A Review on current Methods and application of Digital image Steganography

Chandan Mohapatra* And Manjusha Pandey**

Department of Computer Science, KIIT University, Bhubaneswar*
Assistant Professor, School of Computer Engineering, KIIT University, Bhubaneswar**

ABSTRACT:
Now a days, people mostly use internet to send and receive data because it is accurate, easier and faster than all other data communication techniques. But the main lacuna of this technique for sharing of information is its security. Different techniques are evolved to overcome this problem. Steganography is one of the most effective technique among them for secure data communication. Steganography is the art and science of invisible communication of secrete data in an appropriate multimedia carrier like within image, audio or video files. This technique follows a simple principle i:e if the feature is not visible, the point of attack could not be identified, therefore this technique always conceals the existence of embedded data. Steganography has a large number of useful application and one of the most important characteristics of this technique is its robustness which makes it extraordinary among all other techniques. This paper exposes different type of existing steganographic methods and its techniques along with its application and features.

I. INTRODUCTION

Since many years, people tried to invent and develop innovative methods for secrete communication. Even if in the ancient age, people used to write secrete information on the shaved skull of a man and allow his hair to grow up. Then the person had been sent to the point of destination. At the destination, the secrete information was collected after shaving the hair from the skull of that person. Another method called Cardan Grille was used to transfer secretes information. Here some holes are created in a paper and that is shared among the parties. Then by placing that paper over another paper, the secrete message was written through the holes and rest of the places of the paper are filled by different words. Now receiver get this secrete message by using that same mask on the received paper as shown in fig.[1].

Here the main aim is to hide the secrete information. In this digital era also, for information security, the main aim should be to hide the information. Steganography is used to do the same i:e it kept existence of the message secrete. It hides the secrete information in the multimedia carrier like image, audio, video etc.

Image is one of the most useful and cost effective carrier for this. An image not only contain the information what the human can able to see in the naked eye, but also it can have different secrete messages or any different secrete image which can be retrieved by using the pixel value through a specific procedure.

The mass media named the year of 2011 as the "year of hack" because a huge number of data security breaches in private companies as well as in government sectors and the estimated amount of the volume of the stolen data is in petabytes i:e millions of gigabyte[2]. Unaware user is mostly responsible for this as they open specially crafted email message which creates a back door open for the victims' computer. Another reason is to connect a web site and download HTML or JPEG files which were encoded with command earlier time. So these type of files can easily passed through the firewalls.

For that reason, numerous steganography method and techniques are proposed after that. Main discussion of this paper is about those steganography methods and techniques along with their advantages and applications which will gives a overall brief idea on steganography. Section 2 will give a brief idea about steganography application and section 3 describes different steganography methods. After that, in section 4 we discussed about the techniques used in detail. Section 5 will give conclusion

II. STEGANOGRAPHY APPLICATION

Whenever there is a requirement to hide data, steganography can be used. One of the measure advantages of this technique is whether the image is suspected or not, no one can prove about involvement of the image caring secreting information. Some of the most useful application are as follows. It provides confidential communication and secrete storing of data, provides protection for data alternation so that people can send their digital certificate data or any important document to anywhere in the world. It provides access control system upto some extend so that only appropriate owner of the document can able to view. It is very useful in copyright control of materials, TV broadcasting, in medical image processing where the details of individual are embedded in their photograph or reports. A unique ID can be embedded to image also for analyzing network traffic of a particular user[1].

Now a day, steganography methods used in Telecommunication network and it is termed as network steganography which is applied to IP Telephony. This techniques hides the information in any layer f TCP/IP protocol stack[3].

Steganography works more efficiently if it is applied to encrypted form of secrete data. Terrorist are also using steganography for their secrete communication and it is very difficult to trace out.

III. STEGANOGRAPHY METHODS:

In internet, gif (graphics interchange format), jpeg(joint photographic expert group) and png(portable network groups) are the mostly used image format. All the steganographic techniques work on the structure of these format. Here we are defining the general process of steganography. At first the cover image has to be selected and then the secrete message is merged in cover image and that newly formed image is called stego image. The sender must have merging algorithm and the receiver must have retrieving algorithm.

On the basis of paper followed in this review, we categorized steganography methods into 3 types i:e spatial domain, frequency domain and adaptive methods. Inspite of these three methods, several methods are also there but we only considered widely used methods. Spatial domain directly deals with the location of the pixel and generally works on Least significant bit(LSB). Frequency domain method use DCT(discreet cosine transform), FT(Fourier Transform), DWT(Discreet Wavelet Transform) for merging of secrete message. Recently adaptive method is developed. This method can be applied in booth spatial domain and frequency domain.

IV. DISCUSSION

Here some measure image steganography algorithm and techniques are discussed along with their feature and application based on the image spatial domain, frequency domain and adaptive methods.

Guo-Shiang Lin et al. proposed a technique in the year of 2010 for enhancing the picture quality as well as face steganalysis problem[4]. They used Quantisation based image stegangraphy for optimising picture quality. They designed a close loop computing framework that iteratively searches for proper modification of pixel value and its coefficient. This optimize the visual quality of the stego image and this method is particularly suitable where the secrete message information is spread to multiple pixel and coefficient. But this method is not universally applicable to all other steganograpy technique.

Fangjun Huang et al. proposed a technique to minimize detectable distortion in data hiding in the year of 2012[5]. A new channel selection rule was introduced by author for JPEG image by considering Quantisation step, Magnitude of quantized Discrete cosine transform(DCT) coefficient(MQ), Perturbation error(PE). This technique provide higher security performance, minimize distortion and it is easy to conduct. This technique application is suitable for MME2 and MME3.

S.Premkumar et al. proposed a technique for secure banking application in the year of 2012 where the password of the costumer is encoded by using all eight adjacent neighbour pixel around the target pixel and then divideing this into share. Some share is given to costumer and some share is kept by bank. While transaction, to costumer has to produce their share and then by examining these shares along with bank shares, the costumer is authenticated[6]. Here, this technique provides costumer authentication as well as both cryptography and steganography is used through image processing for better imperceptibility and security.

Saeed Sarreshtedari et al. proposed a technique of one third embedding in the year of 2013 which reduces the probability of changing the pixel value of each pixel for embedding of data to one third of it without sacrificing the embedding capacity[7]. This technique offers the embedding capacity of exactly one bit per pixel with improved imperceptibility and higher robustness to the well known LSB detector. Here stego image is more similar to cover image so that embedding is less detectable. It also provides high embedding capacity and preserves the histogram as much as possible.

Weiqi Luo et al. proposed an effective method to detect the quantization table and then a quantitative method is proposed to estimate the length of spatial modification in those gray scale image[8]. This provides increase in imperceptibility of the image and better security because hackers assume that jpeg steganography based on predefined quantisation table.

Linjie Guo et al. introduced some new uniform embedding distortion(UED) function in the year of 2014[9]. Instead of random modification, this technique uses syndrome trellis coding to determine codeword which minimizes distortion for a given message with appropriate UED. Here author tries to spread the embedding modification uniformly which will quantize

the DCT coefficient of all possible magnitude. This technique leads to less statistical detectability and secure embedding capacity.
In the year of 2011, Wei-Jen Wang et al. proposed a technique for embedding a secrete data into a vector quantisation(VQ) based image which provides more capacity for embedding of secrete data.

Chung-Min Yu et al. proposed a technique in the year of 2011 where secrete message can be embedded into high dynamic range(HDR) of image encoded with radiance RGBE format. The stego image which will be produce is also a high dynamic range image. This is the first approach using HDR image which provides a high capacity of distortion free data embedding. proposed method can hide different amount off homogeneous secrete message which perform adaptive message embedding. One another measure advantage is this technique produce a very small difference between the pixel of stego image and the cover HDR image which increase the difficulty of attacker because they could not able to know whether a hidden message is present or not in the HDR image and also message can be extracted with out referring to the original cover HDR image.

Qian Mao proposed a technique based on spatial method using matrix embedding in the year of 2014[12].This techniques encodes the cover as well as secrete message with an error correction code and modifies the cover image according to the coding result. Here computational complexity is decreased, increase in efficiency and enhanced security. Also the size of the table for embedding is decreased.

Mingwei Tang et al. uses multilayer embedding and improved image interpolation method to propose a high capacitive reversible steganography technique[13]. The difference between neighbouring pixel value is used for data hiding. This enhance the performance of information hiding system with less computational complexity and good quality image also having good PSNR.

Kang Wang et al. proposed a technique for high capacitive reversible data hiding method for JPEG compressed image in the year of 2013 where they modify quantisation table and quantized DCT coefficients[14]. At first the JPEG image is compressed according to DCT compression method. After that they choose a integer and the quantisation table is divided with that integer and DCT coefficient is multiplied with that same integer. Then they add adjustment value to make space for data. They also utilize k-ary based modulo operation. This provides the control of increase in file size after hiding the data. The PSNR value between the original image and the stego image is high, high capacity of embedding data with smaller distortion and most importantly original jpeg cover image can be extracted.

Kazem Qazanfari et al. proposed a technique in the year of 2014 to improve LSB+ technique[15]. This technique prohibits some pixel from changing for reduction of extra bits. Sensitive pixels are distinguished and protect them from extra bit embedding. This provides improved visual quality due to elimination of extra bit, lower distortion in co-occurrence matrix. Histogram is also preserved and no effect to statistical and perceptual attribute of the cover image. So histogram based attack could not be succeed.

Chia-Chun Wu et al. proposed optimal pixel adjustment process in the year of 2011[16]. They used a distinct image identification number as the input of polynomial and keep it as private key for each participant. Only legal participant can retrieve the image identification number as they are having the private key. This method provides high authentication ability with improved image quality but the original cover image could not be recovered from the stego image.

Hamidreza Rashidy Kanan et al. proposed a tuneable visual image quality and data lossless method in spatial domain based on genetic algorithm[17]. Genetic algorithm is used to find proper starting point. Here, the best place for embedding the secrete data in host image is found out to achieve high level security. This allow us to find out the best place in host image for embedding modified secrete data. This technique provides high embedding capacity and enhance the PSNR of the stego image. It also increase the image quality.

Anastasia Ioannidou et al. proposed a technique in the year of 2012 where the advantages of sharp area of the image is used to hide large amount of data[18]. Here a hybrid edge detector and a high payload technique is used for colour image which includes fuzzy edge detector and canny edge detector. Change in smooth areas can easily noticeable in human eye but as it uses sharp areas, it increase imperceptibility. It also provides higher PSNR for embedded image.

M.Ghebleh et al. proposed a lifted wavelet discrete transformation based steganography technique which ensures integer to integer transformation and it uses a 3D chaotic cat map[19]. The irregular output of the cat map is used to embedded secrete message in the digital cover image and DWT is used to provide high robustness. It is fast, efficient, flexible, highly sensitive to its secrete key and guranteed lossless extraction of hidden information.

S.M. Elshoura et al. proposed a technique for secure high capacity image information hiding where two full separate arbitrary full-scale gray level images used, one is for hidden information image and another is authentication watermark image which is hidden or embedded in the Tchebichef moments of a carrier image with very high imperceptibility[20]. Here second watermark used for identification, content integrity verification and authentication of hidden secrete message. It sends 3 block based watermarked image with the same information embedded in them but with different mining weight. these three watermarked image looks same to the naked eye. This provides high tampering detection, high quality recovered hidden image, high accuracy, authentication and security.

Rengarajan Amirtharajan et al. proposed a technique where random k-bit embedding approach is used[21]. Here the original cover is divided into non overlapping blocks of equal size. Then the encrypted confidential data are embedded in each block through four different random walks. A particular random walk which provides minimum degradation for a particular block is fixed for that block. This is recorded for each block and kept it as secrete key. Due to this, it provides robustness and enhance the quality of the stego image.

Ratnakirti Roy et al. proposed an edge adaptive image steganography technique which combines matrix encoding and LSBM for embedding in the edge regions of a cover image[22]. This also use cat chaotic mapping to distort the payload. The payload is restorable only by supplying correct key. This technique provides high fidelity and imperceptibility, performs better LSBR and PVD. But it decrease the data embedding capacity.

V. Nagaraja et al. proposed a technique in the year of 2013 for data hiding by pixel value modification and modulus function in colour image[23]. This method guarantees that no pixel value will exceed the range 0-255 in stego image. And also here one secrete digit is embedded only in one pixel which increase capacity of embedding. It also provides high visual quality and security in colour images.

D.Biswas et al. proposed a steganography technique where dithering technique is used which is basically the process of creating an indexed image approximation in the RGB image and the array RGB by dithering the colours in colour map[24]. Here the retrieved image quality is almost same as the original image quality.

Li Fan et al. proposed in the year of 2013 which directly alters the pixel value in the image instead of flipping the binary bit in the LSB plane[25]. For this, adding and subtracting any value to or from the modular sum by changing at most one pixel which increase embedding efficiently to large extend. Here the security vulnerability of Tseng's scheme is used. It provides good performance and better embedding rate.

Pei-Yu Lin et al. proposed a technique where invertible sharing approach is used so that the secrete image is lossless and the distorted stego iamge can be able to retrieve back to the original cover iamge[26]. To use this, first the secrete pixel is transformed into many rotational system and then calculate the information data used to reconstruct original pixel from common flagged pixel such that the information data and the transformed secrete data are shared using the (t,n)-threshold sharing scheme. Main feature of this technique is it provides no distortion in secrete image and lossless secrete image with large amount of data embedding capacity.

Der-Chyuan Lou et al. introduced a technique for cover selection, pixel grouping and dynamic secrete key adjustment[27]. Here steganography method based on RHTF(Reversible histogram transform function) used to maintain statistical features. This provides improved security, helpful against statistical and regular singular(RS) attack specially under higher embedding rate.

Wafaa Mustafa Abduallah et al. proposed a transformed method based on irreducible polynomial mathematics[28]. After dividing a colour image into blocks, then by applying the proposed transformed method to the specify block and hiding the secrete message with these. This provides improved security as it uses different type of transform for each block. It provide high embedding capacity, acceptable visual quality image with reasonable level of imperceptibility. Time complexity is also reasonable and overall PSNR is improved.

Nameer N.El-Emam proposed a technique where hybrid adaptive neural network with modified adaptive genetic algorithm is used. Here non uniform adaptive image segmentation is done with an intelligent technique[29]. This technique hides a large amount of confidential data into colour image. Here 4 secrete bits per byte can be embedded with better visual quality. Here four security layers are proposed to work against statistical and visual attack. Proposed technique speed up the training process, therefore high rate of data hiding as well as better imperceptibility is achieved.

Z.Eslami et.al proposed a technique in the year of 2010 for secrete image sharing based on cellular automata[30]. They also used digital signature and hash function with double authentication mechanism. This provides no distortion to original secrete image. At most two bits of the pixel can be changed in the given cover image to maintains its visual quality. Integrity also can be achieved of the stego image without processing its blocks.

Soumendu Chakraborty et al. proposed a technique in the year of 2013 where the payload is gray scale image and this is divided into frequency matrix, error matrix and sign matrix[31]. Downscale frequency matrix is obtained from frequency matrix using matrix algorithm. These DSM, EM and SM are embedded in different cover images using X-Or operation between the bit plane of the matrixes and the respective cover image. In the absence of standard encryption technique, it provides high level of confidentiality which minimizes the computational complexity and minimum computational time.

Z.Eslami et al. proposed a technique in the year of 2011 based on the polynomials. Here the secrete bits are embedded in predetermined fixed size block of each cover image[32]. The block size of the cover image determined dynamically according to the size of the hidden data. All the capacity of cover image is utilised, and it is suitable for the use for the authentication purpose.

Hai-Dong Yuan proposed two secrete sharing method which hides the secrete bits adaptively among texture region of cover by a spatial $^{+}$-1 operation[33]. This provide protection from steganalysis technique, difficult to detect and we can embedded location sensitive secrete.

S.Geetha et.al proposed a scheme based on renowned numerical model[34]. Here the data which is to be embedded is dissected into numerals each having variable information carrying capacity. The dissection is based on the amount of adulteration that a pixel can tolerate. This provides efficient visual quality despite of high payload capacity. It is also resistance to RS steganalysis and offer high visual quality in comparison to typical LSB based scheme.

A short and simple representation of the above discussion is given in this following table.

Name Of Author	Year of publication	Steganography Method	Proposed Technique	Features
Guo-Shiang Lin et al.[4]	August 2010	Adaptive	Closed loop computing framework which searches proper modification of pixel value and its coefficient	Better picture quality but not universal to all the techniques suitable where the secrete message information is spread to multiple pixel and coefficient
Fangjun Huang et al.[5]	August 2012	Frequency domain	A new channel selection rule considering QS, MQ & PE.	Higher security performance, Easy to conduct and minimize distortion
S.Premkumar et al.[6]	2012	Spatial domain	the password of the costumer is encoded by using all eight adjacent neighbour pixel around the target pixel	Provides costumer authentication, improved imperceptibility and better security
Saeed Sarreshtedari et al.[7]	July 2013	Spatial domain	One third LSB embedding	Capacity of embedding exactly one bit per pixel, higher robustness against well known LSB detector Preserves the histogram
Weiqi Luo et al.[8]	January 2011	Spatial domain	to detect the quantization table and then a quantitative method is proposed to estimate the length of spatial modification	Better imperceptibility and security
Linjie Guo et al.[9]	May 2014	Frequency domain	Syndrom trellis coding is used to determine the code word which minimizes distortion	Less statistical detectability and secure embedding capacity against steganalysis

Wei-Jen Wang et al.[10]	December 2011	Vector Quantisation based	Embedding secrete data into a cover VQ based image	Can embedded more secrete data in comparison to other
Chung-Min Yu et al.[11]	February 2011	Adaptive	Secrete message can be embedded into high dynamic rang images encoded with radiance RGBE	High capacity of distortion free data embedding, produce a very small difference between the pixel of stego image and the cover image.
Qian Mao[12]	2014	Spatial domain	Uses matrix embedding for both cover and secrete message with an error correction code.	Computational complexity decreases, efficiency and security increases.
Mingwei Tang et al.[13]	2014	Spatial domain	Uses multilayer embedding and the difference between neighbouring pixel values.	Having good PSNR with low computational complexity and good quality image
Kan Wang et al.[14]	2013	Frequency domain	High capacitive data hiding method by modifying quantisation table and quantised DCT	Control the increase of file size after embedding data, high PSNR between original and stego image, high image quality with smaller distortion
Kazem Qazanfari et al.[15]	2014	Adaptive	prohibits some sensitive pixel from changing for reduction of extra bits embedding	Lower distortion, histogram is preserved, no effect to statistical and perceptual attribute.
Chia-Chun Wu et al[16]	2011	Adaptive	Optimal pixel adjustment process	High authentication ability, improved image quality but original cover image could not be recovered

Hamidreza Rashidy Kanan et al[17]	2014	Spatial domain	a tuneable visual image quality and data lossless method in spatial domain based on GA.	allow us to find out the best place in host image for embedding, improved image quality and PSNR
Anastasia Ioannidou et al.[18]	2012	Spatial domain	advantages of sharp area of the image is used to hide large amount of data using hybrid edge detector and a high payload technique	it increase imperceptibility, provides higher PSNR for embedded image.
M.Ghebleh et al.[19]	2014	Frequency domain	a lifted wavelet discrete transformation based steganography technique which ensures integer to integer transformation and it uses a 3D chaotic cat map.	Fast, efficient, flexible, highly robust and give guarantee for lossless extraction of hidden information
S.M. Elshoura et al[20]	2013	Spatial domain	secure high capacity image information hiding where two full separate arbitrary full-scale gray level images used, one is for hidden information image and another is authentication watermark image.	provides high tampering detection, high quality recovered hidden image, high accuracy, authentication and security.

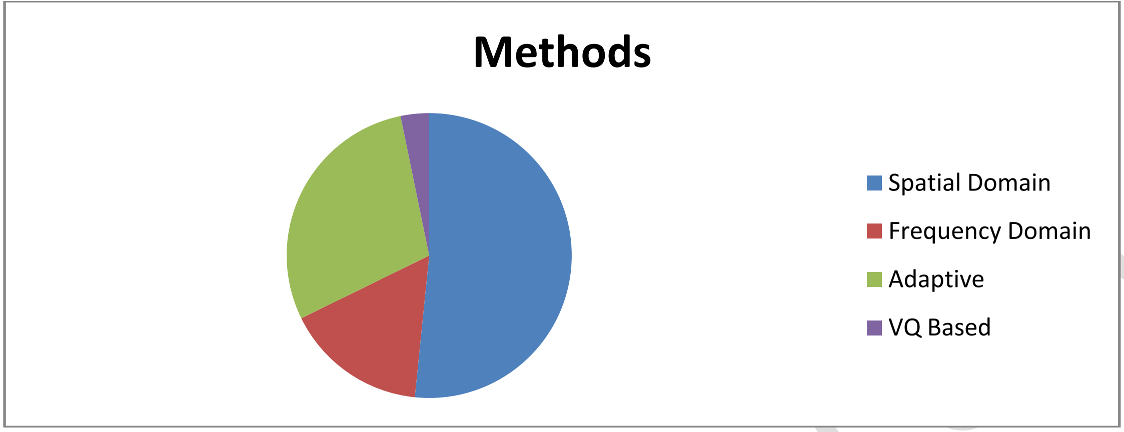
Rengarajan Amirtharajan et al.[21]	2012	Adaptive	random k-bit embedding approach used, original cover is divided into non overlapping blocks of equal size. encrypted confidential data are embedded in each block through four different random walks	it provides robustness and enhance the quality of the stego image.
Ratnakirti Roy et al.[22]	2013	Adaptive	edge adaptive image steganography technique which combines matrix encoding and LSBM for embedding in the edge regions of a cover image	provides high fidelity and imperceptibility, performs better LSBR and PVD.
V.Nagaraja et al.[23]	2013	Spatial domain	data hiding by pixel value modification and modulus function in colour image and one secrete digit is embedded only in one pixel.	no pixel value will exceed the range 0-255 in stego image, which increase capacity of embedding, provides high visual quality and security in colour images.
D. Biswas et al.[24]	2012	Spatial domain	dithering technique is used which is basically the process of creating an indexed image approximation in the RGB image and the array RGB by dithering the colours in colour map	the retrieved image quality is almost same as the original image quality.

Li Fan et al.[25]	2013	Spatial domain	directly alters the pixel value in the image instead of flipping the binary bit in the LSB plane.	provides good performance and better embedding rate.
Pei-Yu Lin et al.[26]	2010	Spatial domain	invertible sharing approach is used i:e (t,n)-threshold sharing scheme.	provides no distortion in secrete image and lossless secrete image with better data embedding capacity.
Der-Chyuan Lou et al.[27]	2013	Spatial domain	steganography method based on RHTF(Reversible histogram transform function) used to maintain statistical features	provides improved security, helpful against statistical and regular singular(RS) attack specially under higher embedding rate
Wafaa Mustafa Abduallah et al.[28]	March 2014	Frequency domain	a transformed method based on irreducible polynomial mathematics, After dividing a colour image into blocks, then by applying the proposed transformed method to the specify block and hiding the secrete message in it	high embedding capacity, acceptable visual quality image with reasonable level of imperceptibility, Time complexity is reasonable and overall PSNR is improved.
Nameer N.El-Emam et al.[29]	2013	Adaptive	Hybrid Adaptive neural network with modified genetic algorithm. Here non uniform adaptive image segmentation is done with an intelligent technique	Hides the secrete message randomly instead of sequentially, 4 secrete bits per byte can be embedded with better visual quality

Z.Eslami et al[30]	2010	Spatial domain	secrete image sharing based on cellular automata with digital signature and hash function with double authentication mechanism	At most two bits of the pixel can be changed in the given cover image to maintains its visual quality. Integrity also achieved of the stego image without processing its blocks
Soumendu Chakraborty et al[31]	2013	Spatial domain	DSM, EM and SM are embedded in different cover images using X-Or operation between the bit plane of the matrixes and the respective cover image.	minimizes the computational complexity and minimum computational time.
Z.Eslami et al[32]	2011	Spatial domain	secrete bits are embedded in predetermined fixed size block of each cover image and the block size determined dynamically.	All the capacity of cover image is utilised, used for the authentication purpose.
Hai-Dong Yuan[33]	2014	Adaptive	two secrete sharing method which hides the secrete bits adaptively among texture region of cover by a spatial $^{+}_{-}$1 operation.	This provide protection from steganalysis technique, difficult to detect and we can embedded location sensitive secrete.
S.Geetha et al[34]	2011	Adaptive	renowned numerical model. Here the data which is to be embedded is dissected into numerals each having variable information carrying capacity.	This provides efficient visual quality despite of high payload capacity. It is also resistance to RS steganalysis and offer high visual quality in comparison to typical LSB based scheme.

V. CONCLUSION

We notice that spatial domain method is mostly used by more number of authors in comparison to frequency domain. Authors also given importance to the adaptive method. This description is shown in this figure for better understanding.



This paper is intended to give an idea about a number of major steganography algorithm and techniques based on digital images developed during the period of 2010-2014. There are different type of steganography method is available. Number of method is not confined. Here the importance is given to Image spatial domain, image frequency domain and to adaptive method. In this paper, effort has been made to discuss about applications and features of each different technique minutely. This paper is mostly confined with in the period of 2010-2014. Yet there is a lot of scope and opportunities to analyze and develop more an effective method for steganography.

REFERENCES

i Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevit, Digital image steganography: Survey and analysis of current methods, Elsevier Signal processing 90(2010) 727-752.

ii Elzbieta Zielinska, Wojciech Mazurczyk, Krzysztof Szczypiorski, Trends in Steganography, Communication of the ACM, Volume 57, No-3, (2014) 86-95.

iii Victor Onomaza Waziri, Audu Isah, Abraham ochoche, Shafi'i Muhammad Abulhamid, Steganography and its Application in Information Dessimilation on the web using image as Securety Embeddment: A wavelet Approach, IJCI volume1(2012) 194-202.

iv Guo-Shiang Lin, Yi-Ting Chang, Wen-Nung Lie, A Frame work of enhancing image quality with picture quality optimization and Anti-Steganalysis based on simulated anneling algorithm, IEEE Transaction on multimedia Vol-12 No.5(2010)345-357.

v Fangiun Huang, Jiwu Huang, Yun-Qing Shi, A new channel selection rule for JPEG steganography IEEE Transaction on information Forensics and Security vol-7 No.4(2012)1181-1191.

vi S.Premkumar, A.E. Narayana, New visual steganography scheme for secure banking application, International conference on computing, electronics and electrical Technologies[ICCEET]IEEE(2012)1013-1016.

vii Saeed Sarreshtedari, Mohammad Ali Akhaee, One third probability embedding: A new +-1 histogram compensating image least significant bit steganography scheme, IET image processing(2013)78-89.

viii Weiqi Luo, Yuangen Wang, Jiwu Huang, Security analysis on spatial +-1 Steganography for JPEG decompressed images, IEEE signal processing letters vol-18, No.1(2011)39-42.

ix Linjie Guo, Jiangqun Ni, Yun Qing Shi, Uniform embedding for efficient JPEG stegangraphy, IEEE Transaction on information Forensics and Security vol-9(2014),814-825.

x Wei-Jen Wang, Cheng-Ta Huang, Shiuh-Jeng Wang, Vq application in steganographic data hiding upon multimedia images, IEEE systems journal, vol-5, No.4(2011)528-537.

xi Chung-Min Yu, Kuo-Chen Wu, Chung-Ming Wang, A distortion free data hiding scheme for dynamic range images, ELSEVIER Displays 32(2011)225-236.

xii Qian Mao, A fast algorithm for matrix embedding steganography, ELSEVIER Digital signal processing 25(2014)248-254.

xiii Mingwei Tang, Jie Hu, Wen Song, A high capacity image steganography using multilayer embedding, ELSEVIER Optik 125(2014)3972-3976.

xiv Kan Wang, Zhe-Ming Lu, Yong-Jian Hu, A high capacity lossless data hiding scheme for JPEG images, ElSEVIER The journal of system and software 86(2013)1965-1975.

xv Kazem Qazanfari, Reza Safabakhsh, A new steganography method which preserves histogram: Generalization of LSB^{++}, ELSEVIER Information Science 277(2014) 90-101.

xvi Chia-Chun Wu, Shang-Juh Kao, Min-Shiang Hawang, A high quality image sharing with steganography and adaptive authentication scheme, ELSEVIER The journal of system and software 84(2011)2196-2207.

xvii Hamidreza Rashidy Kanan, Bahram Nazeri, A novel image steganography scheme with embedding capacity and tunable visual image quality based on genetic algorithm, ELSIVIER Expert system with application 41(2014)6123-6130.

xviii Anastasia Ioannidou, Spyros T.Halkidis, Geoorge Stephanides, A novel technique for image steganography based on a high payload method and edge detection, ELSIVIER Expert system with application 39(2012)11517-11524.

xix M. Ghebleh, A.Kanso, A robust chaotic algorithm for digital image steganography, ELSIVIER Commun nonlinear sci number simulate 19(2014)1898-1907.

xx S.M. Elshoura, D.B. Megherbi, A secure high capacity full gray scale level multi image information hiding and secrete image authentication scheme via Tchebichef moments, ELSIVIER Signal processing: Image communication 28(2013)531-552.

xxi Rengarajan Amirtharajan, Joohn Bosco Balaguru Rayappan, An intelligent chaotic embedding approach to enhance stego-image quality, ELSEVIER Information Science 193(2012) 115-124.

xxii Ratnakirti Roy, Anirban Sarkar, Suvamy Changder, Chaos based edge adaptive image stegangraphy, ELSIVIER Procedia technology 10(2013)138-246.

xxiii V.Nagaraj, Dr. V.Vijayalakshmi, Dr G.Zayaraz, Color image steganography based on pixel value modification method using modulus function, ELSIVIER IERI procedia 4(2013)17-24.

xxiv D.Biswas, S.Biswas, A. Majumder, D.Sarkar, D.Sinha, A.Choowdhury, S.K. Das, Digital image steganogyaphy using dithering technique, ELSIVIER Procedia Technology 4(2012)251-255.

xxvLi Fan, Tiegang Gao, Yanjun Cao, improving the embedding efficiency of weight matrix based steganography for grayscale images, ELSIVIER Computers and Electrical engineering 39(2013)873-881.

xxvi Pei-Yu Lin, Chi-Shiang Chan, Invertible secrete image sharing with steganography, ELSEVIER Pattern recognition letter 31(2010)1887-1893.

xxvii Der-Chyuan Lou, Chen-Hao Hu, LSB steganography method based on reversible histogram transformation function for resisting statistical steganalysis, ELSEVIER Information Science 188(2012) 346-358.

xxviii Wafaa Mustafa Abdullah, Abdul Monem S. Rahma, Al-Sakib Khan Pathan, Mix column transform based on irreducible polynomial mathematics for color image steganography: A new approach, ELSIVIER Computers and Electrical engineering 40(2014)1390-1404.

xxix Nameer N. El-Emam, Rasheed Abdul Shaheed AL-Zubidy, New Steganography algorithm to conceal a large amount of secrete message using hybrid adaptive neural networks with modified adaptive genetic algorithm, ELSEVIER The journal of system and software 86(2013)1465-1481.

xxxZ.Eslami, S.H. Razzaghi, J.Zarepour Ahmasabadi, Secrete image sharing based on cellular aotumata and steganography, ELSIVIER Pattern recognition 41(2010)397-404.

xxxi Soumendu Chakraborty, Anand Singh Jalal, Charul Bhatnagar, Secrete image sharing using grayscale payload decomposition and irreversible image, ELSEVIER Journal of information security and application 18(2013)180-192.

xxxii Z.Eslammi, J.Zarepour Ahmadabadi, Secrete image sharing with authentication-chaining and dynamic embedding, ELSIVIER The journal of system and software 84(2011)803-809.

xxxiii Hai-Dong Yuan, Secrete sharing with multi-cover adaptive steganography, ELSEVIER Information Science 214(2017)197-212.

xxxiv S.Geetha, V.Kabilan, S.P. Chockalingam, N.Kamaraj, Varying radix numeral system based adaptive image steganography, ELSIVIER Information processing Letters111(2011)792-797.