2022 2nd International Conference on Computing and Information Technology (ICCIT)
Jan. 25 - 27, 2022/ FCIT/UT/KSA

Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review

Muhammad Adnan Aslam[1]
[1]Department of Computer & Software Engineering, College of E&ME, National University of Sciences and Technology (NUST), H-12, Islamabad, Pakistan.
adnan.aslam18@ce.ceme.edu.pk

Muhammad Rashid[2]
[2]Computer Engineering Department Umm Al-Qura University, Makkah, Saudi Arabia
mfelahi@uqu.edu.sa

Farooque Azam[1]
[1]Department of Computer & Software Engineering
College of E&ME, National University of Sciences and Technology (NUST), H-12, Islamabad, Pakistan
farooq@ceme.nust.edu.pk

Muhammad Abbas[1]
[1]Department of Computer & Software Engineering
College of E&ME, National University of Sciences and Technology (NUST), H-12, Islamabad, Pakistan
m.abbas@ceme.nust.edu.pk

Yawar Rasheed[1]
[1]Department of Computer & Software Engineering
College of E&ME, National University of Sciences and Technology (NUST), H-12, Islamabad, Pakistan
yawar.rasheed18@ce.ceme.edu.pk

Saud S. Alotaibi[3]
[3]Department of Information Systems,
Umm Al-Qura University, Makkah, Saudi Arabia
ssotaibi@uqu.edu.sa

Muhammad Waseem Anwar[1]
[1]Department of Computer & Software Engineering, College of E&ME, National University of Sciences and Technology (NUST), H-12, Islamabad, Pakistan.
waseemanwar@ceme.nust.edu.pk

2022 2nd International Conference on Computing and Information Technology (ICCIT) | 978-1-6654-3605-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCIT52419.2022.9711628

***Abstract*— Digital image steganography is used to hide confidential data within a cover image. In this context, least significant bit (LSB) is a well-known steganography approach. As LSB is frequently applied for image steganography, there is a strong need to explore and summarize the state-of-the-art LSB approaches for image steganography. Therefore, this article performs a Systematic Literature Review to identify 20 research studies available during 2016-2020. This leads to the identification of 17 image steganography approaches / algorithms and 20 datasets for the evaluation of image steganography techniques. Furthermore, 3 leading frameworks / tools are presented. In addition to that, to evaluate the quality of the image steganography, 4 of the prime parameters which are frequently used have also been identified. It can be safely claimed that the image steganography quality is significantly improved through LSB via enhanced PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Square Error). However, the size and secrecy of secret data is the biggest challenge while applying LSB techniques.**

***Keywords*—Image Steganography, Least Significant Bit, Systematic Literature Review, Peak Signal-to-Noise Ratio, Mean Square Error.**

I. Introduction

Advancement of technology, particularly the evolution of speedy internet for long distance communication, has enabled the information to travel far and wide across the world. This has made the world a global village in true sense. However, at the same time cyber-attacks and leakage of sensitive information have made people and organizations anguish about the secrecy and privacy [1], [2]. Image steganography is the technique of hiding a message into a cover image [3]. Various applications of Image Steganography have emerged over the period of time along with the technological evolution [4], [5], [6]. Many organizations are spread across the globe and they need to communicate frequently by take advantage of the enormous facilities that internet provides, however, mostly, internet users are concerned about their privacy and anonymity. Therefore, Specific methods and algorithms are always more than welcomed by the concerned individuals/ organizations and their respective employees to secure their intellectual properties/ and proprietary assets as well as information sent via internet.

Since image steganography offers variety of approaches/ techniques to hide the information of interest. Thereafter it may serve the purpose of providing sense of security to the internet users by hiding their information of interest. It enables the secret communication of two parties to take place in an undetected manner thus avoiding the malicious attacks [4]. It also offers copyright protection on digital files by utilizing the message as a secret digital watermark. None the less, even top-secret documents can be transmitted, embedded within the images [7]. On the other hand, attackers can also use image steganography to send malware and Trojans to oblivious users.

Several Image Steganography techniques are in vogue, amongst which, Least Significant Bit (LSB) [6]-[20] is a well-known approach. It is used to embed the secret message/ data/ information within a cover image. Two famous sub techniques that can be covered under the umbrella of LSB are (i) Insertion based Method (ii) Substitution based Method [8]. Both are widely adopted and used for hiding data but there are some differences between them. Insertion based method increases the size of the image when secret data is embedded while on other hand the substitution based method is used to replace the bits of the image with secret data without increasing the size of the image [14].

The past decade has seen rich contribution to the domain of image steganography by the researchers due to its obvious significance. In this regard, various steganography techniques are comparatively analyzed in a survey presented by the authors of [21]. However, the limitations of such surveys are that they do not encompass latest advancement in this domain. Moreover, another important aspect that need to be highlighted is that the LSB based image steganography approaches are particularly hard to find in literature. Therefore, there is a dire need that the latest LSB based Image steganography approaches may be explored and summarized. This will certainly help to identify the targeted image steganography areas where modern LSB approaches have been applied so far. Furthermore, this will also facilitate the

practitioners and researchers to select the right LSB approach for a particular image steganography requirement. Therefore, this article performs Systematic Literature Review (SLR) [22]-[24] to answer the following research questions:

RQ1: What are the latest and important research studies where LSB is utilized for image steganography during 2016-2020?

RQ2: What are the leading techniques and algorithms that have been proposed / offered by the researchers for LSB based image steganography?

RQ3: What are the leading and publically available datasets for LSB based image steganography?

RQ4: What are the crucial evaluation parameters for the quality assessment of image steganography?

RQ5: What are the existing implementation frameworks / tools for LSB based image steganography?

RQ6: What are the fundamental advantages and limitations of utilizing LSB for image steganography?

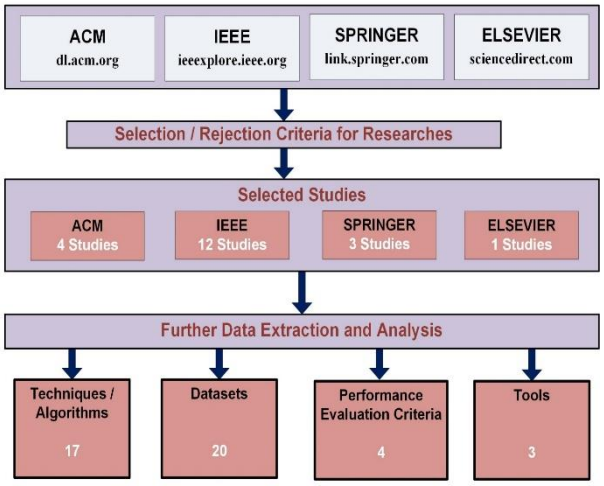

Fig. 1. *Research Study – An Overview*

In order to conduct this study, four of the very renowned repositories (i.e. IEEE, ACM, Springer and Elsevier) have been explored. Developing the review protocol (Section II) including Selection Rules (Section II A and II B), consequently, helped us identify 20 studies in order to achieve the sole purpose of this SLR as shown in Figure 1. The results are presented in Section III. Answers to formulated RQs along with the discussion is presented in Section IV. Finally, Section V presents the concluding remarks.

II. REVIEW PROTOCOL

In this section, the Review Protocol details are summarized. The details are summarized in subsequent sections as:-

A. Selection Rules

Rules have been defined in order to select the research articles. On one hand these rules endeavour to find the answer of the RQ's (Section I) and on the other hand a high quality outcome is enforced. The rules are

- Only those research studies may be selected where LSB Based Image Steganography approach has been explored.
- Only those researches are selected if the research has been published in any one of the renowned scientific repositories of Springer, IEEE, Elsevier and ACM.
- Only those research studies are considered that are published with in the time duration 2016-2020.
- A research study may be selected only if all of the above mentioned rules are followed, the violation of a single rule will cause rejection of the study e.g. a study following the first two rules but published before 2016 should be rejected.

B. Search process

The search process is here in after performed on the basis of well-defined selection rules. Only four recognized and well known repositories as given in the second selection rule (Section A) have been searched. A year filter (i.e. 2016-2020) has been applied during the search process in order to enforce the third selection rule. We have also used the combination of various search terms to get the optimum search results. The results are summarized in **Table I**.

TABLE I. SEARCH RESULTS – SUMMARY

Sr. #	Search Queries	Search Results			
		ACM	IEEE	Springer	Elsevier
1	Image steganography	467	250	345	112
2	LSB steganography	256	348	170	212
3	Steganography Data Protection	650	450	256	354
4	Multilevel data hiding	267	265	338	198
5	Adaptive reversible images	179	188	218	218
6	Steganography Enhancement	80	192	103	201

Table 1 depicts the different search queries that are used to get the corresponding results from each of the repository. The relatively larger search queries (e.g. Steganography Data Protection) enumerate a very large number of search results which cannot be fully evaluated against first selection rule. Therefore, applying advanced filters like journals selection (Springer) to further reduce the search results, served the purpose. To evaluate the first selection rule, we perform certain steps as shown in Figure 2.

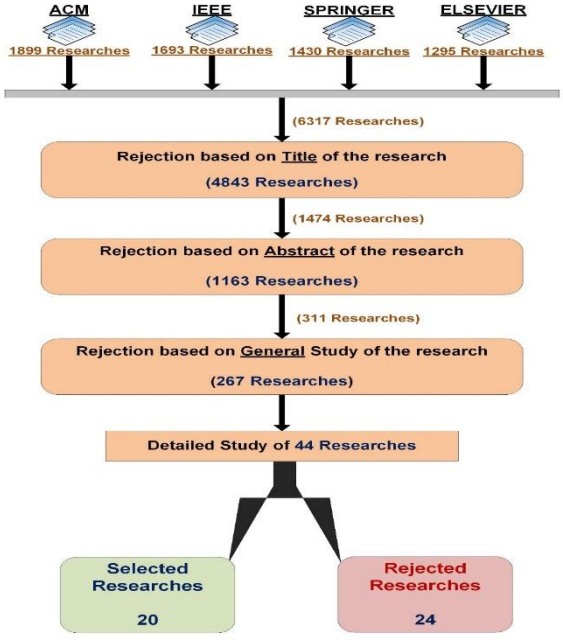

Fig. 2. *Steps for Selection of Research Studies*

Figure 2 shows that a total of 6317 search results were obtained. However, 4843 results were rejected on the basis of

irrelevant study title. Furthermore, 1163 abstract based rejections were made. Subsequently, 267 studies were rejected by reading various sections. Finally, 44 studies were thoroughly investigated to select final 20 studies which are completely satisfying the all three selection rules (Section IIA).

C. Quality Assessment

We have selected the prominent scientific repositories that always publish high quality research studies. In this manner, high quality outcomes of this study has been ensured and the obtained results are considered as reliable. The distribution of selected studies is given in **Table II.**

TABLE II. SELECTED RESEARCHES WITH REFERENCE TO DATABASES

Sr. #	Databases		References	Total
1	IEEE	Conference	[1][2][3][4][5][6][7][8] [9][10][15] [17]	12
		Journal	NIL	0
2	Springer	Conference	NIL	0
		Journal	[18][19][20]	3
3	ACM	Conference	[11][12][13][14]	4
		Journal	NIL	0
4	Elsevier	Conference	[16]	1
		Journal	NIL	0
Total				20

An endeavor has been made to include the latest studies. The year wise distribution of selected studies is given in **Table III.**

TABLE III. SELECTED RESEARCHES AS PER PUBLICATION YEAR

Sr.#	Year	References	Total
1	2016	[3][5][8][10][15][16]	6
2	2017	[2][7][12][13][17][19]	6
3	2018	[1][4][14][18]	4
4	2019	[6][11]	2
5	2020	[9][20]	2

D. Data Extraction

The In order to extract and analyze the information of interest from the selected research studies, various data extraction/ synthesis parameters have been defined so that answers to the RQs may be provided. **Table IV** shows the relevant details.

TABLE IV. PARAMETERS – DATA EXTRACTIONS AND SYNTHESIS

SR. #	Parameter	Specifics
1	Common information	Name of Author, study title, publisher details, publication year
Data Extraction		
2	Summary of study	Purpose of Study, Significance and Findings, impact
3	Limitations	Assumptions (if any)
4	Proof-of-concept	Evaluation via experimentation or other proof-of-concept methods
Synthesis of Data		
5	Techniques & Algorithms	Techniques and algorithms for image steganography in selected studies (**Table V**)
6	Datasets	Data sets used in selected studies (**Table VI**)
7	Evaluation Parameters	Parameters used to evaluate the quality in selected studies (**Table VII**)
8	Leading Tools	Tools used for the implementation of image steganography techniques in selected studies

III. RESULTS

This section summarizes the outcomes of this SLR in order to obtain the answers of RQ's. The details are provided in subsequent sections.

A. Techniques / Algorithms

We have selected 20 LSB based image steganography studies which are published during the period 2016-2020. Since, the isolated application of LSB is not feasible to achieve desired results. Therefore, LSB is frequently applied with other techniques / algorithms. The utilization of LSB with other techniques / algorithm is summarized in Table 5. Particularly, first column of **Table V** provides the reference of selected study. The second column (Substitution LSB Replacement) evaluates the number of bits used in each selected study. Finally, additional techniques / algorithms utilized along with LSB is given in the third column of **Table V**.

TABLE V. IMAGE STEGANOGRAPHY TECHNIQUES IN SELECTED STUDIES

Ref	Substitution LSB Replacement				Additional Techniques/ Algorithm
	One Bit	Two Bits	Three Bits	Four Bits	
[1]	✓				RSA* Encryption algorithm
[2]	✓				SHA-1* hash Algorithm
[3]	✓				AES* + Wavelet Transform +Neural Network
[4]	✓				N/A
[5]		✓	✓		Specific Coordinates Cropping
[6]		✓			LZW* Algorithm
[7]			✓		Character Bit Shuffler
[8]			✓		AES* 256 bit Encryption
[9]				✓	Local Entropy Filter
[10]	✓				RSA*Encryption algorithm
[11]	✓				Hashing Encryption algorithm
[12]		✓	✓		N/A
[13]	✓	✓			Contrast Compression
[14]	✓		✓		Skewness and kurtosis
[15]	✓	✓	✓	✓	Improved LSB with directional algorithm
[16]	✓				Random Pixel Key
[17]	✓				OTP* Algorithm + Canny Algorithm
[18]		✓	✓		CRC-32*+ GZIP* + AES* Encryption
[19]		✓			Pixel Value Difference
[20]	✓	✓			SIPHT Compression algorithm +DWT* +SVD*

RSA* = Rivest–Shamir–Adleman SHA-1*=Secure Hash Algorithm
AES* = Advanced Encryption Standard LZW*= Lempel–Ziv–Welch
OTP* = One Time Pads GZIP* = GNU Zip
CRC-32*=Cyclic Redundancy Check DWT*=Discrete Wavelet Transform
SVD* = Singular Vector Decomposition

It may be noticed in **Table V** that LSB one bit approach is most commonly utilized (thirteen research studies). Furthermore, researchers simultaneously utilized multiple bits LSB approaches e.g. in [15], all four bits LSB approaches have been simultaneously utilized. It can also be analyzed from **Table V** that AES and RSA are leading techniques / algorithms which are used along with LSB to achieve certain

image steganography objectives. In two studies, [4] [12], only LSB is utilized without employing any additional technique / algorithm.

B. Datasets

Datasets have great importance while performing particular steganography operations. Therefore, we have identified and analyzed twenty datasets as given in Table 6. Particularly, first column of Table 6 provides reference of selected study. The name of dataset is given in second column (Dataset Name). The evaluation of datasets on the basis of certain characteristics is performed in third column (Characteristics). Particularly, third column is further sub-divided into five columns to evaluate different characteristics: 1) Cover File Type defines the type of dataset images like grayscale, RGB etc. 2) Cover File Size defines size of images in dataset like 521x512 etc. 3) Cover File Resolution defines resolution of dataset in terms of size e.g. 8 bit etc. 4) Secret Data Type defines type of secret data (e.g. image, text etc.) that need to be hide through LSB. 5) Secret Data Size defines size of secret data e.g. bytes / kilobytes etc. Finally, in last column (Availability), the accessibility of dataset is evaluated i.e. private or publically available. The results are summarized in **Table VI.**

TABLE VI. DATASETS USED IN THE SELECTED STUDIES

Ref.	Dataset Name	Characteristics					Availability
		Cover Image Type	Cover File Size in pixels & KB	Cover File Resolution	Secret Data Type	Secret Data Size	
[1]	Medical Images	Grayscale	512x512 & 320 x 320	8 bit	Image	19k	Public
[2]	Medical Images	Grayscale	512 x512	8 bit	Image	N/A	Private
[3]	Generic Images	RGB	108KB	N/A	Image	19KB	Public
[4]	Paralyzed images of a hand gesture	RGB	800x600 to 4000x3000	N/A	Text	175KB to 4.26 MB	Public
[5]	Child images	RGB	512 x 512	96 x96 dpi	Text	N/A	Public
[6]	Student Information	RGB	N/A	24 bit	Text	N/A	Public
[7]	Aerials Dataset	RGB	100x100	N/A	N/A	1857 Bytes	Private
[8]	Random Dataset	RGB	N/A	8 bit	N/A	N/A	Public
[9]	Aerial dataset	RGB	512x512	N/A	Image	512x512 pixels & 256x256 pixels	Public
[10]	Anime Images	RGB	256x256	N/A	Image	90x90 pixels	Public
[11]	Aerial Dataset	RGB	402 x 566	N/A	Text	N/A	Public
[12]	Window 10 Wallpapers	RGB	1920x1200	24 bit	Text	N/A	Public
[13]	10 Generic Images	RGB	N/A	N/A	Text	N/A	Public
[14]	632 natural images from INRIA Holidays dataset	RGB	600 x 450	180 pixels/inch	Text	270,000 bits	Public
[15]	Aerial dataset	RGB	360 x 360	N/A	Text	N/A	Public
[16]	Aerial dataset	Grayscale	512 x 512	8 bit	Image	128 x 128 pixels	Public
[17]	Opera dataset	Grayscale	512 x 512	8 bit	Text	8 bytes To 1024bytes	Private
[18]	Baboon and Lena Images	RGB	512 x 512	24 bit	Text	1KBS To 256KBS	Public
[19]	USC-SIPI Image Database	Grayscale	512 x 512	8 bit	Text	13116 bytes To 13259 bytes	Public
[20]	USC-SIPI Image Database	RGB	256 x 256 & 512 x 512	N/A	Image	256 x 256 pixels & 512 x 512 pixels	Public

It may be noticed from Table 6 that 12 research studies deal with textual or numerical secret data for steganography while 6 studies employed images as a secret data. There are two studies [7-8] that do not provide the details of secret data. It is important to note that there are 17 datasets [1] [3-6] [8-16] [18-20] which are publically available, so that, researchers and practitioners may utilize them for experimentation. On the

other hand, only 3 studies [2][7][17] utilize private datasets for experimentation.

C. Evaluation Criteria for Improvements

Once image steganography is performed through particular approach, the evaluation for the assessment of improvements is performed. In this regard, several parameters like embedding capacity, quality of original picture after steganography (Stego) etc. are utilized. There are four major parameters to evaluate the steganography quality which are:

- **PSNR :** (Peak Signal-to-Noise Ratio) is an expression to measure the maximum amount of distortion in the stego image after embedding the secret data in the cover image. Particularly, PSNR measures the similarity index between the cover image and the Stego Image. Higher PSNR means lower noise in the Stego image, consequently, the quality of stego image would be almost similar to the cover image.
- **MSE :** (Mean Square Error) represents the cumulative squared error between the stego image and the cover image. The lower the value of MSE, the lower the error.
- **CPU Consumption :** is related to the resources of machines that are utilized during the encoding and / or decoding of secret data. CPU Consumption is directly proportional to the efficiency of the proposed technique / algorithm.
- **Embedding Capacity :** is related to the maximum capacity available to hide the secret data into the cover image. Larger the embedding capacity, greater would be the amount of secret data hidden in the cover image.

In **Table 7**, aforementioned parameters are investigated while performing the evaluation of proposed technique in selected studies. It is analyzed that PSNR is frequently used to evaluate the performance of proposed approach in selected studies because it is a major requirement to keep the stego image same to cover/ original image. MSE is another important criteria as it deals with the encoding / decoding errors of secret data. Embedding capacity is only effective, if PSNR and MSE are also reasonable.

TABLE VII. PARAMETERS USED FOR THE EVALUATION OF IMPROVEMENTS / ENHANCEMENTS

Sr. #	Evaluation Parameters	References
1	PSNR alone	[4][9]
2	PSNR and MSE	[1][2][3][6][7][8][10][12][13] [14][15][16][17][18][19][20]
3	PSNR, MSE and CPU consumption	[5]
4	Embedding Capacity	[11]

D. Tools

It is analyzed from the investigation of selected studies that image steganography is mostly performed through Matlab platform [1-4][6][8-17][19-20]. Particularly, 18 of the selected studies have utilized matlab where different components like Image Processing Toolbox, Simulink, Neural Network Toolbox etc. are exploited to achieve particular image steganography goals. Whereas, only two studies [7][18] have been identified for utilizing other platform and languages. For example, authors in [18] have used Dot Net Framework and C# language for implementation. In [7], authors have used FPGA (field programmable gate array) hardware board and Java Language. It can be safely concluded that Matlab platform is highly supportive for image steganography through LSB approach.

It is important to highlight that Matlab platform is frequently utilized for implementation purposes. However, image steganography may involve other operations e.g. improving security of secret data before actual steganography. For such operations, researchers also employed other framework / tools. For example, few studies utilize Python Stepic and ezPyCrypto libraries [11] in order to perform cryptographic techniques on secret data. Similarly, other libraries / toolkits like OpenCV [25], Deeplearning4j [7], AlgART [26] etc. can be employed through JAVA Language to perform desired operations.

E. Overview of Studies

This section briefly summarizes the selected studies. Arslan et al. [1] proposed LSB technique for image steganography where the canny algorithm for Edge Detection is applied on cover image. Subsequently, the secret message is compressed by applying the swapped Huffman coding lossless compression technique. Finally, the compressed secret data bits are replaced with edges pixels bits of the cover images using classical LSB bits technique. In another study [2], secret data (medical image) is hidden in general cover image. Particularly, the separation of ROI and NROI for secret data is performed. Subsequently, SHA-1 algorithm is utilized to compute the hash of ROI. Finally, ROI is embedded in NROI using even odd incremental embedding algorithm. In another study, Seethalakshmi et al. [3] utilized AES encryption algorithm to encrypt the secret data and then convert the cover image into blocks of 16x16. Subsequently, IWT is applied on cover image to determine the pixels location for steganography using neural network. Finally, classic LSB algorithm is used to replace the LSB bits of pixels with the secrete data bits.

Eakbodin Gedkhaw et al. [4] considered the different size of covered images with different dimension like 1200*2000 and 5000*12000 and embedded the secret data using substitution based LSB technique. In another study, Khalid et al. [5] cropped image to specific coordinates and replaced the secret data bits with substitution LSB for hiding the students' information's in student images. Yıldıray et al. [6] utilized LZW (Lempel–Ziv–Welch) algorithm to compress the secret message. Subsequently, LSB bits of RGB image are replaced with compressed data through LSB. In another study [7], authors first encrypted the secret data using character bit shuffler algorithm. Subsequently, FPGA is employed to replace the image bits with data bits of secret data and covered image after converting in MIF format. In [8], authors propose a scheme to encrypt the secret data using AES (Advanced Encryption Standard) algorithm and then convert data into byte array. Finally, this array is embedded in to image using classic Substitution LSB Method.

Omar et al. [9] proposed K-LSB based data hiding scheme where last four bits are used to embed the secret image in cover image. To enhance the quality of cover image, quality enhancement algorithm i.e. 'relative global histogram stretching' (RGHS) is also utilized. Finally, local entropy filter is applied in order to extract the secret image from cover image. In another study [10], authors employ RSA (Rivest–

Shamir–Adleman) to determine the embedding position of secret image through public and private keys. Finally, LSB technique is applied to perform desired steganography operations. Muyco et al. [11] performed encryption and decryption operations on image through modified hashing and then performed enhanced LSB technique for improved steganography.

G.G Rajput et al. [12] proposed LSB technique where RGB windows wallpaper images are used to hide secret data. The cover images are rotated to 90 degree and then replaced the secret message binary bits to the color red, green, blue bits intensity. Similarly, authors in [13] use contrast compression technique to compress the cover image by calculating new lower maximum colour values of each three channels red, green, blue of RGB coloured image. Subsequently, the secret message is embedded to compressed covered image and after embedding again convert compress image to its original quality. In another study [14], author proposed an interactive scheme to select an appropriate suitable cover image to hide the secret data using secure LSB technique. Initially, the suitability of cover image is checked through skewness and kurtosis of the image. Finally, LSB is applied. Sherin Sugathan et al. [15] hides the secret data in cover image with directional approach. Particularly, LSB approach based on directional bit is proposed for data hiding.

Rupali Bhardwaj et al. [16] proposed an inverted bits substitution LSB technique where random pixels location is determined using a secret key. Subsequently, four bit LSB approach is applied for effective steganography. In [17], authors have employed canny algorithm to perform edge detection process of cover image. Subsequently, OTP random key for cover image is generated and conversion of data in binary format is performed. In [18], authors have proposed a new LSB based technique where the conversion of secret data into byte array is performed and then the checksum is computed using crc-32. Finally, LSB is applied to embed the data inside the stego image. In [19], authors have proposed a data hiding scheme for improving embedding capacity using mixed PVD and LSB by dividing image into two bit plane. LSB substitution is considered in lower bit planes and PVD in higher bit planes. In [20], authors have proposed a scheme to hide data efficiently using LSB technique where SIPHT compression technique is used to compress the secret data.

IV. Answers and Discussion

This section provides answers to each research question:-

RQ1: What are the latest and important research studies where LSB is utilized for image steganography during 2016-2020?

Answer: 20 research studies have been identified where LSB is utilized for image steganography. The categorization of studies on the basis of scientific repositories is given in **Table II**. Furthermore, the year based categorization of selected studies is presented in **Table III**.

RQ2: What are the leading techniques and algorithms that have been proposed / offered by the researchers for LSB based image steganography?

Answer: In this SLR, we have only selected those studies where LSB based approach for image steganography has been explored. Therefore, LSB is an integral part of each study. However, it has also been revealed during the course of SLR that researchers have also utilized additional techniques and algorithms along with LSB to achieve particular image steganography objective. In this regard, 17 techniques / algorithm, as identified, have been presented in **Table V.** Furthermore, analysis of the specific type of LSB approach (i.e. 1 bit, 2 bit, 3 bit and 4 bit) has also been given in **Table V**.

RQ3: What are the leading and publically available datasets for LSB based image steganography?

Answer: We identified 20 datasets, where 17 datasets are publically available and remaining 3 are private. The datasets are thoroughly analyzed through important characteristics. The details are given in Section III B **(Table 6).**

RQ4: What are the crucial evaluation parameters for the quality assessment of image steganography?

Answer: We identify four most frequently utilized parameters (i.e. PSNR, MSE, CPU consumption and embedding capacity) for quality assessment of image steganography. The details are given in **Table 7.**

RQ5: What are the existing implementation frameworks / tools for LSB based image steganography?

Answer: We identify 3 main frameworks / tools / languages to implement LSB for image steganography. The most frequently utilized framework / tool is Matlab followed by Java language and Python. The details are available in Section III D.

RQ6: What are the key benefits and limitations of utilizing LSB for image steganography?

Answer: We identify that LSB is mostly adopted by many researcher because of its big advantage that is simplicity and effective results for hiding the secret data but on the other hand we identify some limitations as well in LSB that is fixed number of secret data insertion up to four bits .The details has also been given in Table 5.

A. Limitations

Although the general guidelines regarding SLR have been followed, yet the room for limitations is always there and unavoidable. For example, four of the well-known repositories have been explored to select relevant studies, however, we may expect that some of the relevant studies may have been missed out which are part of other repositories such as Google Scholars and Wiley etc. Since, the selected repositories are well known/ widely recognized for their quality and high impact therefore this unavoidable limitation is not expected to significantly affect the outcome of this SLR

V. Conclusion

An SLR has been performed to investigate the application of LSB based image Steganography. Particularly, 20 of the most relevant researches (published during 2016-2020) have been selected. Subsequently, 17 approaches/ algorithms have been recognized for image steganography. In addition, for the evaluation of image steganography techniques, 20 data sets have also been identified. Furthermore, 3 leading frameworks/ platforms/ tools for implementation of image steganography and 4 leading parameter that are frequently used to evaluate the quality of image steganography are also identified and presented.

It is concluded that several publically available datasets exist for image steganography. Moreover, Matlab is a leading framework to carryout LSB implementations for image steganography. Furthermore, the parameters like PSNR,

MSE, CPU utilization and embedding capacity are highly effective for the quality assessment. Finally, it is analyzed that the size and secrecy of secret data is biggest challenge while applying LSB techniques. In this article, the application of LSB is investigated. However, we intend to investigate and compare other image steganography approaches in near future.

REFERENCES

[1] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," in Proceedings of 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, pp. 1-4, 2018.

[2] M. S. Sreekutty and P. S. Baiju, "Security enhancement in image steganography for medical integrity verification system," in Proceedings of International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, pp. 1-5, 2017.

[3] K. S. Seethalakshmi, Usha B A and Sangeetha K N, "Security enhancement in image steganography using neural networks and visual cryptography," in Proceedings of International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, pp. 396-403, 2016.

[4] E. Gedkhaw, N. Soodtoetong and M. Ketcham, "The Performance of Cover Image Steganography for Hidden Information within Image File using Least Significant bit algorithm," in Proceedings of 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, pp.504-508, 2018.

[5] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," in Proceedings of 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, pp. 400-404, 2016.

[6] Y. Yiğit and M. Karabatak, "A Stenography Application for Hiding Student Information into an Image," in Proceedings of 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, pp. 1-4, 2019.

[7] A.AlWatyan, W. Mater, O. Almutairi, M. Almutairi, A. Al-Noori and S. Abed, "Security approach for LSB steganography-based FPGA implementation," in Proceedings of 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Sharjah, 2017.

[8] A.Arora, M. P. Singh, P. Thakral and N. Jarwal, "Image steganography using enhanced LSB substitution technique," in Proceedings of Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, pp. 386-389, 2016.

[9] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in Proceedings of IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, pp. 131-135, 2020.

[10] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in Proceedings of IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, pp.1-4, 2016.

[11] Stella D. Muyco and Alexander A. Hernandez, "A Modified Hash Based Least Significant Bits Algorithm for Steganography", In Proceedings of 4th International Conference on Big Data and Computing (ICBD). Association for Computing Machinery, New York, NY, USA, pp. 215–220, 2019.

[12] G. G. Rajput and Ramesh Chavan, "A Novel Approach for Image Steganography based on LSB Technique," In Proceedings of the International Conference on Compute and Data Analysis (ICCDA). Association for Computing Machinery, NY, USA, pp. 167–170, 2017.

[13] Antoniya Tasheva, Zhaneta Tasheva, and Plamen Nakov, "Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretchin,". In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech). Association for Computing Machinery, New York, NY, USA, pp. 233–240, 2017.

[14] Mark Rennel D. Molato and Bobby D. Gerardo, "Cover Image Selection Technique for Secured LSB-based Image Steganography," In Proceedings of the International Conference on Algorithms, Computing and Artificial Intelligence (ACAI). Association for Computing Machinery, New York, NY, USA, Article 17, pp, 1–6, 2018.

[15] S. Sugathan, "An improved LSB embedding technique for image steganography," in Proceedings of 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, pp. 609-612, 2016.

[16] Bhardwaj, R., & Sharma, V, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," Procedia Computer Science, vol. 93, pp. 832-838, 2016.

[17] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and securing message on edge areas of image using LSB steganography and OTP encryption," in Proceedings of 1st International Conference on Informatics and Computational Sciences (ICICoS), Semarang, pp. 1-6, 2017.

[18] M. C. Kasapbaşi., and W. Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check," Sādhanā, vol. 43, 2018.

[19] Jung, K, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," Journal of Real-Time Image Processing, vol.14, pp, 127–136, 2018.

[20] Gutub, A., and Al-Shaarani. F, "Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons," Arabian Journal for Science Engineering, vol. 45, pp. 2631–2644, 2020.

[21] A.Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[22] M. Rashid, M. W. Anwar, and A. M. Khan, "Towards the Tools Selection in Model Based System Engineering for Embedded Systems - A Systematic Literature Review," Journal of Systems and Software, vol. 106, pp.150-163, 2015.

[23] M. Rashid, M. Imran, A. R. Jafri, and Turki Al-Somani, "Flexible Architectures for Cryptographic Algorithms - A Systematic Literature Review," Journal of Circuits, Systems and Computers, vol. 28, no. 3, 2019.

[24] M. Imran, F. Bashir, A. R. Jafri, M. Rashid, and M. N. Islam, "A Systematic Review of Scalable Hardware Architectures for Pattern Matching in Network Security," Computers and Electrical Engineering, vol. 92, 107169, 2021.

[25] S. Sriram, B. Karthikeyan, V. Vaithiyanathan and M. M. Anishin Raj, "An approach of cryptography and steganography using rotor cipher for secure transmission," in Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, pp. 1-4, 2015.

[26] Begum, M. Baritha, and Y. Venkataramani. "LSB based audio steganography based on text compression<" Procedia Engineering, vol. 30 pp. 703-710, 2012.