Analytic Survey on Various Techniques of Image Steganography

Gajendra Singh Rajput
Research Scholar
VITM Gwalior

Shilky Shrivastava
Asst. Professor
VITM Gwalior

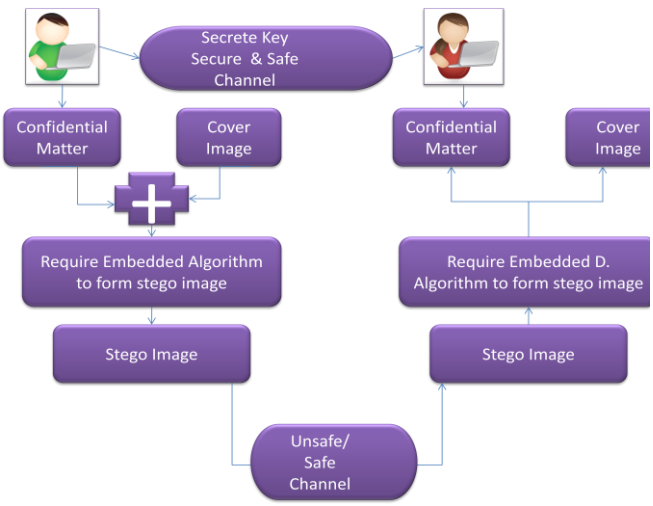
Anand Singh Bisen
Asst. Professor
VITM Gwalior

ABSTRACT
In this paper we have analytic survey on various techniques of image steganography, these technique are paying their role more efficiently to establish secure communication in more effective way, these idea work on various pattern, text and images also and help to hide confidential matter or information sharing in a newly created steganography techniques. Some latest invented steganography ideas on image with their advantages and disadvantages are disclosing though this analytic survey. It is basically a growing technique of confidentiality in various aspects of safe and confidential communication.

Keywords
Image stagnography;PSNR;SSIM;OBIS;DCT;DWT;

1. INTRODUCTION
Graphical media such as image, sound, video, text and pattern could play their role in stenography that may also define as secret or confidential graphics because steganos represent "secret" and the graphic represent writing way in secret form. Mainly steganography are combinational form of cover message, secret message, and the embedded algorithm. Cover message cover the secret or confidential information with embedded or attached algorithm.

Mainly following number of method are in use to cover the confidential information to establish secure communication Domain spatiality – Domain transmission – way of distortion and masking with filtration. The entire system of image steganography is shown in Block diagram - GRW1.1



Block Diagram: GRW 1.1: entire system of image steganography.

The entire system of image steganography has three basic component cover image, plan text (confidential matter (message)), secrete key which work with embedded algorithm that work on cover image and confidential matter form stego image by addition of cover image and confidential message and then to retrieve secure message back from stego image the key which travel by secure channel and embedded function or algorithm work simultaneously as it is well cleared form above block diagram GRW 1.1.

This function or embedded algorithm used in image steganography to hide secret information or data in cover image with minimum visual produced artifacts. Visual Fidelity is an important parameter of the stego image which is considered by all image steganography ideas. The stego image quality could be measured by compression of its similarity with the cover image. Peak Signal to Noise Ratio and Structural Similarity Index Measure are well-known techniques ascertain the quality of the stego image.

1.1 Integrity of the Specifications
The effectiveness of steganography could be measure by three parameters.

1. Steganography technique must provide the large amount of information.
2. Embedded data must not be perceptible to the viewer.
3. Hidden information should be successfully retrieved exactly at the receiver side.

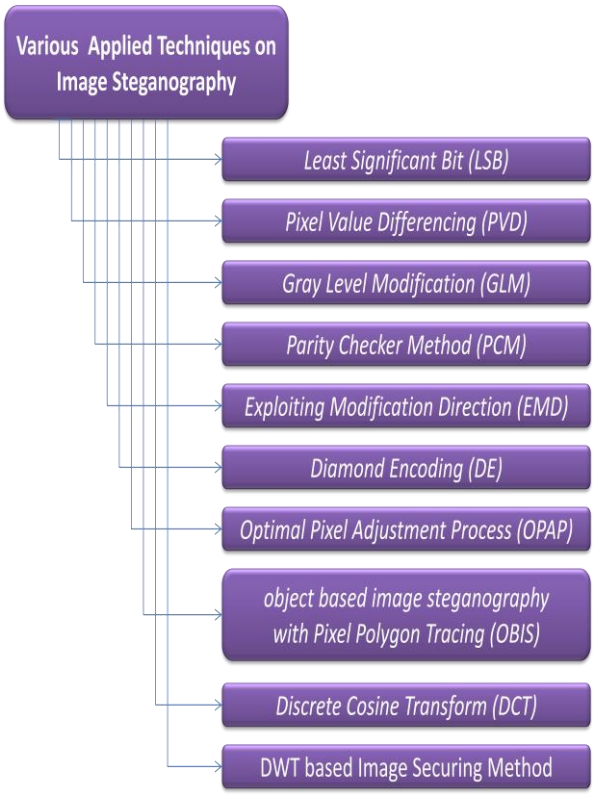
2. LITERATURE HIGHLIGHTS
PSNR: Peak signal to noise ratio is a parameter that calculate the digital quality of an image. Higher value of PSNR Shows the higher quality, it mean there is a least variation in stego image from cover image. Smaller value of PNSR shows there are less similerty between stego image and cover image. This could be mathematically denoted as

$$PSNR=10\log_{10}(255_2/MSE)$$

The average Mean Square Error(MSE) value obtained for stego image is around 5-10.

SSIM (Structural Similarity Index Matrix): a method which is use to improve the conventional parameter such as PSNR and MSE to determine the similarity of between cover image and stego image. The weight factor which decides the details of embedded image is called by steganographic weight. This weight is the frequency components that are assigned to a plane the cover image plane. The optimum value of weight obtained as it gives the best output when it extracted back. This weight decide the embedding rate and SSIM value in the steganographic work.

This literature review highlights the various techniques that are being used or newly proposed [6][7][8]. The techniques or methods those are playing their effective role in image steganography are shown bellow by block diagram Fig – GRW 2.1.



Block Diagram – GRW 2.1: The techniques or methods those are playing their effective role in image steganography

2.1 Least Significant Bit (LSB)

This was the first proposed technique in which least significant bit had modified to embed the secure information inside the image as carrier. In this least significant bit replacement by secret bit stream is done. This LSB is added or subtracted abruptly from pixel value of cover image when embedding bit doesn't match. Revised LSB match were also proposed with lowering the some modification.

2.2 Pixel Value Differencing (PVD)

In this technique the carrier image is segmented in to number of block that block does not overlapped one on another. In this confidential information is covered by using pixel difference in various pair of generated blocks. This difference value for information hiding was difficult to make in use.

2.3 Gray Level Modifications (GLM)

In this method image representation were in gray level or intensity level of each pixel. This gray level used to embed secure message [10]. Gray level and intensity value of pixel is taken first then values of bits of secure information hide by this match.

2.4 Parity Checker Method (PCM)

In this scheme even and odd parity is used to recognize pixel had parity to be odd then zero value is placed at place of pixel similarly recognition had done by pixel to be even parity, the one replaced at that pixel location.

2.5 Exploiting Modification Direction (EMD)

This technique did the modification at only one pixel, this scheme uses pixels pair to concealing confidential information inside the image that are being uses as cover image. This scheme has got improved the payload capacity and had limitation with number of notation systems to hide information or message.

2.6 Diamond Encoding (DE)

Data storing or pay load capacity is improved then exploitation modification direction. This scheme had provided robustness to communication system to transmit over secure or unsecure medium. This whole strategy works on pixel pairing.

2.7 Optimal Pixel Adjustment Process (OPAP)

This proposed scheme gives proper appearance of image, in this approach adjustment of the pixel value for information hiding were in existence. That technique is most similar LSB Substitution scheme. Cover image appearance before hiding information in it was very similar after hiding or safe information in it.

Object based image steganography (OBIS) by pixel polygon tracing:

Object based image steganography technique uses pixel polygonal area tracing in cover image which select suitable pixels for embedding confidential information [2]. The polygon is formed by convex hull for specificslly selected image pixels and distortion function is hybrid between high efficiency dembedding scheme and LSB matching. This technique is simple with effective impact. Experimental results of this work exhibits high fidelity of stego-image and performs decently to well-known spatial domain steganalysis techniques to moderate payload capacity, shown below in fig GRW 2.2.

Figure: GRW2.2: Cover Image with Payload

Fidelity metrics performance

GRW table 2.1

Cover image	Payload size	PSNR (in dB)	SSIM
Baboon	16 × 16	83.07	0.997
	32 × 32	80.06	0.994
	64 × 64	78.67	0.979
Landscape	16 × 16	81.12	0.985
	32 × 32	80.01	0.982
	64 × 64	78.14	0.977

This method uses convex hull to generate region of interest polygon to tracing out the suitable area for embedding confidential or secrete data. The edges of polygon are chosen

to hide information. The distortion function of the proposed technique uses hybrid data hiding scheme combining highly embedding efficient scheme with LSB matching features. Experiments with various numbers of cover images and moderate variant payload sizes which shows result for the visual quality of stego image in form of Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM).

2.8 Discrete Cosine Transform (DCT)

Data hiding could effectively perform at frequency domain slot3. Steganography approach for securing image by using DCT [Discrete Cosine Transform] is widely used Technique. DCT [4] allows image to be split into three frequency bands named as Low-frequency band (LFB), High-frequency band (HFB) and Mid-frequency band (MFB). In this effort, the secret data or confidential information is embedded into the DCT blocks that contain mid frequency (MF) sub band component whereas high frequency sub band components remain unused by using frequency domain steganography is safe, sound, and most flexible approach, and these are its updated benefits. It has different techniques for management.

2.9 DWT based image securing

In this scheme Discrete Wavelet transform is used to hide multicolor images into a single color image. The cover image split up into RED R, GREEN G and BLUE B Planes. Secret image is embedded in to these images. N-level decomposition of cover images and secret images are made and some frequency components of same are merged. Secret images are then extracted from stego image. Here, the obtained stego image which has less changes compared with original image with high security. Steganography uses DWT [1] has more advantages over DCT because it provides compression ratios and it also avoid interferences due to artifact. So comparatively DWT is better for hiding confidential data. The Discrete Wavelet Transform (DWT) can identify portions of cover image where secret information could be efficiently hidden. DWT splits the information into its high and low components of frequency [5]. The high frequency part of the signal store details about edge components, whereas the low frequency part contains most portion of the signal information of mage which is again split in two higher and lower frequency parts for every level of decomposition in two dimensional application, first DWT is performed in vertical direction that followed by horizontal direction.

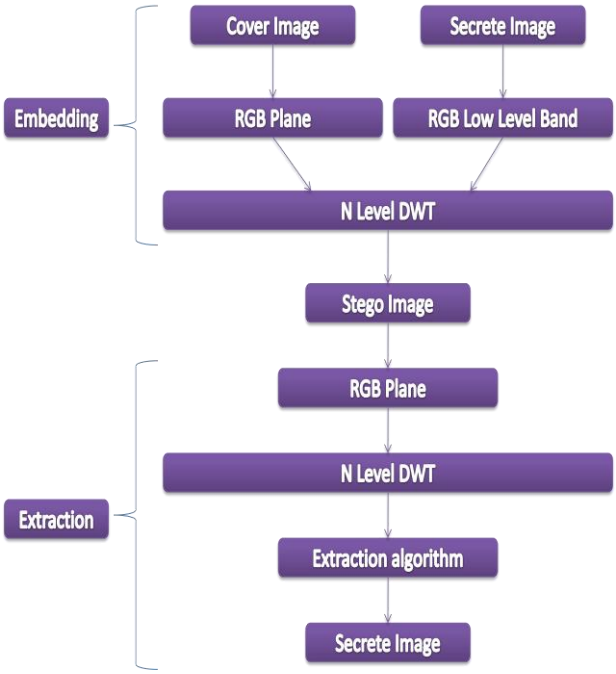


Figure:- GRW 2.3 DWT Image Steganography system

Table GRW T1:

S. No.	Various Technique	Advantages	Disadvantages
1.	Least Significant Bit	Simple, Substitution base only	Got cracked. , Low payload.
2.	Pixel Value Differencing	Great focus on image quality, Problem 100% in retrieving back.	Complexity higher
3.	Gray Level Modification	Less Complexity then PVD	Sometimes data lost probability exist
4.	Parity Checker Method	Parity even and odd mechanism is used.	Data storing capacity is low
5.	Exploiting Modification Direction	Highly secure to secret message transmission.	Data storing capacity is greater than PCM but maximum value is 1.61bpp only.
6.	Diamond Encoding	Degradation effect reduced.	Payload capacity Is high.
7.	Optimal Pixel Adjustment Process	Improved quality of image.	Little amount of distortion after data hiding.
8.	object based image steganography by Pixel Polygon Tracing	uses pixel polygonal area tracing , moderate payload capacity, promising	Polygonal area bound the region,

		results for visual quality of stego image	
9.	Discrete Cosine Transform	frequency domain steganography give safe, sound, and flexible approach	sub band components remain unused
10.	DWT based Image Securing Method	hide multicolor images into a single color image	stego image obtained has less perceptible changes compared with original image with high security.

A brief comparative survey to all proposed scheme yet is shown in above table GRW T1.

3 CONCLUSION AND FUTURE VISION

Secure Communication is always a popular human being need to fulfill that need several effective effort has been putted by several way, this is endless research topic because as technology growing, we always need a new security trick to secure entire communication system to save it from unauthorized accessing. This consecutive survey placed my target in steganography to achieve a new mile stone with new attractive algorithm by a most positive effort to remove all drawbacks of currently available algorithms with considering theirs benefits with this conclusive survey.

In future vision we have clear vision about new algorithm for image steganography with consideration of high quality image and artificial neural network or soft computing effort to hide confidential information in specifically trained learning system that could perform hiding by designed binary architecture for secrete information [9] to form stego image which would be most similar then taken cover image to hide confidential information.

4 REFERENCES

[1] Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela, "A Novel DWT based Image Securing Method using Steganography," International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 612 – 618

[2] Ratnakirti Roy and Suvamoy Changder, "Object Based Image Steganography with Pixel Polygon Tracing", Springer India 2015.

[3] S.G.Shelke, S.K.Jagtap, "Analysis of special domain Image steganography technique, 2015 International Conference on Computing Communication Control and Automation, 2015 978-1-4799-6892-3/15 $31.00 © 2015 IEEE.

[4] Blossom Kaur, AmandeepKaur, Jasdeep Singh, Steganographic Approach for Hiding Image in DCT Domain, International Journal of Advances in Engineering & Technology, July 2011.

[5] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 4, 3: 275-290. 2006

[6] R. Singh, G. Chawla, "A Review on Image Steganography,"Internationl Journal of Advanced Research inComputer Science and Software Engineering , vol. 4, pp. 686-689, May. 2014.

[7] Rakhi, S. Gawande, "A Review on Steganography Methods," Internationl Journal of Advanced Research in Electrical ,Electronics and Instrumentation Engineering , vol. 2, no. 6, pp. 4635-4638, Oct. 2013.

[8] C. Gayathri, V. Kalpana, "A Study on Image Steganography Techniques," Internationl Journal of Engineering and Technology(IJET) , vol. 5, no. 2, pp. 572-577, Apr-May. 2013.

[9] Jitendra Singh Sengar, Enhanced Artificial Neural Network Approach to indentify specific binary pattern International Journal of Hybrid Information Technology Vol.8, No.6 (2015), pp.391-396

[10] W. Hong and T.S. Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," IEEE Transactions on InformationForensics and Security, vol. 7, Feb. 2012

[11] Yadav, Rajkumar, Rishi, Rahul, Batra, Sudhir, "A new Steganography Method for Gray Level Images using Parity Checker," International Journal of Computer Applications, vol. 11, no. 11, Dec. 2010.