Volume 6, Issue 7, July 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review of Various Image Steganography and Steganalysis Techniques

Priyanka Sharma
M.Tech. Student, Dept. of CSE
JSS Academy of Technical Education (JSSATEN)
Noida, Uttar Pradesh, India

Pradeep Kumar
Asst. Professor, Dept. of CSE
JSS Academy of Technical Education (JSSATEN)
Noida, Uttar Pradesh, India

Abstract— Information is wealth of each association and in present period in that data transferred across digital mass media and internet, it came to be a top priority for each association to protect this wealth. Whatever method we accept for the protection patriotic, the degree and level of protection always stays top concern. Steganography is one such method in that attendance of hidden memo cannot be noticed and we can use it as an instrument for protection intention to send the confidential data in a safeguard way. It is an ongoing research span possessing large number of requests in different fields such as protection and intellect, health, on-line investment, on-line deal, to halt music piracy and supplementary commercial and business purposes. There are assorted steganography ways continue and they differ reliant on memo to be embedded, use of file kind as messenger or compression method utilized etc. The focus of this paper is to categorize different picture steganography methods as well providing overview, significance and trials of steganography techniques. Supplementary connected protection methods are additionally being debated in brief in this paper. The association of steganography methods could furnish not merely understanding and guidelines to researchers in this earth but additionally furnish orders for upcoming work in this earth.

Keywords— Confidential; information; Data Security;Steganography; Steganalysis

I. INTRODUCTION

Digital mass media is most favored basis for transfer of data and contact nowadays days. With the development and admission of internet to everyone, it came to be easier and probable to duplicate and to allocate the digital data illegally. Digitally transferred data can be duplicated lacking each defeat of content and quality as well, that is a large setback to the protection, authenticity and copyright to the proprietor of the data. To retain secrecy of data has come to be a vital subject and steganography proposal an extremely reliable resolution for such problems. Steganography is a fine art and science of embedding hidden memo into cover medium. In steganography, hidden memo is embedded in an appropriate messenger object that could be picture, video, sound or supplementary file to be sent above internet and embedding is parametrized by a key that makes tough to even notice the attendance of data and more to find a key to admission it. After cover object is embedded, it is recognized as stego object. Steganography had been in use from past times. steganography additionally usually recognized as 'Prison's Problem' because in preceding periods prisoners utilized it in prisons for contact purposes. Most frank method of steganography is to use the redundant data obtainable in digital medium. There is a rising attention in employing pictures as cover mass media for steganographic contact and detection of covert contact that use pictures has come to be a vital issue.

There are countless methods to embed data in a messenger and every single method uses its own mathematical approach. It is consequently tough to categorize the techniques. The subject has by now arisen preceding by R. it is large trial and question that- "Can the present and upcoming steganography algorithms be categorized into different classes of mathematical techniques?", as every single method uses a different approach.

In this paper, a power is made to categorize assorted picture steganography methods along with overview, significance and trials to steganography techniques. An endeavor additionally been made to categorize presently obtainable steganography methods into manipulated set of groups established on connected works survey and their qualitative analysis. The focus is extra on picture steganography as pictures are most accepted and extensively utilized medium above internet.

There are assorted supplementary data obscuring methods for disparate intentions and applications. These methods are recognized as 'information hiding' techniques. A little of these are namely steganography, cryptography; watermarking and fingerprinting are inter-linked to every single supplementary as well. Steganography additionally shouted 'Covered Writing 'conceals extremely attendance of hidden data in cover object whereas cryptography scrambles the data to stop the attacker from understanding the contents. Steganography additionally utilized whereas cryptography is whichever not allowed or not to be used. Steganography and cryptography are complementary and orthogonal to every single supplementary and both can be utilized in joined form furnish higher level of security. Watermarking is the procedure of embedding watermark gesture into multimedia data to produce watermarked object to protect authenticity of proprietor on that digital object and generally focuses on the robustness of embedded memo rather than capacity or concealment. As rising capacity and robustness at the alike period is not possible therefore watermarking can be utilized for copyright protection and pursuing legitimate use of a particular multimedia or media. In fingerprinting, on the supplementary hand, distinct marks are embedded in the duplicates of the object that are supplied to disparate clients such as hidden serial numbers that enables the intellectual property proprietor to recognize people who break their license accord and supply the property to third parties.

Steganography provides an ultimate promise of authentication that no supplementary protection instrument can ensure. The main aim of steganography methods is to maximize embedding rate and minimizing the detectability of the emerging stego pictures opposing steganalysis techniques.

To notice the hidden text in the stego object is shouted Steganalysis. It has two main kinds of analysis: Discernible Research and statistical Analysis. Discernible research deals alongside detection of hidden memo alongside naked eyes or alongside the aid of computer in that bit planes are analyzed separately for each infrequent change in the emergence for the attendance of hidden message. Statistical research deals alongside checking of each change in statistical properties of stego object provoked by steganographic algorithm. Steganalysis can be tear into two main types: Universal steganalysis and Specific kind of steganalysis techniques. Universal steganalysis methods can notice hidden memo in stego objects embedded by a scope of steganographic algorithms and specific steganalysis methods, that are extra urbane methods and work corresponding to a particular steganographic algorithm only. In order to design a good steganographic algorithm there is demand to comprehend steganalysis thoughts and methods as well.

REQUIREMENTS FOR A STEGANOGRPHY ALGORITHM

The main goals for each steganography algorithm are capacity, undetectibility and robustness. Even though it is tough for a steganography algorithm to have all the characteristics at the alike period because there is usually trade-off amid these characteristics.

- **Capacity:** The number of data to be embedded in cover medium and can retrieved afterward prosperously lacking considerably changing the cover medium.
- **Undetectibility:** There ought to be no discernible difference amid cover and stego object i.e. embedded memo ought to not be visible to human eye.
- **Robustness:** A stego arrangement is said to be robust if it can bear each attack and if it experiences makeover such as scaling, rotation, filtering and loss compression etc. it ought to stay intact.
- **Security:** An embedding algorithm is said to be safeguard if the embedded data might not be removed afterward detection by the attacker. It depends on the vision concerning the embedded algorithm and hidden key.

Steganography algorithms could differ from every single supplementary reliant upon: kind of cover object utilized, kind of area (spatial or change domain), kind of file format or compression utilized and kind of embedding method utilized to adjust the cover object etc. and can be categorized accordingly as shown in Fig. 1.

II. STEGANOGRAPHY BASED ON TYPE OF COVER OBJECT

Different types of cover objects like text, image, audio or video files can be used to hide secret data.

(1) Image Steganography: Picture steganography is most accepted form of steganography. Here hidden memo is embedded into a picture as sound, that is nearly impossible to notice by human eyes. Data obscuring in yet picture imposes precise trials to cope up alongside human discernible arrangements (HVS). Yet pictures more subject to assorted procedures like fluctuating from easy to nonlinear makeover such as cropping, blurring, filtering and loss compression etc. and data obscuring method ought to be resistant to these kinds of transformations. Pictures are extensively utilized medium above internets and this expects to produce unceasingly as computer graphics manipulation will grow. Pictures additionally have elevated degree of redundancy and furnish higher capacity and distortion tolerance. Countless plans are by now obtainable established on picture steganography to obscure text as steganography tools.

(2) Text Steganography: It is one of the first and most tough kinds of steganography. It is a method of employing composed usual speech to obscure a hidden message. Text steganography is most challenging due to the attendance of lesser redundancy in text documents as contrasted to the pictures and audio files.

(3) Audio Steganography: Audio steganography embeds the memo as sound into a cover audio file at a frequency out of human hearing range. Embedding hidden memos in digital sound is usually extra tough than embedding memos in supplementary mass media, Sensitivity to additive random sound is additionally acute. Usually utilized methods for audio Steganography are LSB coding, parity coding, period coding, range spectrum, and echo hiding.

(4) Video Steganography: It pertains to obscure data in video files, that are usually collection of sound and images. Steganography methods that are applicable to sound and pictures are additionally applicable to video files. Supremacy of this method is that colossal number of data can be hidden inside video alongside tinier number of distortion because of constant flow of data and that could go unobserved by observer.

(5) Protocol Steganography: It pertains to obscuring data in new or discretional fields of web manipulation protocols utilized in transmission above a network. In the layers of the OSI web ideal, there continue covert channels whereas steganography can be used. Data can additionally be hidden in the header of a TCP/IP packet in a little field that are whichever discretional or are not ever used. Supremacy of obscuring data in header is that human beings elucidate a little field scarcely and these fields assist as a flawless locale for obscuring data but there is disadvantage that after we configure firewalls for protection intention to filter out packet whereas kept fields encompass infrequent data next hidden data could additionally become lost. As picture steganography is generally utilized, hence basis for subsequent level of association is picture steganography merely as shown in Fig. 1.

STEGANOGRAPHY BASED ON DOMAIN TYPE

Based on area kind, spatial area and change area methods are usually utilized steganography techniques.

Spatial Area Techniques: Spatial area methods contain bitwise manipulation of intensity of pixels and sound manipulation. There are assorted ways to embed data in spatial domain. Most usually utilized and easy methods for spatial area are Least Momentous Bit (LSB) Methods.

LSB Method: It replaces least momentous bits of cover object alongside hidden message. It is most accepted and easy method after dealing alongside images. It has low computational intricacy and elevated embedding capacity [5]. Modulating the LSB does not consequence in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the emerging stego-image will gaze identical to the cover image. This permits elevated perceptual transparency of LSB. Even though it is extremely easy method but it is susceptible to loss compression and picture manipulation such as scaling, rotation, cropping etc., and in supplement, of sound or loss compression the stego-image will obliterate the memo as well. It works best after the picture file is larger than the memo file and if the picture is grayscale alongside sluggish adjustments in shades. LSB can be of fixed kind bit and variable bit.

Transform Area Techniques: Change area methods are additionally recognized as frequency area techniques. Change area methods early change picture from spatial area to frequency area and next hidden memo is embedded. These methods obscure data by employing mathematical functions. We frequently use these methods in compression algorithms and makeover involve obscuring hidden memo in change space of the cover object. In Frequency area schemes, the hidden data will be embedded into change coefficients that are transformed early into frequency area by assorted frequency area methods like Discrete Cosine Makeover (DCT), Discrete Wavelet Change (DWT), Discrete Fourier Change (DFT) etc. next hidden data will be embedded into change coefficients.

A change charts picture data into a disparate mathematical space via a makeover equation. Discrete makeovers are giving, that are established on specific purposes shouted the basic functions. The discrete edition of 1-D basis purpose is shouted basis vectors. The discrete edition of 2-D basis purpose is shouted basis pictures (or basis matrices). Difference amid the disparate kinds of change is the basis picture used. Every single kind of change has its own equation to produce the basis images. 2D Walsh-Hadamard change is the tensor of the 1D transform.

Table1. Comparisons Between Spatial Domain Techniques And Transform Domain Techniques

Criteria	**Spatial Domain Techniques**	**Transform Domain or Frequency Domain Techniques**
Embedding Process	In spatial domain steganography methods secret messages are embedded by manipulation of pixel values i.e. intensity of pixel values.	Transform domain techniques, first convert image from spatial domain to frequency domain and then message is embedded.
Robustness Against Attacks	Data embedding in the spatial domain is more robust to geometrical attacks, such as cropping and down sampling.	Data embedding in the frequency domain usually has more robustness to signal processing attacks, such as addition of noise, compression and low pass filtering [20].
Capacity	Data embedding in spatial domain category provides higher capacity.	Data embedding is lower as compare to transform domain [10].
Complexity	Spatial domain techniques are quite simpler.	These techniques are complex.
Examples	Commonly used techniques for spatial domain are LSB techniques.	Masking and filtering techniques are more commonly used with frequency domain techniques.

DCT: Most usually utilized makeover area method is DCT. It transforms a gesture or picture from the spatial area to the frequency domain. It can distinct the picture into elevated, middle and low frequency components. Embedding in DCT area is plainly did by changing the DCT coefficients. DCT makeover and compression employing quantization and run-length coding on raw pictures can be utilized to attain safeguard stego images. DCT is a loss compression change because its cosine benefits cannot be computed precisely, and recapped calculations employing manipulated precision numbers familiarize rounding errors in results. Variances amid early data benefits and refurbished data benefits depend on the method utilized to compute DCT.

DFT: The Fourier change is the well-known and extensively utilized transform. Fourier change decomposes a picture into a weighted sum of 2-D sinusoidal term. After all the needed basis pictures have been obtained, we can present the change operation. Later giving the change, we can become back the early picture by requesting the inverse Fourier change.

Comparisons between spatial domain and transform domain techniques can be based upon various criteria like robustness, payload capacity, complexity of technique etc. as shown in table1.

Wavelets: For image processing applications, we need wavelets that are two-dimensional. Wavelets are functions that "wave" above and below the x-axis, have

1. varying frequency,
2. limited duration, and
3. an average value of zero.

This is in difference to sinusoids, utilized by FT, that have infinite energy. Like sines and cosines in FT, wavelets are utilized as basic functions. The locale of the wavelet permits to explicitly representing the locale of events in time. The form of the wavelet permits representing disparate detail or resolution. Nowadays a dates, wavelet change is being increasingly utilized not merely in the earth of picture and gesture processing requests but additionally in countless supplementary disparate spans fluctuating from mathematics, physics, astronomy to statistics and economics.

(1) STEGANOGRAPHY BASED ON FILE FORMAT AND TYPE OF COMPRESSION USED

The Most usually utilized picture format on internet are Graphic Interchange Format (GIF), Combined Photographic Expert Cluster (JPEG), and to lesser extent– the Handy Web Graphics (PNG). Most of the steganography methods exploit these picture formats and a little of the methods are established on Bitmap format (BMP). To send and store colossal picture files in a reasonable number of period, picture compression is used. There are two kinds of compression methods for images: loss and lossless compression. Even though both methods save space but has disparate result on uncompressed hidden data.

GIF files and Steganography: In 8-bit GIF files, eachpixel embodied as a solitary byte and merely points to a color index table (a palette) alongside 256 probable colors. Therefore, pixel's worth lies in amid 0 and 255. Embedding in palette is completed normally alongside GIF formatted images. Palette picture consists of three parts-- a header, a palette and a picture data. The palette encompasses RGB triplets of all colors that transpire in image. Hidden memo can be embedded in palette or in picture data but palette-based pictures depart facilely noticed distortions.

BMP Pictures and Steganography: Bitmap pictures were giving by Microsoft as average picture file format amid users of windows working arrangement but it is utilized less frequently due to colossal size. Colossal size of bmp files is due to poor compression that makes this format functional for steganography. BMP files use a kind of compression shouted "run length encoding", that is lossless compression. This file format encompasses a little exceptional property, that can be utilized for steganography intentions like picture is stored in reverse order i.e. early blue byte, pursued by green and next red byte. Pixels are composed explicitly in the file, that permits facile identification and modification for steganography. Recognizing bit planes and how these are accessed is vital in understanding and employing steganography techniques. One public method is to use solitary plane to adjust rather than interjecting whole image.

JPEG Pictures and Steganography: Preceding it was trusted that steganography cannot be utilized alongside JPEG pictures due to loss compression and their compression algorithm does not prop a manage LSB embedding into spatial domain. Now a days steganographic arrangements for the JPEG format seem extra interesting because nowadays the arrangement work in a change space and is not altered by discernible attacks. JPEG picture uses DCT to accomplish compression. JPEG compression uses two periods:

(i) DCT and quantization, which form the part of loss stage
(ii) Huffman coding, which compresses lossless data.

Embedding data alongside JPEG picture can seize locale amid these two stages. By embedding the data at this period, in the change area, it becomes tremendously tough to notice, as it is not in the discernible domain.

While working alongside steganography, it is extremely vital to comprehend the compression and kind of compression utilized in cover object. Uncompressed formats (GIF & BMP) have larger file size than each supplementary format and have extra discernible redundancy hence can accommodate higher volume of hidden data and are extra convenient for data obscuring algorithms.

1) Embedding Methods

Some of usually utilized methods established on a little specific way to impact the cover object to obscure hidden data are believed here:

Spread Spectrum: This method is established on range spectrum contact that is spreading the bandwidth of an arrow group signal. In range spectrum steganography hidden memo is embedded in sound and next joined alongside cover picture to produce stego picture whereas manipulation of embedded gesture is far lower than cover picture and stego picture is not perceptible to HVS. Masking: This method masks hidden data above early data by changing the luminance of particular areas. It embeds the memo inside momentous bits of the cover image. Unlike LSB, masking is not susceptible to loss methods because picture manipulation does not alter the hidden memo because masking adds redundancy to the hidden information. This makes the masking method extra suitable than LSB alongside loss JPEG images. It could additionally aid to protect opposing a little picture processing procedures such as cropping and rotating.

Statistical: Here obscuring and removing the data are established on precise statistical properties of cover object. It uses attendance of "1-bit" steganography and modifies cover in such method that "1" is transferred by changing precise statistical properties of cover or else, cover stays unchanged.

Distortion: Here hidden memo is embedded by distortion of cover and computing deviation amid early cover and stages at decoding stage. Distortion methods are less safeguard and are not utilized in assorted requests because early cover object could obtainable to steganalyst for comparison. Text established steganography methods usually use distortion kind for embedding.

III. FACTORS AFFECTING SECURITY LEVEL OF A STEGANOGRAPHY ALGORITHM

As each works there are assorted factors altering the level of protection of a steganography algorithm. Choice of cover object and length of embedded hidden memo is vital factors that could alter the protection of embedding algorithm as lesser the embedded data lesser will be the detectable artifacts gave by embedding process. Gray scale pictures are usually the best cover objects for embedding hidden data. Uncompressed scan pictures as obtained from digital cameras encompassing colossal no of colors are additionally favored for steganography. Choice of compression method additionally plays a momentous role. JPEG pictures employing change area aftermath in extra safeguard embedding and these additionally cannot noticed visually. Computerized pictures or pictures alongside exceptional semantics such as fonts ought to be evaded in steganography. More difference, brightness, attendance of sound and assorted supplementary factors are additionally demanded to ponder making contact safeguard employing steganography etc.

Challenges and Issues with Steganography

After studying and analyzing obtainable works and continuing methods, it was noted that steganography algorithms are confronting assorted trials and subjects that demand more discovering and investigations. A little of the prominent subjects and spans are as follows -

- Data obscuring in yet picture poses assorted trials as these furnish less redundancy and imperceptibility as contrasted to audio and video files.
- It is additionally a trial to embed memo into cluster pictures, that are exceedingly inter correlated and frequently manipulated in compressed form.
- Steganography algorithms usually fight for bestowing elevated data rate and imperceptibility. If a method provides elevated payload capacity next it could come to be less robust and vice versa. Necessities for higher capacity and safeguard contact are frequently contradictory. Reliant on the specific request this transaction off needs to pursue out and at the alike period there is additionally demand to produce elevated quality stego algorithm by accomplished elevated worth of PSNR (Peak Gesture to Sound Ratio).
- Steganographic methods are extremely sensitive to assorted modifications in cover medium like Picture processing procedures (smoothing, filtering, picture makeovers etc.) compression methods, removing and filtering digital sound methods because these methods lead to removal or modifications of hidden embedded data too. There is additionally demand to design steganographic algorithms capable of bearing picture processing operations.
- Hidden memo have to be safeguard both from perceptual and statistical attacks. There is necessity to design extra robust steganography algorithms and there is demand to wage distinct attention for the attendance of alert and malicious attacks.
- Steganography has assorted functional requests but like supplementary technologies, convicts and terrorists can additionally misuse it for ill purposes. There is demand to comprehend all steganography as well as steganalysis are thoughts, habits and its requests for communal intentions rather next ill intentions.

IV. RELATED WORK

M. Manisha et al, in "Devanagari text embedding in a gray image: An offbeat approach" 2015 [1], the authors describe Steganography is a tool which helps in hiding information that plays a crucial role in many ways and in many lives. With the advent of the Internet, information exchange is possible in many languages other than English. This technology eventually carries with it a disadvantage which is the loss of security and privacy of information. Steganography an insipid medium, is one such way to ensure privacy. Steganography plays a vital role in securing the secret data. In this paper, a different approach is chosen for encoding Devanagari (Hindi) Text in the cover image. This approach of hiding Devanagari (Hindi) and English Text in an alternate manner is very efficient and simple to use. This paper describes a duplet algorithm, one for encoding and another for decoding. The image parameters are calculated by this proposed methodology, which proves that this process is more efficient and innovative.

Drago et al, in "A study of industrial strength of TSM watermarks" 2013 [2], the authors describe The purpose of this paper is to provide a method of verification for digital watermarks, based on removing the watermark with the help of another low quality audio track, lacking the watermark. They present results of a study on modern steganography systems implemented in industry. The attack is based on the fact that they have little prior knowledge about the algorithm used on a certain steganography scheme, with emphasis on the time scale modification method. The cross-correlation method represents the foundation of specific detection of the function used to dilate and contract the time space between two local extreme values.

Titian Bianchi et al, in "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts" 2012 [3], the authors describe in this paper, they propose a forensic algorithm to discriminate between original and forged regions in JPEG images, under the hypothesis that the tampered image presents a double JPEG compression, either aligned (A-DJPG) or nonaligned (NA-DJPG). Unlike previous approaches, the proposed algorithm does not need to manually select a suspect region in order to test the presence or the absence of double compression artifacts. Based on an improved and unified statistical model characterizing the artifacts that appear in the presence of both A-DJPG or NA-DJPG, the proposed algorithm automatically computes a likelihood map indicating the probability for each 8x8 discrete cosine transform block of being doubly compressed. The validity of the proposed approach has been assessed by evaluating the performance of a detector based on thresholding the likelihood map, considering different forensic scenarios. The effectiveness of the proposed method is also confirmed by tests carried on realistic tampered images. An interesting property of the proposed Bayesian approach is that it can be easily extended to work with traces left by other kinds of processing.

Thomas Monoth et al, in "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns" 2010 [4], the authors describe Visual cryptography is a kind of secret image sharing scheme that uses the human visual system to perform the decryption computations. A visual cryptography scheme allows confidential messages to be encrypted into k-out-of-n secret sharing schemes. Whenever the number of participants from the group (n) is larger than or equal to the predetermined threshold value (k), the confidential message can be obtained by these participants. Contrast is one of the most important parameters in visual cryptography schemes. Usually, the reconstructed secret image will be darker (through contrast degradation) than the original secret image. The proposed scheme achieves better contrast and reduces the noise in the reconstructed secret image without any computational complexity. In this method, additional pixel patterns are used to improve the contrast of the reconstructed secret image. By using additional pixel patterns for the white pixels, the contrast of the reconstructed secret image can be improved than in the case of existing visual cryptography schemes.

Fausto Galvan et al, in "First Quantization Matrix Estimation From Double Compressed JPEG Images" 2014 [5], the authors describe One of the most common problems in the image forensics field is the reconstruction of the history of an image or a video. The data related to the characteristics of the camera that carried out the shooting, together with the reconstruction of the (possible) further processing, allow them to have some useful hints about the originality of the visual document under analysis. For example, if an image has been subjected to more than one JPEG compression, they can state that the considered image is not the exact bitstream generated by the camera at the time of shooting. It is then useful to estimate the quantization steps of the first compression, which, in case of JPEG images edited and then saved again in the same format, are no more available in the embedded metadata. In this paper, they present a novel algorithm to achieve this goal in case of double JPEG compressed images. The proposed approach copes with the case when the second quantization step is lower than the first one, exploiting the effects of successive quantizations followed by dequantizations. To improve the results of the estimation, a proper filtering strategy together with a function devoted to find the first quantization step, have been designed. Experimental results and comparisons with the state-of-the-art methods, confirm the effectiveness of the proposed approach.

Amarjeet Kaur et al, in "Digital steganography in neural networks models" 2014 [6], the authors describe Digital Steganography is the act of hiding a message related to digital signal (i.e an image, song, and video) within the signal itself. Steganography tries to hide a message related to the actual content of the digital image. This paper present two digital steganography techniques for embedding a text watermark image into gray scale image. This proposed method uses FCNN and Hopfield Model for embed the watermark to achieve almost zero visible distortion in the watermarked image. Therefore watermarked image is almost same as the original cover image and extracted watermark at the output is same as the watermark at the input. Performance of these two models is compared on the basis of nop, Elapsed time, PSNR before adding a watermark, PSNR for extracted watermark image, Attack recover time, Ncor.

Hsien-Wen Tseng et al, in "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion" 2014 [7], the authors describe Data hiding is a technique that is embedding the secret message into the media. In 2010, Chen et al.'s proposed a scheme combined the `Canny' edge detector and fuzzy edge detector to increase edge pixels, and embedded more secret data into the edge pixels than the non-edge pixels based on the least-significant-bit (LSB) substitution scheme. In this study, the authors use Kaur et al.'s fuzzy logic-based algorithm and extend the original design to block-based design. The experimental results show that the proposed method achieves higher payload with Kaur et al.'s fuzzy logic-based algorithm, and achieve minimal distortion by selecting the number of edge pixel's embedding length of each block which has minimum mean-squared error.

Sangeeta Gupta et al, in "Invisible steganography using a novel MRA-based image fusion method" 2012 [8], the authors describe In today's technical era, transmission of digital data plays a key role in their everyday lives; it is only natural that the protection of data integrity and confidentiality has assumed paramount proportions. To avoid interception and misuse, an efficient and reliable data hiding technique has to be developed and deployed in almost every sphere of electronic data management. For this purpose, the concept of steganography has always been used widely. In this paper they have presented a novel technique based on wavelet transforms and image fusion and proposed a new algorithm for robust and effective steganography. In this algorithm, they have used the Multi-Resolution Analysis (MRA) technique to decompose an image and then fusing it with a logo image rather than a pseudo-random number sequence. The algorithm has been applied on multiple images and results have proved its effectiveness.

Zhenhua Qu et al, in "Forensic sensor pattern noise extraction from large image data set" 2013 [9], the authors describe The sensor pattern noise (SPN) can be regarded as the unique identity of a digital camera which is highly useful in digital image forensics. Existing methods which works by denoising each individual natural image often took an investigator a long time and great efforts to collect sufficient photos of diversified enough natural scenes. These processes are hard to repeat or standardized for officially using by an authority. In this work, they create noise image data set by taking photos of random noises displayed on a high definition monitor and propose a homomorphic based SPN extraction method. It offers the forensic researcher a fast way to create a large image data set in a few minutes. And the extraction method only needs to denoise once, which is highly efficient to deal with large numbers of photos. They compared the source camera identification performance of the proposed SPN extraction method to a prior state-of-art with identical experimental settings. The experimental results confirm the effectiveness of the proposed method.

Rupendra Kumar Pathak et al, in "LSB based image steganography using PN sequence & GCD transform" 2015 [10], the authors describe This paper has been proposed for the image steganography. It is based on a modification of LSB (least significant bit) of pixels and this modification is the replacement of LSB bits of the cover image (CI) pixels that carries the most significant bits (MSB) of data image (DI). This makes the algorithm modest. In steganography of image, security is also a major concern. Here, key based PN (Pseudo Number) sequence is generated. It is used to provide security to algorithm against the stegano-analytic attack. The algorithm also has been improved to detect and locate tampering done by malicious attackers. This is obtained by conversion of image into a fixed point image using GCD (Gaussian convolution and de-convolution) transform.

Boulat A. Bash et al, in "Square root law for communication with low probability of detection on AWGN channels" 2012 [11], the authors describe We present a square root limit on low probability of detection (LPD) communication over additive white Gaussian noise (AWGN) channels. Specifically, if a warden has an AWGN channel to the transmitter with non-zero noise power, they prove that o(. Further, they show that LPD communication on the AWGN channel allows one to send a nonzero symbol on every channel use, in contrast to what might be expected from the square root law found recently in image-based steganography.

V. CONCLUSION AND FUTURE WORK

With the progress, development, ease and admission of internet to everyone and use of digital mass media for transfer of data, there is demand to converse hidden and confidential data above the internet securely. Steganography provides a reliable resolution by obscuring the extremely attendance of memo and hence utilized as a protection tool. The technical trial of data obscuring is discovering redundant bits in messenger gesture that cannot be statistical and perceptually attacked. Uncompressed file formats (BMP, GIFF, TIFF) established on lossless compression provides elevated data capacity and are extra convenient for data obscuring algorithms. There are assorted steganography ways reliant on kind of cover object utilized, kind of area, kind of file format or compression utilized and kind of embedding method utilized to adjust the cover object etc. There is additionally demand to choose characteristics to compromise in order to safeguard elevated performance. Steganography has requests in assorted fields such as confidential transmission, video surveillance; martial and health requests, group captioning, integration of several mass media for convenient and reliable storage, association, transmission, embedding executables for purpose domination, error correction, and edition enhancing etc.

In preceding work, researchers emphasized on specific steganography methods and merely slight research work has been completed in association direction. Steganography is an ongoing research span and lacking association or categorization, it becomes tough for new researchers to pursue an association and enhance their research. Across this paper, a power has been made to categorize the assorted steganography methods established on obtainable works and qualitative aspects of techniques. The frank thoughts and association given in this paper could furnish the researchers alongside an association to pursue so that advancements can be made in the earth of steganography.

Like each supplementary science this can additionally be utilized for ill intentions by convict and terrorists, it is consequently vital to comprehend steganography and steganalysis concepts. Researchers demand to wage distinct attention in the direction of this challenging but priceless span.

REFERENCES

[1] M. Manisha, S. S. Malvika, B. Karthikeyan, V. Vaithiyanathan, B. Srinivasan, "Devanagari text embedding in a gray image: An offbeat approach", School of Computing, SASTRA University, Thanjavur, India, 10.1109/ECS.2015.7124791, 1284-1288, 2015

[2] Drago&#x015F, Dr&#x0103, ghicescu, "A study of industrial strength of TSM watermarks", University POLITEHNICA of Bucharest, Faculty of Electronics, Telecommunications and Information Technology, Bucharest, Romania, 10.1109/IWSSIP.2013.6623478, 159-162, 2013

[3] Tiziano Bianchi, Alessandro Piva, "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts", Department of Electronics and Telecommunications, University of Florence,, 10.1109/TIFS.2012.2187516, 1003-1017, 2012

[4] Thomas Monoth, Babu Anto P., "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns", Dept. of Comput. Sci., Mary Matha Arts & Sci. Coll., Mananthavady, India, 10.1109/CW.2010.39, 171-178, 2010

[5] Fausto Galvan, Giovanni Puglisi, Arcangelo Ranieri Bruna, Sebastiano Battiato, "First Quantization Matrix Estimation From Double Compressed JPEG Images", , University of Udine, Udine, Italy, 10.1109/TIFS.2014.2330312, 1299-1310, 2014

[6] Amarjeet Kaur, Arti Goel, Hitender Gupta, "Digital watermarking in neural networks models", Department of Electronics & Communication Engineering, Swami Devi Dyal Institute of Engineering & Technology, Barwala, India, 10.1109/RAECS.2014.6799538, 1-6, 2014

[7] Hsien-Wen Tseng, Hui-Shih Leng, "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion", Dept. of Inf. Manage., Chaoyang Univ. of Technol., Taichung, Taiwan, 10.1049/iet-ipr.2013.0584, 647-654, 2014

[8] Sangeeta Gupta, Sujoy Bhattacharya, "Invisible watermarking using a novel MRA-based image fusion method", Padmasri Dr B V Raju Inst of Technology, Narsapur, Hyderabad, India, 10.1109/INDCON.2012.6420682, 567-571, 2012

[9] Zhenhua Qu, Xiangui Kang, Jiwu Huang, Yinxiang Li, "Forensic sensor pattern noise extraction from large image data set", School of Information Science and Technology, Sun Yat-Sen Univ. Guangzhou 510006, China, 10.1109/ICASSP.2013.6638213, 3023-3027, 2013

[10] Rupendra Kumar Pathak, Shweta Meena, "LSB based image steganography using PN sequence & GCD transform", Dept. of Electronics & Communication Engineering, NIT, Kurukshetra, India, 10.1109/ICCIC.2015.7435692, 1-5, 2015

[11] Boulat A. Bash, Dennis Goeckel, Don Towsley, "Square root law for communication with low probability of detection on AWGN channels", Department of Computer Science, University of Massachusetts, Amherst, Massachusetts 01003-9264, 10.1109/ISIT.2012.6284228, 448-452, 2012