	High accuracy and low computational complexity. Satisfactory results.	
Q. Shi, *et al*.,[47]	2007	Representatives steganographic schemes, Text image database, Cross tests.	Both images with and without additional compression in training are helpful for ways to handle the issue of recompression.	Cross test should not be adopted in handling the steganalysis issue of recompression as it have insufficient training.
Ryabko and Ryabko [41]	2007	Simple non randomized universal stegosystem, General construction of a universal stegosystem.	Hidden information can be encoded in number of blocks which have the same probability as the original.	
Savoldi and Gubian [48]	2007	SIM/USIM cards, Imaging tools.	More widespread and sophisticated.	Some of the steps latterly can be time consuming and similar to the problem of detecting a hidden message in digital images.
Agaian and Cherukuri [46]	2006	CBER, VBER, Computer simulation.	Universally used for all binary digital media. Enhances the robustness and reduces the error in reconstruction.	Incorporate the shuffling and matrix encoding techniques so as to make the system more robust is not well achieved by this system.
Raja, *et al*.,[44]	2006	DWT, 8 x 8 Payload encryption.	Increased security.	The stego image is not robustness against different attacks.
Wu and Shih [53]	2006	Digital watermarking, Genetic algorithm, Fitness function, VSS, SDSS, FDSS.	Enhance PSNR ratio of stego-images and Increased the capacity of the embedded message.	More iterations are required in GA-based algorithm as lower bit plane used for embedding.

Zhang and Wang [49]	2006	Embedding efficiency, Embedding rate, Covert Communication.	Secret message can be conveniently hidden irrespective of the ratio between size of cover signal and payload by EMD method.	
Adli and Nakao [56]	2005	MIDI, LSB, Command code algorithm, SysEx algorithm.	User can choose any algorithm of their choice. Efficient way to stegane information with high security and does not affect the music	Original file size can be changed. If file type is changed or open in MIDI editor then steganed data can be corrupted with this algorithm.
Kong, *et al*.,[51]	2005	OPA algorithm, Multimedia security, RTS, CCR.	Accurately estimates the length of hidden message. Successfully attack the OPA method.	May fluctuate largely in estimation a small embedding capacity.
Luo, *et al*., [54]	2005	DRS algorithm, LSB :- 24 bit colour images, RS method.	Lower missing rate, more accurate and more powerful steganalysis methods.	Two masks are not equal, have some deviations and These initial deviations may lead a serious estimate error.
Martín, *et al*.,[55]	2005	Natural images, Image models, DCT, MHPDM algorithm.	Achieves significant classification performance and Best classification results.	Unnatural information is not sufficient to move the results outside of the natural range unless the knowledge of the embedding algorithm is available.
Niimi, *et al*.,[50]	2005	Visual attacks, Conjugation flags, BPCS.	Unnatural patterns used in signature do not appear in stego-images.	Conjugation flags are not embedded by complexity thresholding and Desire to choose information for key which does ‘not depend on image data and secret data.
Raja, *et al*.,[52]	2005	LSB, DCT, DWT, MSE, BER.	Without any password images is transferred securely with low MSE and BER.	
Trivedi and Chandramouli [64]	2005	Sequential steganography, CUSUM- LMP, Abrupt change detection based steganalysis	Well performance for stationary host signals and Good accuracy of secret key estimation is achieved.	Low frequency embedding in DCT domain affects its performance.

		DCT.		
Dou, *et al*., [57]	2004	ICA, Kernel SVM.	Secret message is independent with cover image.	Lower accuracy rate for DCT.
H. Sung, *et al*.,[65]	2004	CFG for animation, Error control coding, ASCII text embedding.	Animation is used to encode a secret message. Payload is encoded in carrier rather than embedded into it.	Serious limitation of this model is capacity.
Jiang, *et al*., [60]	2004	Compression bit rate, Flipping pixels, Estimating message length.	Stegano-graphic embedding process can be detected reliably and Reasonable accuracy can be estimated with embedding rate.	
Khan, *et al*., [58]	2004	GLM, Architecture platform, Embedding.	Capacity of GLM is as much as the size of image as in GLM each binary bit is embedded in the image.	Key is depended on both the size of the picture and size of the message.
Potdar and Chang [61]	2004	GLM, LSB, GLM algorithm.	Useful in server security, network data and industry scale system without having trustees of third party.	First element of the bit stream should be mapped with the first selected pixel in the image.
Sui and Luo [59]	2004	HTML, Steganographic method, Frangibility analysis of algorithm.	High efficiency and security with large capacity and high imperceptibility.	Steganography is difficult with HTML and is immature in theory and applications.
Zhi and Fen [63]	2004	GEFR, LSB, Flipping algorithm: - 2-cycles.	Error emendation method is presented and analyzed the applicability of all kind of images.	Improvement is needed in embedding length estimation precision, especially when the embedding length is relatively short.
Ashar, *et al*., [62]	2003	Compression module, Cryptographic module, Hash module :- SHA-1: $<2^{64}$ bits is input, produces a 160 bit output, Steganographic module, 24-bit true color image, ECDLP.	Proposed model is efficient and effective, used to store secret data in computer without anyone's noticed and Well fits in circumstances when we are absent but other person is using our computer.	8 bits and 16 bits color images cannot be used for this steganographic purposes.

LSB: Least Significant Bit; SDS: Structural Digital Signature; PSNR: Peak Signal-to-Noise Ratio; ATMED: Asymmetrical Triangular Median; ATMAV: Asymmetrical Triangular Moving Average; MED: Median Filter; RGB: Red, Green and Blue; DES: Data Encryption Standard; AES: Advanced Encryption Standard; HTML: Hyper Text Mark-up Language; DWT: Discrete Wavelet Transforms; MLA: Method of Linear Algebra; GA: Genetic Algorithm; PR: Path Ranking; HWT: Hybrid Wavelet Transform; DCT: Discrete Cosine Transform; DKT: Discrete Kekre Transform; MSE: Mean Squared Error; LSBM: Least Significant Bit Matching; LSBMR: Least Significant Bit Matching Revisited; SSHDT: Secure Steganography Using Hybrid Domain Technique; LWT: Lifting Wavelet Transforms; DFBM: Decision Factor Based Manipulation; KCCA: Kernel Canonical Correlation Analysis; SKT: Secret Key Table; CCM

: Characteristic Code Mapping; RS: Regular Singular; ASCII: American Standard Code for Information Interchange; HVS: Human Visual System; L-GEM: Local Generalization Error Model; RBFNN: Radial Basis Function Neural Networks; SVM: Support Vector Machines; RSTEG: Retransmission Steganography; TCP: Transmission Control Protocol; IRSTEG: Improved Retransmission Steganography; SITMSVC: Secret Image/Message Transmission through Meaningful Shares using (2,2) Visual Cryptography; RSA: Rivest, Shamir and Adleman; BPCS: Bit Plane Complexity Segmentation; RIPEMED: RACE Integrity Primitives Evaluation Message Digest; BBS: Blum Blum Shub; OOE: Object-Oriented Embedding; BRGC: Binary Reflected Gray Code; ARP: Address Resolution Protocol; MSP: More Surrounding Pixels; HICCUPS: Hidden Communication System for Corrupted Networks; CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance; WLAN: Wireless Local Area Networks; MQIM: Multi Quantization Index Modulation; IWT: Integer Wavelet Transform; OPA: Optimum Pixel Adjustment; PCA: Principle Component Analysis; IQM: Image Quality Matrices) DMC: Discrete Memory less Channel; MPMI: Maximum Penalized Mutual information; SIM/USIM: Subscriber Identity Module/Universal Subscriber Identity Module; PKS: Public Key Steganography; ANOVA: Analysis Of Variance; ML: Maximum Likelihood; CBER: Constant Block Embedding Rate; VBER: Variable Block Embedding Rate; EMD: Exploiting Modification Direction; VSS: Visual Steganography System; SDSS: Spatial-Domain Steganalytic System; FDSS: Frequency-Domain Steganalytic System; MHPDM: Modfied version of the Histogram-Preserving Data Mapping; MIDI: Musical Instrument Digital Interface; BER: Bit Rate Error; BPCS: Bit-Plane Complexity Segmentation-Steganography; CUSUM: Cumulative Sum; LMP: Locally Most Powerful; DRS: Dynamic Regular Groups Steganalysis; RTS: Replacement-Transfer Structure; CCR: Convergent Continuous Replacement; CFG: Context-Free Grammar; ICA: Independent Component Analysis; GEFR: Gradient Energy–Flipping Rate detection SHA: Secured hash Algorithm; ECDLP: Elliptic Curve Discrete Logarithm problem;

3. Results and Discussion

A survey was conducted to review the papers on various steganographic techniques used in recent years. A total of 65 research paper has been cited to gather theinformation about steganographic techniques. Information so far collected has been summarized in Table 2 Search was made by using various keywords some of them are steganography, steganography applications, steganography techniques, steganography detection algorithm etc.

Table 2: No. of papers of steganography on yearly basis

Years	No. of papers
2013	8
2012	17
2011	5
2010	4
2009	4
2008	3
2007	5
2006	4
2005	7
2004	7
2003	1
Total	65

Table 2 shows a no. of papers published on steganography in different years. It was found that in 2003 researchers were not very much interested in the work of steganography but from 2004 to 2011 some better results were found. In 2012 maximum number of papers were published which means that researchers gave their great contribution in the field of steganography. Researchers used many different steganography techniques (LSBM, LSBMR, SSHDT, RS) along with some cryptography techniques (AES, Visual cryptography techniques) in 2012.The publications in 2013 shows that the researchers made the good use of combined approach of steganography and cryptography which provide a very strong security

Fig 1, presents a year wise distribution of number of papers. It was clearly shown that number of papers published in 2012 were made a peek but before this from 2003-2011 and including 2013 the no. of papers goes down, it was the year when researchers made the maximum use of LSB technique along with some other techniques (MLA, HVS, ASCII, Blind extraction). The average rate of no. of papers published from 2003-2013 were not exceeding than 6-7. It was also observed that during 2012 and 2013, maximum numbers of different techniques were used by the researchers such as SDS, Filtering, Edge detection method, DES, S-Box, DWT, DCT, DKT, KCCA, L-GEM, REFNN etc. In most of the reviewed papers, the use of LSB technique was mostly preferred by researchers rather than MSB.

Fig 2 shows a percentage distribution of no. of papers in yearly basis. Among the selected papers the maximum contribution was recorded from 2012 with 26% followed by 12% from 2013, 11% from 2004 and 2005, 8% from 2007 and 2011, 6% from 2006, 2009 and 2010, 5% from 2008 and 1% from 2003.This survey revealed that in 2012 and 2013 the maximum research was done by researchers as the percentage of papers published in these two years showed there maximum contribution. As LSB was the most popular technique during 2012 therefore many researchers got very significant advantages in their work, they made the best possible use of LSB in which way they can. The steganography was most widely used in 2012 as it was clear from figure 2; it was 26% which is much

greater than 2011 having only 8% contribution which was 18% less than 2012, at that time steganography was most popular as many researchers used this in their work for stronger information security.

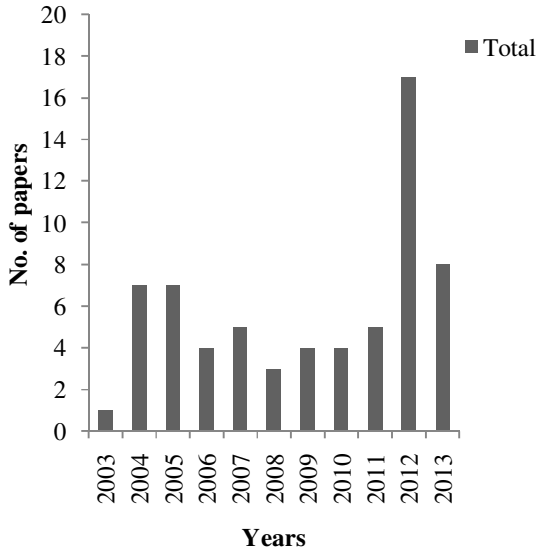

Figure 1: No. of papers vs. Years

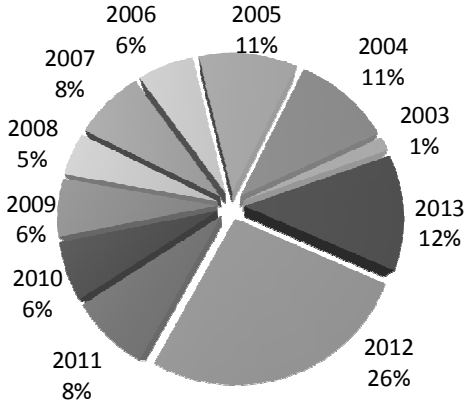

Fig 2: Percentages of papers in a year

Out of 65 papers collected for survey it was founded that almost 24 papers used the LSB technique as it provides the alternative ways to tackle different complex situations. Strong and weak points of the papers were briefly mentioned in literature for the prior knowledge of the beginners. In 2013 some of the authors used the LSB technique with AES and DES technique of cryptography which increased the data security level by encryption. Some of authors made the use of Spatial domain, Transform domain, Double JPEG compression, Improved RSTEG algorithm, TCP, SITMSVC, RIPEMD, BRGC, ARP, HICCUPS, CSMA/CA, MQIM, OPA, PCA, DMC, Watermarking, ANOVA, CBER, VBER, MHPDM, Distortion techniques, Masking and Filtering etc. techniques in their work which provide more strong ways to secure the transmission of information through internet. Even some of the authors overcome the limitation of the existing techniques of the previous papers in their papers.

Also it was clearly reflected that the interest of the researchers in the field of steganography was not consistent, in some years researchers showed least interest but in some years they showed very much interest, it might be due to the unavailability of the resources they need or they knew less about this field. It was also found that some the techniques have common concepts and type of methodologies, some of the authors gave new or different methodologies and applications. Some of the applications also provide a greater opportunity for the use of different steganography techniques such as Uyghur text; Markov reduced feature, Rich models, Genetic algorithm, Henon map, BPCS etc. Some authors revised the old methods instead of using the existing one.

Furthermore, all the papers discussed here were sourced from IEEE Explore. All the information collected in this survey retains their year values, as all the papers were arranged on year scale. The importance of steganography for various applications is very useful and effective in our opinion. Some of the papers were very good and highly effective for the future work, they can provide a better platform for the beginners to work in this field. They have no need to read the all papers completely. They just need to go through this review paper and may get some ideas for their work. No doubt other tools can also provide a best information security but its importance can't be ignored as it provides very beneficial results.

4. Conclusion

This paper presents a literature review on various steganography techniques from 2003 to 2013. The search was made by using keywords: steganography, steganography techniques, steganography methods, steganography detection, steganography algorithm, etc. It is concluded that at the starting period of 2003 researchers showed least interest in steganography but as time passes the level of their interest raises, in 2012 and 2013 researchers shown much interest It was also seen that most of the papers used the LSB technique, especially in 2012 and 2013 maximum papers are based on LSB steganography technique, also some researchers used some cryptographic techniques along with steganography techniques and several other techniques were also used.This study may provide some prior knowledge to the beginners who want to work in steganography. By examining advantages and limitations of the existing techniques one can generate a better techniques or can used in some different ways or can improved the existing one. As the research in

the field of steganography is an ongoing process. It will set a better platform for the beginners. By going through this survey paper beginners surely get some ideas for the future research in steganography.

References

[1] F. I Alam, and M. M Islam,"An investigation into image hiding steganography with digital signature framework," Informatics, Electronics & Vision (ICIEV), 2013 international conference on 17-18 May 2013, page(s):1-6.

[2] W. W Zin, and T. N Soe," Implementation and analysis of three steganographic approaches," Computer research and development (ICCRD), 2011 3rd international conference on (Volume: 2) 11-13 March 2011, page(s):456-460.

[3] S. Thenmozhi, and M. Chandrasekaran," A novel technique for image steganography using nonlinear chaotic map," Intelligent systems and control (ISCO), 2013 7th international conference on 4-5 Jan. 2013,page(s):307-311.

[4] M. K Ramaiya, N. Hemrajani, and A. K Saxena," Improvisation of security aspect in steganography applying DES," Communication systems and network technologies (CSNT), 2013 international conference on 6-8 April 2013, page(s):431-436.

[5] Y. J Chanu, T. Tuithung, and K. M Singh," A short survey on image steganography and steganalysis techniques," Emerging trends and applications in computer science (NCETACS), 2012 3rd national conference on 30-31 March 2012,page(s):52-55.

[6] S. Mahato,D. K Yadav, and D. A Khan," A modified approach to text steganography using hypertext markup language," Advanced computing and communication technologies (ACCT), 2013 third international conference on 6-7 April 2013, page(s):40-44.

[7] R. Jose, and G. Abraham, "A separable reversible data hiding in encrypted image with improved performance, "Emerging research areas and 2013 international conference on microelectronics, communications and renewable energy (AICERA/ICMiCR), 2013 annual international conference on 4-6 June 2013,page(s):1-5.

[8] S Usha, G A Kumal, and K Boopathybagan, "A secure triple level encryption method using cryptography and steganography, "Computer science and network technology (ICCSNT), 2011 international conference on (Volume:2) 24-26 Dec. 2011,page(s):1017-1020.

[9] P. Kadam, A. Kandhare, M. Nawale, and M. Patil, "Separable reversible encrypted data hiding in encrypted image using AES algorithm and lossy technique, "Pattern recognition, Informatics and medical engineering (PRIME), 2013 international conference on 21-22 Feb. 2013,page(s):312-316.

[10] S. P. Bansod, V. M. Mane, and L. R. Ragha," Modified BPCS steganography using hybrid cryptography for improving data embedding capacity," Communication, information & computing technology (ICCICT), 2012 international conference on 19-20 Oct. 2012,page(s):1-6.

[11] Y. Zheng, F. Liu, X. Luo, and C. Yang, "A method based on feature matching to identify steganography software, "Multimedia information networking and security (MINES), 2012 fourth international conference on 2-4 Nov. 2012,page(s):989-994.

[12] S. Manoharan, "Steganalysis of synthetic low-colour images, "Information theory and its applications (ISITA), 2012 international symposium on 28-31 Oct. 2012,page(s):784-788.

[13] J. Yang, and S. Pingzhong, "A JPEG image blind steganography detection method using KCCA feature fusion, "Wavelet analysis and pattern recognition (ICWAPR), 2012 international conference on 15-17 July 2012,page(s):222-226.

[14] Y. F. Zhou, W. W.Y.NG, and Z. M. He,"Effects of double JPEG compression on steganalysis, "Wavelet analysis and pattern recognition (ICWAPR), 2012 international conference on 15-17 July 2012,page(s):106-112.

[15] S. F. Mare, M. Vladutiu, and L. Prodan,"High capacity steganographic algorithm based on payload adaptation and optimization,"Applied computational intelligence and informatics (SACI), 2012 7th IEEE international symposium on 24-26 May 2012,page(s):87-92.

[16] J. Zhai, G. Liu, and Y. Dai, "An improved retransmission steganography and its detection algorithm, "Multimedia information networking and security (MINES), 2011 third international conference on 4-6 Nov. 2011,page(s):628-632.

[17] F. Zhou, R. Yang, Z. Zheng, and J. He, "Steganography in multimedia messaging service of mobile intelligent terminal, "Image and signal processing (CISP), 2012 5th international congress on 16-18 Oct. 2012,page(s):1340-1343.

[18] H. Motamedi, and A. Jafari, "A new image steganography based on denoising methods in wavelet domain, "Information security and cryptology (ISCISC), 2012 9th international ISC conference on 13-14 Sept. 2012,page(s):18-25.

[19] H. S. M. Reddy, N Sathisha, A. Kumad, and K. B. Raja, "Secure steganography using hybrid domain technique, "Computing communication & networking technologies (ICCCNT), 2012 third international conference on 26-28 July 2012,page(s):1-11.

[20] M. Talip, A. Jamal, and G. W. Qiang, "A proposed steganography method to uyghur script, "Cyber-enabled distributed computing and knowledge discovery (CyberC), 2012 international conference on 10-12 Oct. 2012,page(s):125-128.

[21] S. Das, P. Bandyopadhyay, Prof. A. Chaudhuri and Dr. M. Banerjee, "A secured key-based digital text passing system through color image pixels, "Advances in engineering, science and management (ICAESM), 2012 international conference on 30-31 March 2012,page(s):320-325.

[22] S. Premkumar, and A. E. Narayanan, "New visual steganography scheme for secure banking application, "Computing, electronics and electrical technologies (ICCEET), 2012 international conference on 21-22 March 2012,page(s): 1013-1016.

[23] J. Fridrich, and J. Kodovsky ,"Rich models for steganalysis of digital images, "Information forensics and security, IEEE transactions on (Volume:7 , Issue: 3) June 2012,page(s):868-882.

[24] T. Pevny, J. Fridrich, and A. D. Ker, "From blind to quantitative steganalysis, "Information forensics and security, IEEE transactions on (Volume:7 , Issue: 2) April 2012,page(s):445-454.

[25] J. K. Mandal, and S. Ghatak, " Secret image/message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC), "Recent trends in

information technology (ICRTIT), 2011 international conference on 3-5 June 2011,page(s):263-268.

[26] C.R Geetha, S. Basavaraju, and Dr. C. Puttamadappa, "Variable load image steganography using multiple edge detection and minimum error replacement method, "Information & communication technologies (ICT), 2013 IEEE conference on 11-12 April 2013,page(s):53-58.

[27] A. Danti, and G. R. Manjula, "Secured data hiding of invariant sized secrete image based on discrete and hybrid wavelet transform, "Computational intelligence & computing research (ICCIC), 2012 IEEE international conference on 18-20 Dec. 2012,page(s):1-6.

[28] Dr. D. Samidha, and D. Agrawal, "Random image steganography in spatial domain, "Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on 7-9 Jan. 2013,page(s):1-3.

[29] A. Sanchez, A. Conci, E. Zeljkovic, N. Behlilovic, and V. Karahodzic, "A new approach to relatively short message steganography, "Telecommunications (BIHTEL), 2012 IX international symposium on 25-27 Oct. 2012,page(s):1-4.

[30] G. K. Seivi, L. Mariadhasan, and K. L. Shunmuganathan, "Steganography using edge adaptive image, "Computing, electronics and electrical technologies (ICCEET), 2012 international conference on 21-22 March 2012,page(s):1023-1027.

[31] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "Information hiding using improper frame padding, "Telecommunications network strategy and planning symposium (NETWORKS), 2010 14th international conference on 27-30 Sept. 2010,page(s):1-6.

[32] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Towards objectifying information hiding, "Acoustics speech and signal processing (ICASSP), 2010 IEEE international conference on 14-19 March 2010,page(s):1770-1773.

[33] M. Afrakhteh, and S, Ibrahim,"Enhanced least significant bit scheme robust against chi-squared attack,"Mathematical/analytical modelling and computer simulation (AMS), 2010 fourth asia international conference on 26-28 May 2010,page(s):286-290.

[34] Y. Sun, and F. Liu, "Selecting cover for image steganography by correlation coefficient, "Education technology and computer science (ETCS), 2010 second international workshop on (Volume:2) 6-7 March 2010,page(s):159-162.

[35] K. Szczypiorski,"A performance analysis of HICCUPS – a steganographic system for WLAN,"Multimedia information networking and security, 2009. MINES '09. International conference on (Volume: 1) 18-20 Nov. 2009, page(s):569-572.

[36] QI Ke, X. D. qing, and Z. D. fang, "An adaptive high-capacity steganographic algorithm for 3D models, "Information technology and computer science, 2009. ITCS 2009. international conference on (Volume:1) 25-26 July 2009,page(s):162-166.

[37] A. Almohammad, G. Ghinea, and R. M. Hierons,"JPEG steganography:a performance evaluation of quantization tables, "Advanced information networking and applications, 2009. AINA '09. International conference on 26-29 May 2009,page(s):471-478.

[38] R. O. E Safy, H. H. Zayed, and A. E. Dessouki,"An adaptive steganographic technique based on integer wavelet transform,"Networking and media convergence, 2009. ICNM 2009. International conference on 24-25 March 2009, page(s):111-117.

[39] S. Geetha, S. S. S. Sindhu, and N. Kamaraj,"Stego-breaker:Defeating the steganographic systems through genetic-X-means approach using image muality Metrics, "Advanced computing and communications, 2008. ADCOM 2008. 16th international conference on 14-17 Dec. 2008,page(s):382-391.

[40] M. C.Chen, S. S. Agaian, C. L. P. Chen, and B. M. Rodriguez,"Steganography detection using RBFNN,"Machine learning and cybernetics, 2008 international conference on (Volume:7) 12-15 July 2008,page(s):3720-3725.

[41] B. Ryabko, and D. Ryabko,"Information-theoretic approach to steganographic systems,"Information theory, 2007. ISIT 2007. IEEE international symposium on 24-29 June 2007, page(s):2461-2464.

[42] Y. Wang, and P. Moulin,"Perfectly secure steganography: Capacity, error exponents, and code constructions,"Information theory, IEEE transactions on (Volume: 54, Issue: 6) June 2008, page(s):2706-2722.

[43] R. Böhme, and C. Keiler,"On the security of "A steganographic scheme for secure communications based on the chaos and the euler theorem,"Multimedia, IEEE transactions on (Volume:9 , Issue: 6) Oct. 2007,page(s):1325-1329.

[44] K B Raja, Vikas, K. R. Venugopal, and L. M. Patnaik,"High capacity lossless secure image steganography using wavelets,"Advanced computing and communications, 2006. ADCOM 2006. International conference on 20-23 Dec. 2006, page(s):230-235.

[45] Z. Deng, X. Shao, and Z. Yang,"A novel approach to detect the presence of LSB steganographic messages,"Software engineering, artificial intelligence, networking, and parallel/distributed computing, 2007. SNPD 2007. eighth ACIS international conference on (Volume:3) July 30 2007-Aug. 1 2007,page(s):404-408.

[46] S. S. Agaian, and R. C. Cherukuri,"Adaptive steganographic system for binary images using variable block embedding rate,"Systems, man and cybernetics, 2006. SMC '06. IEEE international conference on (Volume: 3) 8-11 Oct. 2006,page(s):1879-1883.

[47] Y. Q. Shi, C. Chen, W. Chen, and M. P. Kaundinya,"Effect of recompression on attacking JPEG steganographic schemes ─ An experimental study,"Circuits and systems, 2007. ISCAS 2007. IEEE international symposium on 27-30 May 2007, page(s):1265-1268.

[48] A. Savoldi, and P. Gubian,"Data hiding in SIM/USIM cards: A steganographic approach,"Systematic approaches to digital forensic engineering, 2007. SADFE 2007. second international workshop on 10-12 April 2007,page(s):86-100.

[49] X. Zhang, and S. Wang,"Efficient steganographic embedding by exploiting modification direction, "Communications (Volume:10 , Issue: 11) November 2006,page(s):781-783.

[50] M. Niimi, H. Noda, and B. Segee," A robust BPCS-steganography against the visual attack,"Information,

communications and signal processing, 2005 fifth international conference,page(s):1116-1120.

[51] X. Kong, Z. Wang, and X. You,"Steganalysis of palette images: Attack optimal parity assignment algorithm,"Information, communications and signal processing, 2005 fifth international conference,page(s):860-864.

[52] K. B. Raja, C. R. Chowdary, K. R. Venugopal, and L. M. Patnaik,"A secure image steganography using LSB, DCT and Compression techniques on raw images, "Intelligent 14-17 Dec. 2005, page(s):170-176.

[53] Y. T. Wu, and F. Y. Shih,"Genetic algorithm based methodology for breaking the steganalytic systems,"Systems, man, and cybernetics, part B: Cybernetics, IEEE transactions on (Volume: 36, Issue: 1) Feb. 2006,page(s):24-31.

[54] X. Luo, B. Liu, and F. Liu," Detecting LSB steganography based on dynamic masks, "Intelligent 8-10 Sept. 2005,page(s):251-255.

[55] A. Martín, G. Sapiro, and G. Seroussi,"Is image steganography natural?,"Image processing, IEEE transactions on (Volume:14 , Issue: 12) Dec. 2005,page(s):2040-2050.

[56] A. Adli and Z. Nakao,"Three steganography algorithms for MIDI files,"Machine learning and cybernetics, 2005. Proceedings of 2005 international conference on (Volume:4) 18-21 Aug. 2005,page(s):2401-2404.

[57] H. Dou, H. Zhang, and S. Zhan,"Independent components analysis applied to steganalysis,"Signal processing, 2004. Proceedings. ICSP '04. 2004 7th international conference on (Volume: 3) 31 Aug.-4 Sept. 2004, page(s):2498-2501.

[58] M. A. Khan,V. Potdar, and E. Chang," An architecture platform for grey level modification steganography system," Industrial electronics society, 2004. IECON 2004. 30th annual conference of IEEE (Volume:1) 2-6 Nov. 2004,page(s):463-471.

[59] X. G. Sui, and H. Lilo, "A new .steganography method based on hypertext, "Radio 24-27 Aug. 2004,page(s):181-184.

[60] M. Jiang, N. Memon, E. Wong, and X. Wu, "Quantitative steganalysis of binary images," Image processing, 2004. ICIP '04. 2004 international conference on (Volume: 1) 24-27 Oct. 2004,page(s):29-32.

[61] V. M. Potdar, and E. Chang, "Grey level modification steganography for secret communication," Industrial informatics, 2004. INDIN '04. 2004 2nd IEEE international conference on 26-26 June 2004, page(s):223-228.

[62] S. M. Ashar, T. M. Shah, and R. Khalid,"Message encryption with image processing,"Multi topic conference, 2003. INMIC 2003. 7th international 9-9 Dec. 2003, page(s):7-15.

[63] L. Zhi, and S. A. Fen, "Detection of random LSB image steganography," Vehicular technology conference, 2004. VTC2004-Fall. 2004 IEEE 60th (Volume:3) 26-29 Sept. 2004,page(s):2113-2117.

[64] S. Trivedi, and R. Chandramouli, "Secret key estimation in sequential steganography," Signal processing, IEEE transactions on (Volume:53 , Issue: 2) Feb. 2005,page(s):746-757.

[65] A. H. Sung, G. R. Tadiparthi, and S. Mukkamala, "Defeating the current steganalysis techniques (Robust Steganography)," Information technology: Coding and computing, 2004. Proceedings. ITCC 2004. International conference on (Volume:1) 5-7 April 2004, page(s):440-444.