Vol. 2, No. 1 | January - June 2019

Investigation of LSB based Image Steganographic Techniques in Spatial Domain for Secure Communication

Shahid Rahman[1], Fahad Masood[1], Wajid Ullah Khan[1], Abdus Salam[1], Syed Irfan Ullah[1]

Abstract:

Confidentiality, integrity and authenticity for secure data are required for all the conveying bodies. Distinctive methodologies are utilized to adopt the security issues like digital certificate, digital signature and cryptography. These techniques alone cannot be traded off. Steganography is one of the answers to the security as it hides the secret information. Steganography has the importance in view of its exponential advancement and riddle data of possible PC customers over the web. It can likewise be depicted as the examination of indistinct information that usually manages the methodologies for concealing the closeness of the passed-on message. Mostly part of data covering is refined in correspondence to image, content, voice or sight and sound substance for copyright, military correspondence, confirmation and various diverse purposes. In this paper Least Significant Bit (LSB) technique for image steganography has been observed under various cases. Results for different scenarios have been looked at and the condition of the science assessment and examination of various accessible strategies for steganography have been given. The principles pursued are equivalent to give into the writing. Normal models and procedures drawn from the literature are utilized to obtain the results. This survey concludes with recommendations and supporters for the caries-oriented mechanism.

Keywords: *Steganography, Data concealing, Cover writing*

1. Introduction

Steganography is derived from two Greek words, "Steganos" means' 'covered/protected" and "graphic" representing "writing". So Steganography infers covered writing. It is one of a kind branches of "information stowing away or hiding". It is characterized as "The way towards composing secret message with the end goal that the nearness of the message is just known to the sender and receiver"[1]. It is the workmanship and study of undetectable communication and a push to cover the presence of the embedding data. Cover steganography is the art of conveying information that can't be distinguished or detected [2]. Steganography not only changes the course of action of the mysterious message, but also covers it inside a cover-dissent or question. Resulting to conceal strategy cover test and stego-Image (passing on secured data contradict) is indistinguishable. In this manner, steganography (concealing data) and cryptography (anchoring data) are absolutely astonishing from one another. By virtue of subtlety or shrouded factors it is hard to recuperate the data without knowing the framework in steganography. Systems for steganography insinuated as Steganalysis are the same as cryptanalysis [3].

A. Digital medium for steganography

There are five types of Steganography techniques used for embedding secret messages depending upon a cover protest or object.

[1] Department of Computing Abasyn University Peshawar KPK, Pakistan
Corresponding Author: rahmanshahid@gmail.com

i) ***Image Steganography***: A steganography type, in which image is used as a cover object. In this framework, pixel energy of the cover image is utilized to cover information. Images are thought to be the best cover objects for disguising information since it contains a generous measure of respective bits [4].

ii) ***Network Steganography:*** In network Steganography, network protocols are used as cover object such as TCP, IP, UDP and ICMP and so on. Data is covered up in a few fields of the header of TCP/IP packet that are open or never utilized [5].

iii) ***Audio Steganography:*** In this type audio is utilized as a cover object for data embedding. It has turned out to be an extremely critical medium because of voice over IP (VOIP) factor. It uses some digital plans like as Waveform Audio file format (WAVE), Audio Video Interleave (AVI), Moving Picture Experts Group (MPED), Musical Instrument Digital Interface (MIDI) etc. [6].

iv) ***Video Steganography:*** In video Steganography, collection of an image (video) is utilized as a cover object for concealing data. This strategy is able to shroud any type of records or data into computerized video design. Discrete cosine transforms usually modify values 8.667 - 9. Shrouded information for every image in video is utilized which is not recognizable by the HVS. The formats utilized by video steganography are Mp4, MPEG, H.264, and AVI and so on [7, 8].

vi) ***Text Steganography*:** In text Steganography text is utilized as a cover object. In this strategy mystery message is covered up in the nth letter of each cover text. Text steganography is thought to be the most difficult type of steganography because of the absence of excess in text when contrasted with different kinds of steganography. However, it requires less memory and is used for straightforward information [8]. Fig.1 shows the digital mediums for steganography.

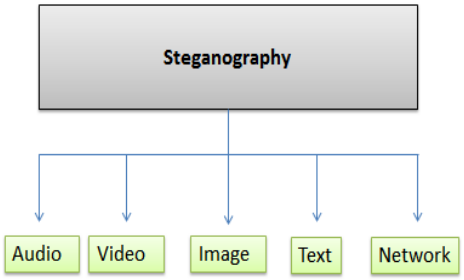

Fig.1. Digital Medium of Steganography

B. Structure of Steganography

Steganography has three main parts.

i) ***The Cover or Carrier:*** It can be an image or painting, a digital image (tiff, jpg, bmp, png), an mp3 (audio files), a text file, a video file or TCP/IP packet as well. It is the object that will carry the hidden message.

ii) ***The Message:*** It can be a simple text or content, a secret image, an audio or video which will be transmitted securely.

iii) ***The Key:*** It can be a password, pattern, a black-light or a pseudo random number known to both sender and receiver. It is used at the time of embedding and extraction of secret information. It provides more protection against third parties/hackers.

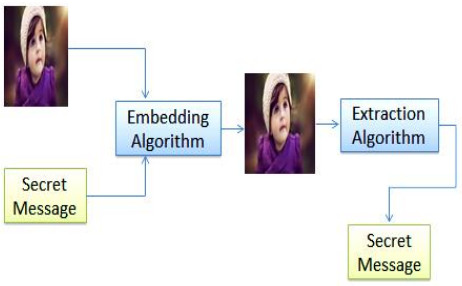

Fig.2. Image Steganography [1]

Fig.2 shows a fundamental plan of image steganography. Secret image is hidden within the image in such a manner that the intended

user is prevented to detect the hidden message. Stego-image is formed through an embedding algorithm. The stego- images when formed have a mirror distortion of the image which is negligible for the naked eye. The hidden message can be an extracted algorithm from the stego-object.

C. Categorizations of image steganography

Image steganography is classified in different types on the basis of measuring algorithm which is shown in table-1[10].

i) ***Perceptual Transparency*****:** Once procedure is concealed into a carrier object, detectable quality will be debased into embedded image as equate with the original-object.

ii) ***High Payload or Capacity:*** In cover object extreme mass of information can be inserted.

iii) ***Robustness*****:** Information should remain in place after covering, if embedded -image is changed, For example, editing, filtering, scaling and expansion of clamor (noise).

iv) Temper protection**:** It is a problematic issue to change the secret message after it has been secured into embedded object.

v) ***Calculation Complexity:*** How much costly it is computationally to embed and extract a covered message?

Table I: MEASURING ALGORITHM

Measures	Advantages	Disadvantages
Perceptual Transparency(HVS)	High	Low
High Capacity (Pay Load)	High	Low
Calculation Complexity	Low	High
Robustness (Security)	High	Low
Temper protection	High	Low

Table 1 shows the measuring algorithms for steganography, which is the basic criteria of steganography which will be analyzed through different existing methods in spatial domain based on these measuring algorithms which is shown in Table V.

D. Techniques of Image steganography

Image or image steganography plans can be confined into following area:

i) ***Methods of Spatial Domain:*** In spatial steganography distinctive executions are available. LSB based steganography is one of the smallest complex techniques that covers an inside secret message in the LSB's of pixel without showing different distinguishable damages or twisting. Changes in the estimation of the LSB are refined or impalpable for HVS. Some standard approaches in spatial domains are given below:

- EBE (Edges based embedding method)
- LSB (Least significant bit)
- RPE (Random pixel embedding method)
- Gray level modification and Multi level Encryption (MLE)
- Hidden data pixel mapping method
- Connectivity method or labelling
- Cyclic steganography randomization methods
- Pixel value differencing (PVD)
- Method of Pixel intensity
- Method of content or texture
- Shifting methods of Histogram

There are some common focal points and weakness of a spatial area based on LSB methods:

Focal points:

- Lesser shot for debasement of the cover object.
- In the image extreme size of data or information can be embedded.

Weaknesses:

- Less energy, with manipulation of image concealed information can be lost.
- Concealed data can be effectively crushed by open assaults if there is no robustness.

ii) ***Transform domain:*** In this technique we initially change the image from spatial space in recurrence area, conceal the mystery message and change it to the spatial domain. To conceal data utilizing these systems,

distinctive calculations and changes are connected with images which increment its many-sided quality. This strategy is thought to be considerably more grounded than spatial domain procedures. This method shroud data in those territories of the image that are less powerless by image pressure, trimming, and cropping. This system less inclined to measurable assaults and image corruption is additionally kept at least as we change co-proficient in the change space, they have also brought down the payload and not are against editing, turn, interpretation and commotion [11]. Some Transform domain methods are:
Coefficient bits embedding

- Reversible method or lossless
- Discrete Fourier Transform (DFT)
- Discrete Wavelet Transform (DWT)
- Discrete Cosine Transform (DCT)

iii) ***Misrepresentations or Distortion Techniques****:* In this framework we require information of the chief cover picture with the confining strategy. Here the decoder capacity check between the primary cover picture and the wasted cover picture with a specific extreme target to re-establish the mystery message. The encoder adds a social occasion of advancement to the cover challenge. Thus, data is explained as being secured by flag twisting [12]. Using this structure, a stego dissent or question is made by applying a course of action for adjustment of the cover picture. This movement of modification is used to rewrite the problem message required to transmit [13]. The message is encoded in pseudo-haphazardly picked pixels. The stego-picture is fascinating in association with the cover picture at the given message pixel, the message bit is a "1." normally it is "0". The encoder can change the "1" respect pixels in such a course to the point that the honest properties of the picture are not influenced. Regardless the need for sending the cover picture restrains the upside of this framework. In any steganographic structure, the cover picture to never be utilized more than once. On the off chance that an aggressor changes the stego-picture by altering, scaling or turning, the beneficiary cannot recollect it. From time to time, if the message is encoded with spoil reviewing the data, the change can even be traded and the fundamental message can be recovered [14].

iv) ***Filtering and Masking:*** This method conceals data by denoting an image similarly as paper watermark. This strategy embeds the data in the huger regions than simply concealing it into the noise level. The concealed message is more important to cover picture. They are more joined into the picture when watermarking methods can be associated without the fear of picture damage in light of pressure.

Some focal points and weaknesses of filtering and masking techniques:

Focal point:

- Significantly the said technique is much powerful as compared to least significant bit. Data is covered up into unmistakable slices of the image or picture.

Weaknesses:

- Strategies can be associated just excessively dim or dark scale pictures and restrict it to 24 bits.

2. Analysis

Steganography is an upcoming research area that uses images, videos, and network protocols, and audio for information concealment. From the last time in the spatial domain, several approaches for digital steganography have been proposed. These approaches are based on LSB substitution, edge based embedded, and pixel indicator based embedded.
Every approach has its relating advantages and disadvantages. Some methods have high payload limits and great softness were blurriness depend on the chosen cover for covert or unknown information, concealing (Spatial domain) but more vulnerable against assaults (Noise tossing, rotation, revolution, resizing and so forth) while other schemes are strong against factual or statistical assaults, so far, they have brought down payload boundary. This implies that is reliably an exchange off between the three mechanisms (Payload, Imperceptibility& Robustness).

We will summarize different methods with their related advantages and disadvantages based on image steganography, which is discussed one by one below.

Hanling et al. proposed a new pixel esteem (value) differencing procedure; for data embedding near the goal pixel it used the three pixels. It utilizes essential k-bit LSB technique for mystery information implanting with high refinement regard where the number of k-bit is assessed by pretty much three pixels. It basically uses a perfect pixel adjustment method on target pixels to hold better visual quality and high breaking point. Histogram of stego-picture and cover-picture is generally same in the great position of the procedure, however dataset for tests are closed to nothing [15].

Channalli et al. proposed LSB based picture covering approach. Conventional outline bits (stego-key) are utilized to cover information. The minimum noteworthy piece of the pixel is adjusted relying on the (stego-key) layout bits and the secret message bits. Representation bits are composite of MxN measure lines and regions (of a piece) and with erratic key esteem. Whenever fulfilled it change the second LSB bits of cover picture generally continues as already. Every illustration bit is facilitated with the message bit in covering the system. This method centers to achieve security of masked message in the stego-picture using a run of the mill case key. The major disadvantage in the proposed procedure his a low covered farthest point since single secured bit requires a bit of (MxN) pixel [16].

Jung, K. H et al. proposed a strategy for Multi-Pixel Differencing (MPD) for data implanting, It process aggregate of refinement estimation of four pixels square and uses extra two pixels to scale smoothness of each pixel. It is utilized for little refinement esteem. For high complexity esteem it uses a multi pixel differencing system for data covering. So exploratory dataset is too much obliged, but quality is its straightforwardness of figuring [17].

Yang, et al. proposed a data covering methodology to cover the data using LSB where it finds the darkness locale of the picture. Using 8 pixels organize plans for concealing data bits; it changes over it to two-fold picture and denotes each dissent. The strategy requires high tally to discover diminish region. Its openness and has no endeavoured to high surface sort of picture. Thoroughly, endless supply of image which covers its limits. [18]

Mahdi et al. proposed another picture steganography strategy, with assertion of emotional pixel of the required picture region and in light of LSB substitution. The mystery key is incorporated by LSB pixels this technique is centred to upgrade. A Mystery message must be concealed if it creates irregular numbers and picks the region by combining. It is not yet considered a perceptual straightforwardness but the nature of the technique is its security of hiding messages in stego-image. [19].

Babita et al. proposed a new image steganography method, to embed data. It uses 4 LSB of each RGB channel. It applies focuses sifting to upgrade the possibility of the stego picture and encodes the refinement of cover and stego picture as key information. To isolate the covered data in separating stage the stego-picture is added with key data. It also needs to supervise stego-key which it fabricates the multifaceted nature of applying filters. The major demerit of the proposed scheme is covering limit of high secret data. [20].

Bailey et al. proposed stego shading cycle (SCC) strategy for shading images that conceals information in various channels of the cover image in a cyclic way. The primary mystery bit is covered up in pixel1's red channel, the second mystery bit is covered up in the green channel of pixel2 and the third mystery bit is covered up in the blue channel of pixel3. The significant confinement in SCC technique is that the mystery data is installed in cover image pixels in a settled cyclic and orderly way. So, aggressors can without much of a stretch find this strategy if mystery data from a couple of pixels is effectively separated [21].

Gutub et al. proposed a high payload pixel pointer method (PIT) what one channel is utilized as a marker and the other two channels are information channels. The proposed strategy shrouded the puzzle information in either of the information which

directs in a predefined cyclic way. The provisional outcomes demonstrate the incredible limit and better delicate quality of the arranged calculation and furthermore dodge the key trade overhead. The major feeble purpose of this technique is that the payload limit is absolutely subject to have pictures and marker bits which can result in low payload. Similarly, this method hides fixed numbers of bits in each pixel which can be brought more changes in the cover image if we embed a greater number of secret bits in each pixel. The major limitation in the proposed method is that the secret information can be extracted easily if an attacker finds out the algorithm being used for message hiding because secret data is in plain text form not encrypted. Moreover, these methods result in stego images of low quality which can be detected using HVS [22].

Karim et.al presented a new approach to enhance the security of the existing LSB substitution method by adding one extra barrier of the secret key. In the said method, secret key and red channel are used as an indicator while green and blue channels are data channels. Basis of covered key bits and red channel LSBs the secret data bits are embedded either in green channel or in the blue channel. If either the bit of the red channel LSB or the secret key bit is 1, then the LSB of green channel is replaced with secret message bits otherwise LSB of blue channel is replaced by secret bit. Although this approach possesses the same payload as LSB based approaches, it increases security by making the use of a secret key. An intruder cannot easily extract the secret information without the correct secret key [23].

Muhammad et.al presents an ensured strategy for shading picture steganography using gray-level modification and multilevel encryption. The security of information between two social gatherings is noteworthy issue in this front-line area. To adjust these issues proposed plot is a viable procedure for RGB pictures in light of diminishing or dim dimension change gray level modification (GLM) and staggered encryption (MLE). The mystery key and secret information are encoded utilizing MLE calculation before mapping it to the dark levels of the cover image. At this point, a transposition work is connected on cover image preceding information stowing away. The use of the transpose mystery key, MLE, and GLM includes four unique levels of security to the proposed calculation making it extremely troublesome for a vindictive client to extricate the first secret data. However, the proposed scheme provides a robust, efficient and time saving way to hide secret information inside the cover image. The main advantages of the proposed scheme improve quality of stego images, high imperceptibility, cost-effectiveness, and enhanced robustness. Moreover, the utilization of MLE and image transposition adds multiple security levels to the said technique. The major shortcoming of this method is its vulnerability to different attacks (cropping, scaling and noise attacks) which exist in all spatial domain techniques including the existing five schemes. Since the spatial domain is used in the proposed approach, the hidden data cannot be fully recovered if the image is compressed, scaled or attacked with noises [24].

F. A Jassim et al proposed a protected strategy whose key thought depends on the way that adjoining pixels in pictures are firmly connected with one another. In FMM plot, the picture is isolated into various obstructs, every one of which contains k×k pixels where k demonstrates the window measure and every pixel speaks to a number in the range 0-255 distinct by 5 for 8-bit pictures. The proposed ST-FMM strategy is better in power and accomplishes great nature of stego pictures. In any case, there is an exchange off between the payload and window size with the end goal that expands the window estimate diminishes the payload and the other way around [25].

Wang, et al proposed a superb steganographic technique dependent on pixel value differencing (PVD) and modulus work, which is more secure against the different identification assault and performs superior to anything the PVD conspire. This plan expands the pinnacle motion (PSNR) qualities to 44.15 dB while disguised 51,219 bytes. It abuses the rest of the two continuous pixels to record the data of the inserted information. It accomplishes greater adaptability, fit for

determining the ideal rest of the two pixels in any event mutilation. This strategy expands the PSNR (up to 8.9%) more than the straightforward PVD technique. To keep up the distinction in a similar range when inserting process, this technique utilizes rearranging system to change the notice of the pixel combine [26].

Joo, et al. exhibited an improvement on [32] technique by installing distinctive measures of mystery information depending on pixel-match intricacy. The test in this strategy demonstrates that the distinction histogram had a shape nearer to the cover-picture which was difficult to be identified by histogram examination. Despite the fact that this technique enhanced the issue of the shape in the distinction histograms. The inserting limit isn't higher than Wang et al strategy, which is differing for the odd and even implanting zones [27].

Chen et al presented a PVD strategy utilizing pixel pair matching (PPM). In this strategy, the cover-picture is apportioned into 2 × 2 inserting cells for installing by arbitrary implanting plans. To expand the arbitrary inserting trademark, two reference tables are made. This irregular system raises the security of the implanted information from discovery and different steganalysis assaults. The real commitments of this methodology are: (1) PPM was used subsequently a bigger number of information disguised than unique PVD, (2) Effectively diminishing the tumbling off-limit issue of controlling just on Pivot Embedding Unit (PEU). (3) The mystery information was covered which was dependent on two reference tables which raised the irregular trademark and the visual quality. (4) This strategy is harder to be recognized for its distinction histogram. It shows that the estimations of the stego-picture are near the estimations of the cover-picture. Chen plot altogether had higher limit and picture quality [28].

Al Dhamari et al proposed another square based steganographic calculation utilizing PVD and modulus work procedures, to be specific, MF-PVD. To assess the execution of MF-PVD calculation, they contrast it and six relevant conditions of-workmanship calculations, as an obvious truth, the proposed MF-PVD calculation is exceptional to these reference techniques in two fundamental highlights, the inserting limit and the security. Actually, the security of calculation is high because of producing numerous stages and existing the separate extend table. The calculation's system can be stretched out to the RGB shading pictures for enhancing the ability of inserting. In addition, it may be a decent expansion to build up a methodology that considers the half breed area. So there are tentative arrangements to create modulus work based plans for other media, for example, sounds and video [29].

Khan et al proposed a novel picture steganographic procedure (M-LSB-SM) for shading pictures with better indistinctness and security. A normal PSNR of 47.93 dB is registered more than one hundred and fifty pictures. The mystery data are separated into four sub-squares and is gone through MLEA, which makes the assault on this calculation dreadful and therefore, deceives the procedure of steganalysis. This is the reason that their proposed plan is equipped for producing stego pictures of an adequate quality that satisfies the ideal requests of current security frameworks and clients. The calculation is straightforward, simple to execute and a decent blend of subtlety and security and therefore is more possible to be embraced by steganographic applications. Still extra upgrades are feasible broadening MLE calculation and payload capacity.

Table II shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 50-65.
Table III shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 45-50
Table IV shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 38-45.

Table II: Analysis of Different Image Steganographic Techniques in Spatial Domain Based on PSNR in the Range of 50-65

S.NO	Existing Methods	PSNR Values
1	Khan et al method 2[36]	63.0034
2	Khan et al method 1[24]	58.7344
3	Karim's Method[23]	52.2172
4	Classic LSB Method[7]	52.2416
5	SCC Method[27]	52.2023
6	Channali et al [16]	51.9764

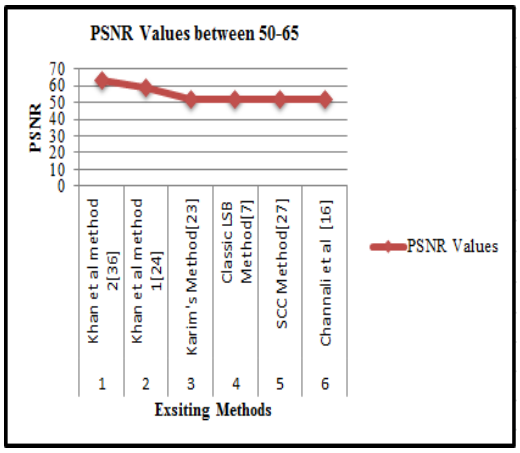

Fig.3. PSNR values of Exsiting methods Between 50-65

Figure 3 shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 50-65. It seems that khan et al method [36] having PSNR value 63.0034 which dominate over all other methods, that show the visual quality of the image.

Table III.: Analysis of Different Image Steganographic Techniques in Spatial Domain Based on PSNR in the Range of 45-50

S.NO	Existing Methods	PSNR Values
1	Hangling et al [15]	49.5545
2	Wang et al [32]	49.2565
3	PIT [11]	48.5249
4	Mehdi et al [19]	48.2454
5	Gutub et al [22]	47.4536
6	Jung K H et al [17]	45.5677

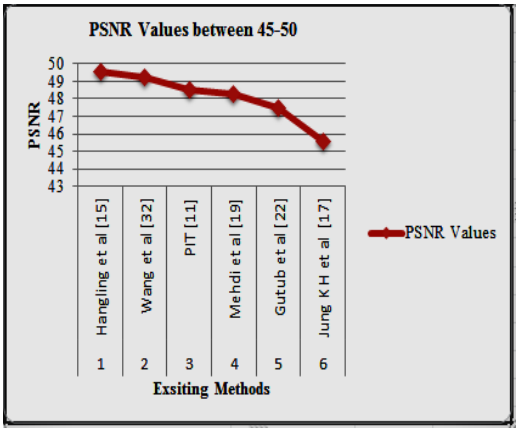

Fig. 4. PSNR values of Exsiting methods Between 45-50

Figure 4 shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 45-50. It seems that Hangling et al method [15] having PSNR value 49.5545 which dominate over all other methods, that show the visual quality of the image.

Table IV: Analysis of Different Image Steganographic Techniques in Spatial Domain Based on PSNR in the Range of 38-45

S.NO	Existing Methods	PSNR Values
1	F A jassm et al [25]	44.3455
2	Baily et al [21]	43.3425
3	Joo et al [33]	42.5352
4	Yang et al [18]	42.4553
5	FMM[26]	41.294 4
6	Al Dhamari et al [35]	39.5676

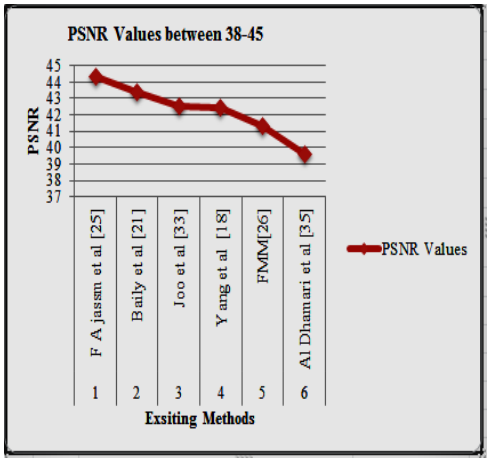

Fig.5. PSNR values of Exsiting methods Between 38-45

Figure 5 shows the analysis of different image steganographic techniques in spatial domain based on PSNR in the range of 38-45. It seems that F A jassm et al method [25] having PSNR value 44.3455 which dominates over all other methods, that show the visual quality of the image.

Table.V shows ciritical analysis up to eighteen methods with their advantages and disadvantages and also analyzed based on measuring alogrithm (Capacity, Robustness, Perception, Temp protection, computation) which is the basic criteria of steganography, which is also shown in Table I.

3. Conclusion and Future Work

Specialists have introduced different plans to adapt web security issues. In this specific situation, both steganography and cryptography can be utilized successfully. However, real restriction in the current steganographic techniques is the low-quality yield stego images, which subsequently brings about the absence of security.

This paper provides an illustration of a number of steganographic methods; its significant kinds and arrangement of steganography in the recent couple of years have been proposed. We have dissected various proposed systems. It is demonstrated the visual nature of the image is corrupted when shrouded information expanded up as far as possible utilizing LSB based strategies. Analysis of the truthful properties of commotion or visually investigation strategies can be broken or demonstrates significant adjustment of image.

In this study, distinctive steganographic articles were contemplated and were ordered into various methods. The same numbers of new application zones are recognized like web managing an account, portable correspondence security, cloud security and so on. The understanding into the steganographic standards will certainly control us to recognize new zones and to enhance its applications in the effectively existing application regions also.

ACKNOWLEDGEMENT

The authors wish to thank every one of the supporters for their basic and specialized review of the proposed work and their important help and direction. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers.

Table V: Investigation of Different Image Steganography Techniques in Spatial Domain

SNo	Domain	Techniques	Advantages	Disadvantages	Analysis based on				
					Capacity	Robustness	Perception	Temp protection.	computation
1	Spatial[15]	PVD with Adaptive LSB	Histogram of both original and stego image is always same	for experimental results Data sets is too small	Yes	Yes	No	No	No
2	Spatial[16]	Pattern bits combinations along with (Stego-Key) using LSB	Hidden Data	Hidden Capacity is Low	No	No	No	No	No
3	Spatial[17]	MPD with LSB	Same as PVD but on some level is valuable from common PVD methods	Limited data sets, and Threshold, both sides Stego key require	Yes	Yes	No	No	No
4	Spatial[18]	Dark area of image with LSB substitution	Helpful for smooth district with strong limit of object based dataset	High calculation required and not tried on high surface zones	No	Yes	No	No	No
5	Spatial[19]	LSB substitution with Random pixel selection	Safety of hidden message in Stego-image	Implanting without thinking about Graphic Quality in Arbitrary pixel determination	No	No	No	No	No
6	Spatial[20]	LSB substitution with Median Filtering	High hidden capacity	Computationally confusing (sifting) in Stego-key essential	Yes	No	No	No	No
7	Spatial[21]	Stego Colour Cycle	Hiding data different channels	Embedding is a fixed cyclic and systematic way, easily can extracted if a few bit extracted	Yes	No	Yes	No	No
8	Spatial[22]	PIT	High hidden data better imperceptibility	shipment limit is absolutely reliant on host picture and pointer bits	Yes	Yes	Yes	No	No
9	Spatial[23]	LSB substitution replacement method	High payload , better imperceptibility by adding one extra barrier of secret key	Increasing security depending on secret key can easily extracted without correct key	Yes	Yes	Yes	No	Yes
10	Spatial[24]	GL- Modification and MLE	high imperceptibility, times Saving and robustness	vulnerability to different attacks (cropping, scaling and noise)	No	Yes	Yes	Yes	Yes
11	Spatial[31]	hiding text in image using five modulus method	Achievement of robustness and good quality of stego images	If increasing the window size then will be decrease payload	Yes	No	Yes	No	No
12	Spatial[32]	pixel-esteem differencing and modulus work	High Capacity, and good Image quality	vulnerability to different attacks	Yes	No	Yes	No	No
13	Spatial[33]	protecting pixel-esteem differencing histogram with modulus work	Enhanced Security and perception transparency	Hidden data too low	No	Yes	Yes	No	Yes
14	Spatial[34]	histogram preserving using pixel pair matching	Higher limit and Better Quality	vulnerability to different attacks	Yes	No	Yes	No	Yes
15	Spatial[35]	modulus function and pixel-value differencing	Embedding capacity and the security	Perception and vulnerability to different attacks(Noise ,cropping)	Yes	Yes	No	No	Yes
16	Spatial[36]	MLE and achromatic component of an image	Security and good imperceptibility	visual quality, payload limit and vulnerability of statistical attacks	No	Yes	Yes	No	Yes
17	Spatial[38]	Data Mapping and LSB Substitution	Embedding capacity and visual quality	Temper protection and computation	Yes	Yes	Yes	No	No
18	Spatial [39]	logistic map and secret key	High security, payload, Visual quality	Vulnerabilities(noise, copping) computation	Yes	No	Yes	Yes	No

REFERENCES

[1] Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. *IEEE Journal on selected areas in communications*, *16*(4), 474-481.

[2] I. Diop, S. Farss, K. Tall, P. Fall, M. Diouf, and A. Diop, "Adaptive Steganography scheme based on LDPC codes," in *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, 2014, pp. 162-166.

[3] Pfitzmann, B. (1996, May). Information hiding terminology-results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding* (pp. 347-350). Springer-Verlag.

[4] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2).

[5] Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. *IEEE signal processing letters*, *12*(6), 441-444.

[6] Kour, J., & Verma, D. (2014). Steganography Techniques–A Review Paper. *International Journal of Emerging Research in Management &Technology ISSN*, 2278-9359.

[7] A. Sharp, Q. Qi, Y. Yang, D. Peng, and H. Sharif, "A video steganography attack using multi-dimensional Discrete Spring Transform," in *Signal and Image Processing Applications (ICSIPA), 2013 IEEE International Conference on*, 2013, pp. 182-186.

[8] Hu, S. D. (2011, August). A novel video steganography based on non-uniform rectangular partition. In The 14th IEEE International Conference on Computational Science and Engineering (pp. 57-61). IEEE.

[9] Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2)..

[10] Lin, E. T., & Delp, E. J. (1999, April). A review of data hiding in digital images. In *PICS* (Vol. 299, pp. 274-278).

[11] Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In *Information hiding* (pp. 43-78).

[12] Reddy, H. M., & Raja, K. B. (2009). High capacity and security steganography using discrete wavelet transform. *International Journal of Computer Science and Security (IJCSS)*, *3*(6), 462.

[13] Aos, A. Z., Naji, A. W., Hameed, S. A., Othman, F., & Zaidan, B. B. (2009, April). Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File. In *Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of*(pp. 437-441). IEEE.

[14] Kruus, P., Scace, C., Heyman, M., & Mundy, M. (2003). A survey of steganography techniques for image files. *Advanced Security Research Journal.[On line]*, *5*(1), 41-52.

[15] Hanling, Z., Guangzhi, G., & Caiqiong, X. (2009, May). Image steganography using pixel-value differencing. In *Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on* (Vol. 2, pp. 109-112). IEEE..

[16] Channalli, S., & Jadhav, A. (2009). Steganography an art of hiding data. *arXiv preprint arXiv:0912.2319*.

[17] Jung, K. H., Ha, K. J., & Yoo, K. Y. (2008, August). Image data hiding method based on multi-pixel differencing and LSB substitution methods. In *Convergence and Hybrid Information Technology, 2008. ICHIT'08. International Conference on* (pp. 355-358). IEEE.

[18] Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, *3*(3), 488-497..

[19] Islam, A. U., Khalid, F., Shah, M., Khan, Z., Mahmood, T., Khan, A., ... & Naeem, M. (2016, August). An improved image steganography technique based on MSB using bit differencing. In *Innovative Computing Technology (INTECH), 2016 Sixth International Conference on* (pp. 265-269). IEEE.

[20] Chen, W. J., Chang, C. C., & Le, T. H. N. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with applications*, *37*(4), 3292-3301..

[21] Motameni, H., Norouzi, M., Jahandar, M., & Hatami, A. (2007). Labeling method in Steganography. *World Academy of Science, Engineering and Technology*, *24*, 349-354...

[22] Viswanatham, V. M., & Manikonda, J. (2010). A novel technique for embedding data in spatial domain. *International Journal on Computer Science and Engineering, IJCSE*, *2*(2010)....

[23] Yang, H., Sun, X., & Sun, G. (2009). A high-capacity image data hiding scheme using adaptive LSB

substitution. *Radioengineering*, *18*(4), 509-516.

[24] Parvez, M. T., & Gutub, A. A. A. (2008, December). RGB intensity based variable-bits image steganography. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE* (pp. 1322-1327). IEEE.

[25] F. A. Jassim, "A novel steganography algorithm for hiding text in image using five modulus method," *arXiv preprint arXiv:1307.0642*, 2013. Article (CrossRef Link)

[26] Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software, 81(1), 150-158..

[27] Joo,J. C., Lee, H. Y., & Lee, H. K. (2010). Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP Journal on Advances in Signal Processing, 2010(1), 249826.

[28] Chen, J. (2014). A PVD-based data hiding method with histogram preserving using pixel pair matching. Signal Processing: Image Communication, 29(3), 375-384.

[29] Al-Dhamari, A. K., & Darabkh, K. A. (2017). Block-based steganographic algorithm using modulus function and pixel-value differencing. Journal of Software Engineering and Applications, 10(01), 56.

[33] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. *TIIS*, *9*(5), 1938-1962..

[34] Zakaria, A., Hussain, M., Wahab, A., Idris, M., Abdullah, N., & Jung, K. H. (2018). High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution. Applied Sciences, 8(11), 2199.

[35] Majeed, A., Mat Kiah, M. L., Madhloom, H. T., Zaidan, B. B., & Zaidan, A. A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. *International Journal of Engineering and Technology*, *1*(2), 63-69..

[36] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications, 75(22), 14867-14893.

[37] Solanki, R., Chuahan, M., & Desai, M. SURVEY OF IMAGE STEGANOGRAPHY TECHNIQUES..

[38] Bandhyopadhyay, A., Dey, D., Pal, R. K., & Maji, A. K. (2018). An Indirect Addressing Image Steganographic Scheme Using 9× 9 Sudoku Matrix. In Proceedings of the International Conference on Computing and Communication Systems (pp. 689-703). Springer, Singapore.

[39] Ulker, M., & Arslan, B. (2018, March). A novel secure model: Image steganography with logistic map and secret key. In Digital Forensic and Security (ISDFS), 2018 6th International Symposium on (pp. 1-5). IEEE.

[40] Liao, X., Yin, J., Guo, S., Li, X., & Sangaiah, A. K. (2018). Medical JPEG image steganography based on preserving inter-block dependencies. Computers & Electrical Engineering, 67, 320-329.