SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Cover Selection in Steganography: A Systematic Literature Review

Taqiyuddin Anas[1], Farida Ridzuan[1,2,*], Sakinah Ali Pitchay[1,2]

[1] Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Malaysia
[2] Cybersecurity and Systems Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Malaysia

ARTICLE INFO

Article history:
Received 27 December 2023
Received in revised form 16 May 2024
Accepted 21 August 2024
Available online 20 September 2024

Keywords:
Cover Selection; Carrier Selection; Steganography; Systematic Literature Review

ABSTRACT

Steganography involves embedding a secret message within another message, image, or video. This practice obscures the message and ensures that only the intended receiver can read it. Generally, the cover quality significantly impacts the overall effectiveness of the steganography system. Nevertheless, limited audio steganography-related articles on cover selection analysis have been observed. Therefore, this systematic literature review (SLR) presented a comprehensive analysis of the steganography-based cover selection, including their contexts and contents. An extensive search for relevant articles was initially conducted in this SLR. Specific inclusion and exclusion criteria were employed to ensure that only relevant articles were selected. A total of 44 articles were then selected and analyzed to identify the parameters and evaluation metrics used in cover selection. Consequently, the analysis determined four primary categories containing the cover selection techniques: image, audio, text, and video-based cover selections. Several factors influencing the cover selection were also identified based on the articles, such as parameters used in different mediums, standard evaluation metrics on each medium, and correlation between metrics performance and parameters. These findings indicated that the frequently utilized parameters were message and cover sizes. The imperceptibility [Peak-Signal-Noise-Ratio (PSNR) and Signal-Noise-Ratio (SNR)] was also the highest evaluation metric used in determining the effectiveness of the cover selection technique. Overall, this SLR served as a valuable resource for steganography researchers, bridging the gap between two research fields [machine learning (ML) and steganography]. A clear direction could be provided to future researchers through advanced analysis using this SLR to improve ML-related cover selection methods.

1. Introduction

Steganography implies concealing information in a way that is not easily detectable. This technique enables the concealment of a message, image, or file within another message, image, or file, rendering the hidden information challenging to detect. The term "steganography" is derived from the Greek words "steganos" (covered or concealed) and "graphein" (to write) [1]. Historically, steganography has been employed for several reasons, including military and political communications. During ancient times, individuals concealed messages using wax tablets, invisible

* *Corresponding author.*
E-mail address: farida@usim.edu.my

https://doi.org/10.37934/araset.52.2.107129

ink, and tattoos. Meanwhile, steganography has frequently been employed in the digital era to hide sensitive information from unauthorized individuals, such as financial data or trade secrets.

Digital media (images, audio, and video files) are the predominant means of concealing hidden messages, which are commonly known as covers. Nonetheless, each cover of a medium applies a slightly different method of encoding messages. Text-based steganography involves encoding hidden messages by modifying word choices or sentence structures. Image steganography can be achieved through pixel value modifications or in the frequency domain to enable data embedding. Likewise, audio steganography involves manipulating audio signals for discreet message transmission, while video steganography utilizes temporal redundancies or frame modifications for concealed information. These steganography types demonstrate several methods of embedding information into different mediums. Each technique is evaluated using specific metrics tailored to the nature of the cover type.

The characteristics of cover samples necessitate consideration for producing an efficient cover selection. Therefore, attaining equilibrium between these characteristics is essential. The interdependencies between the capacity, robustness, imperceptibility, and dynamic security of the embedded cover should be well-balanced to generate an effective cover selection mechanism [2]. Typically, capacity is denoted as the steganographic characteristic to embed and store hidden messages. Meanwhile, robustness pertains to the ability of the method to withstand modifications without compromising the secret data. Imperceptibility is also the degree to which the changes made through steganography remain undetectable to human perception. Finally, security describes how the embedding approach can spread the secret data throughout the cover audio to prevent statistical or visual attacks under any circumstance [2, 3].

Numerous factors affect the cover selection choice in steganography, such as the medium, the size and type of the hidden message, and the required security level. Hence, text-based steganography is appropriate for small and simple messages that can be embedded in the white spaces of a document or email. Likewise, image-based steganography is better for larger and more complex messages [4]. Although these studies have demonstrated their significant outcomes, limited studies regarding cover selection analysis have been observed. This systematic literature review (SLR) comprehensively analyzed the articles concerning cover selection in steganography, in which their contexts and contents were examined. Consequently, this SLR could be applied as a steganography-based reference while bridging the gap between two research fields [machine learning (ML) and steganography]. The contents of this SLR are structured as follows: Section 2 presents the background and motivation; Section 3 highlights the methodology used; Section 4 provides the results and discussion; Section 5 concludes this SLR.

2. Background and Motivation

The cover selection process in steganography entails selecting suitable covers for hiding a message. An appropriate cover selection containing the least detectable stego output is necessary to ensure the security of covert communication [5]. Even though previous steganography-related articles by Majeed *et al.,* [6], Vimal [7], and Subhedar and Mankar [8] focused on the embedding approach, the cover selection method was disregarded. Thus, this SLR improved the comprehension of steganography-based cover selection methods, providing a comprehensive analysis of these articles concerning cover selection. Table 1 tabulates the research questions (RQs) used in this SLR. The RQ1 addresses the overall perspective of research trends on cover selection in steganography, in which the number of articles between 2010 and 2023 are identified. Subsequently, RQ2 extracts

the parameters utilized in previous articles to discover the most common parameters. Finally, RQ3 assesses the evaluation metrics commonly used in steganography-based articles.

Table 1
Research questions in SLR

RQ#	Research question
RQ1	What is the current landscape of steganography-based cover selection methods in previous articles?
RQ2	What parameters are used for the steganography-based cover selection methods in previous articles?
RQ3	How are the steganography-based cover selection methods in previous articles evaluated?

Figure 1 illustrates the stego output production across different mediums using the steganographic process. Most articles have incorporated the cover selection process into their review, which is pivotal for the effectiveness and security of steganographic techniques. The review process of these articles has focused only on one specific medium throughout the steganography process [9]. Therefore, this SLR specifically examined the selection process across different mediums. Four categories were applied to classify the covers in this SLR: image, audio, text, and video.

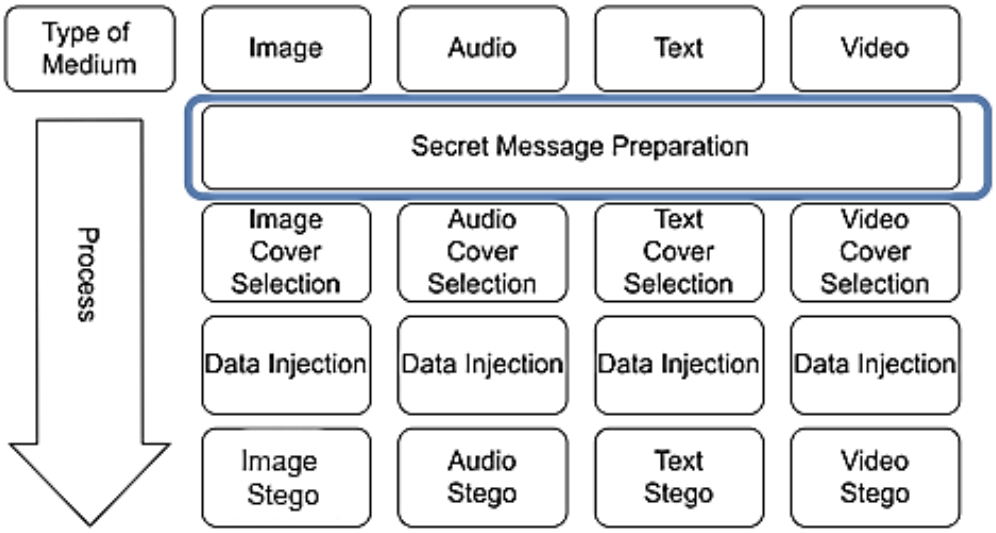

Fig. 1. The stego output production process across different mediums using the steganographic approach

3. Methodology

The methodology employed in this SLR involving numerous steps (SLR, data collection, method analysis, relation construction between metrics and parameters, and evaluation metric extractions) was based on the approach proposed by AlSabhany *et al.,* [5]. Initially, this methodology addressed the first research objective regarding the current state of steganography-based cover selection. Figure 2 depicts the data collection process using this methodology, in which a structured approach is applied for the data collection process to ensure the inclusion of relevant academic articles. A comprehensive search query used different key terms in this SLR: cover selection, optimization, and carrier selection. This procedure also included the steganography keyword to refine the search process. Overall, four reputable digital databases were used for the query execution: ScienceDirect, ProQuest, Springer, and Scopus.

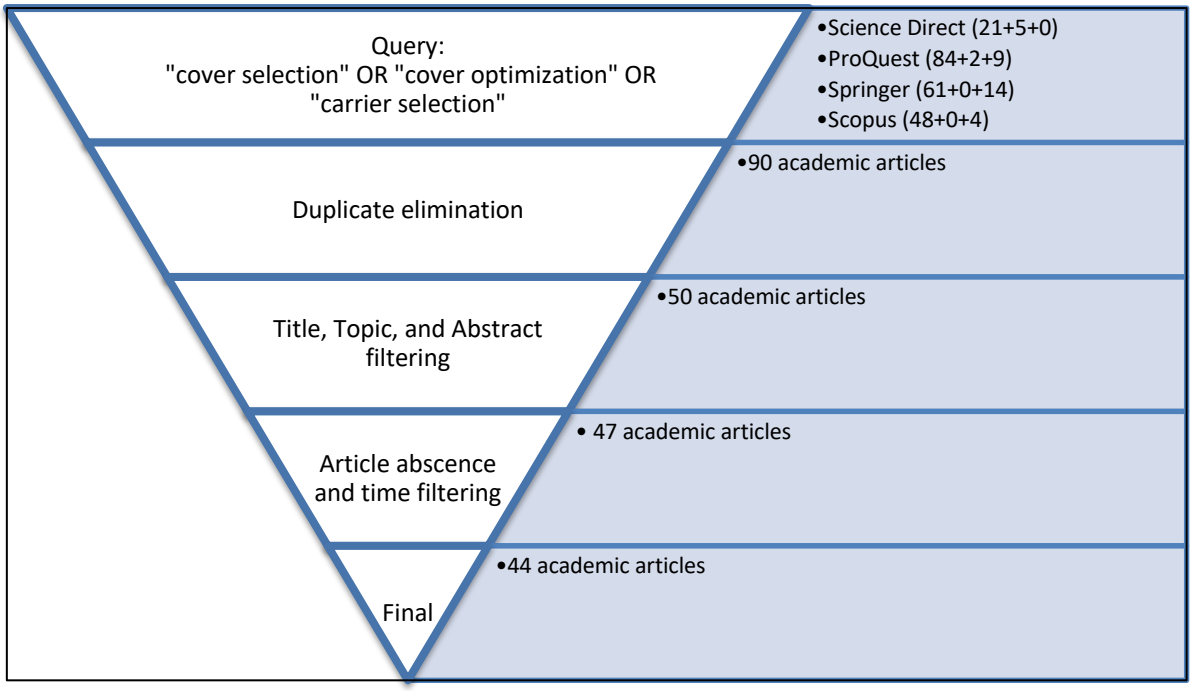

Fig. 2. The filtration process regarding the number of duplicated academic articles to be reviewed

Each database generated a significant number of articles for the initial search process: 21 (ScienceDirect), 84 (ProQuest), 61 (Springer), and 48 (Scopus). Conversely, duplicated articles present in multiple databases were eliminated. A filtering process was also implemented to evaluate the relevance of articles using several aspects: title, topic, and abstract. Only articles on the research topic were retained. Further refining was then conducted to exclude articles that did not fulfill the research criteria or were published before 2010. This process ensured that only the most recent and relevant articles were emphasized. Table 2 lists the requirements for the filtering process. A total of 44 articles were selected to be reviewed and analyzed based on the inclusion and exclusion criteria. The cover type was also classified into four categories: text, video, audio, and image-based covers. A comprehensive list of all the reviewed articles is listed in Table 3 for image, Table 4 for audio, Table 5 for text, and Table 6 for video.

Table 2
Summary of the criteria for the filtering process

Criteria	Inclusion	Exclusion
Type of Article	Journal and conference proceeding	Other sources (e.g., PowerPoint slides, thesis, and patent).
Article Contribution and Relevancy	Clear contribution and high relevancy to Cover Selection Techniques	Irrelevant to the research topic
Publication Year	2010-2023	Published before 2010
Language	English	Non-English
Article Availability	Available on the public domain	Unavailable for download

Table 3
List of reviewed articles for image cover

Author	Cover details	Technique	Parameters	Evaluation Metrics	Result			
					C	R	I	S
Sajedi & Jamzad [13]	512 × 512 Grayscale Joint Photographic Experts Group (JPEG)	Pre-processing stage before applying steganography methods	Cover image payloads	Embedding capacity, Embedding complexity			√	
Sajedi & Jamzad [18]	512 × 512 Grayscale	Extracts signature of cover images against stego images, then apply fuzzy rules and Evolution Algo	Cover image signature	Peak Signal-Noise-Ratio (PSNR)			√	
Sun & Liu [43]	614 × 418 Grayscale Tag Image File(TIF)	Cover selection method based on correlation coefficient	Cover correlation value	Spread Spectrum Image Steganography (SSIS), LSB matching			√	
Sajedi & Jamzad [19]	512x512	adaptive contourlet-based steganography	Embedding rate (by researcher) Coefficient value	PSNR Coefficient histogram	√		√	
Abbadi [20]	640x480 Grayscale	Cover weight features determined by using Analytic Hierarchy Process (AHP)	Entropy Capacity Mean Variance Histogram Energy Robustness Expected Secrecy	Similarity Security PSNR			√	
Nazari & Moin [16]	512 × 512 Grayscale JPEG	Run the length matrix and texture feature of images to choose a cover	Image feature [Short Run Emphasis (SRE), Long Run Emphasis (LRE), Gray Level Non Uniformity (GLNU), Run Length Non-Uniformity (RLN)]	Structural Similarity Measurement (SSIM)	√			
Subhedar & Mankar [21]	[Lena, Mandrill, House Tiffany, Boat] Grayscale	Using contrast measurement, a cover is chosen, and contourlet subbands are embedded.	Cover image contrast	Root Mean Square Error (RMSE), PSNR, Mean SSIM	√			
Yuan & Chen [44]	512 × 512 Grayscale	Spatial image cover selection using prior knowledge of image embedding suitability, which is the inverse of embedding distortion under	Payload size, Image embedding, suitability	Capacity size			√	

		constraints of empirical security and payload					
Jalili *et al.,* [45]	512 × 512 Grayscale	Run the length matrix and texture feature of images to choose a cover	Gray-Level Run Length(LRL) Matrix of cover	N/A	√	√	
Amin Seyyedi & Ivanov [22]	512 × 512 Grayscale Portable gray map (PGM)	Unsupervised image classification based on edge and texture features of an image	Cover image content	PSNR, Mean Square Error (MSE), Kullback-Leibler (KL) divergence,		√	
Bin Li *et al.,* [14]	512 × 512 Grayscale	Clustering modification direction (CMD)	Neighboring pixel	Time execution (All other most for steganalysis)		√	
Wu *et al.,* [46[	512 × 512 Grayscale	A new measure for hiding the ability of the cover image based on the Fisher Information Matrix and Gaussian Mixture Model	Cover Quality Factor (QF)	N/A (only have steganalysis metric)	√	√	
Sedighi *et al.,* [1]	512 × 512	Locally estimated multivariate Gaussian cover image model	Pixel variance, payload	Security (Steganalysis)	√		
Hajduk & Levicky [47]	512 × 512 Color BMP	Cover image database pre-process and comparison of secret message and appropriate cover image area	Database of pre-process image	Time execution Number of changes Diff changes % Diff changes		√	
Umamaheswari & Sumathi [23]	64 × 64 Color	Difference between the secret message value and the green Pixel Value Difference (PVD) of the image	Pixel difference threshold value	PSNR MSE		√	
Evsutin *et al.,* [15]	756 × 504 JPEG	Cover selection based on the application of the principles of optimality	Compression complexity blockiness heterogeneity deviation	PSNR		√	
Molato & Gerardo [24]	600 × 450 Color	Proposed skewness and kurtosis for cover image suitability	Skewness Kurtosis	PSNR SSIM		√	
Hajduk & Levicky [25]	512 × 512 Color BMP	Intra-image scanning in the database for comparative calculations	Message size Number of changes	PSNR Time execution			√
Subhedar & Mankar [26]	512 × 512 Grayscale JPEG	Curvelet-based image steganography	Message size	PSNR , Mean structural similarity index (MSSIM),		√	√

				Normalized Correlation Coefficient (NCC), Avg Dif (AD), Max Dif (MD), Bit error rate (BER), Correlation Quality (CQ), Normalized Absolute Error (NAE), Quality Factor (QF)			
Wang *et al.,* [50]	512 × 512 Grayscale	Batch steganography, which combines cover selection and payload allocation by steganographic distortion optimization	Message size	N/A		√	
Abed *et al.,* [10]	512 × 512 Grayscale	Global-level filtered and block-level analysis	Pixel intensity entropy histogram	PSNR MSE		√	
Wang & Zhang [51]	512 × 512 Grayscale	Secure image and individual level by restraining MMD distance and searching the minimal steganographic distortion images	Maximum Mean Discrepancy (MMD) threshold	N/A		√	
Ren *et al.,* [12]	2048 × 2048 Jpeg		Pixel pair, Correlation coefficient	QF, Time execution, Testing error			√
Shah & Bichkar [27]	256 × 256 Grayscale	GA will choose the cover image depending on the characteristics of the secret data.	Message Characteristic in Image	PSNR MSE		√	
Wang *et al.,* [52]	512 × 512 Grayscale	The cover selection method considers processing distortion and embedding distortion.	Image total distortion	N/A		√	
Zhong *et al.,* [48]	512 × 512	Generative Network with entropy loss and steganalysis loss	Payload allocation, distortion evaluation	steganography quality called LossS			√
Subhedar [17]	512 × 512 Color	Optimal cover selection from image database based on statistical texture analysis.	Gray values, heterogeneity content	PSNR, MSSIM, Universal Image Quality Index (UQI), Normalized Cross-Correlation (NC), Image Fidelity (IF)	√	√	

Hamid *et al.,* [49]	256 × 256 Color	CNN-based to select images after the process of embedding.	Quality compression complexity lowest levels of blocking, heterogeneity, deviation	SSIM F1 Score Recall Precision (ML)		√	
Wang *et al.,* [11]	512 × 512 Grayscale JPEG	Cover selection method to joint image similarity and embedding distortion	Singular Value Decomposition (SVD) of each image payload	Time execution			
Chen *et al,.* [53]	256 × 256 Color	Cover Selection Algorithm of color images based on Hybrid Local Texture Descriptor (HLTD)	Intra-channel Local Binary Pattern (LBP) for color image Green channel	Error rate Deviation			√

*C: Capacity, R: Robustness, I: Imperceptibility, S: Security

Table 4
List of reviewed articles for audio cover

Author	Cover details	Technique	Parameters	Evaluation Metrics	Result		
					C	R	I
Kekre *et al.,* [3]	44.1 kiloHertz (kHz)	Considering MSB for larger LSB	Cover Most Significant Bit (MSB) (either 1 MSB or 2 MSB)	MSE PSNR SNR			√
Ali *et al.,* [28]	512 × 512 Grayscale JPEG	Cover selection method to joint image similarity and embedding distortion	Cover size to message size ratio bits for each iteration code.	Objective Listening SNR Hiding Capacity Normal Correction	√		√
Nasrullah *et al.,* [31]	44.1 Khz, 22.0 4kHz, 11 kHz 16 bps	Embed carious size message in cover by increasing capacity and SNR	Message size, Cover size, Signal-Noise-Ratio (SNR)	Avg segmental SNR N of failing samples Czekanowski distance (CZD)	√		
Noor Azam *et al.,* [2]	44.1 kHz 16bps	Multi-Objective Evolutionary Algorithm (MOEA) using Non-dominated Sorting Genetic Algorithm (NSGA-II) with adaptive Least Significant Byte (LSB)	Audio bit-per-second (bps), Database solution [audioindex, bps]	SNR Sample difference	√	√	√
Zhang *et al.*, [54]	44.1 kHz	Complexity indicator to characterize the complexity of the audio	Original audio residuals convoluted audio	Histogram C values (complex values)			√

*C: Capacity, R: Robustness, I: Imperceptibility

Table 5
List of reviewed articles for text cover

Author	Cover details	Technique	Parameters	Evaluation Metrics	Result		
					C	R	I
Zhang *et al.*, [37]	Declaration of Independence (secret message) 10,731,668 post crawled	High-capacity behavioral steganography method on social networks based on carrier selection with timestamp modulation.	Behavior delays Time sequence	Bit per words Embed capacity	√		
Shniperov & Nikitina [36]	Markov chain text pattern	Texts with a good approximation to the natural language model	Message size	Capacity	√		
Luo & Huang [34]	Neural-based poetry generation for cover medium	A template-constrained generation method and develop a word-choosing approach using inner-word mutual information	Quatrain lines	Naturalness embedding	√		
El Rahman [35]	Document letter as the cover medium	Using adaptive embedding upon	Word length White space	Jaro-Winklermetric	√	√	

*C: Capacity, R: Robustness, I: Imperceptibility

Table 6
List of reviewed articles for video cover

Author	Cover details	Technique	Parameters	Evaluation Metrics	Result		
					C	R	I
Wang *et al.,* [41]	23 YUV. YUV stands for (Y) luma, or brightness, (U) blue projection and (V) red projection.	Features of High Efficiency Video Coding (HEVC) used for cover selection	Embedding rate, Capacity of current Coding Unit (CU)	Bjotegaard Delta Bitrate (BD-BR), BD-SSIM, Intra-Prediction Mode (IPM) Calibration, Accuracy Rate (AR)	√		
Dasgupta *et al.,* [40]	320 × 320 107–450 frames	Using Genetic Algorithm (GA) for optimal imperceptibility	Imperceptibility and video quality	PSNR, IF, MSE, Time Complexity analysis, Space Complexity analysis			√
Cao *et al.,* [42]	H264 Advance Video Coding in raster graphic file (YUV) format	Video steganography by intra-prediction and matrix coding	Two different blocks. intra-macroblock	Peak Signal Noise Ratio (PSNR) Accuracy Rate (AR)	√		√

*C: Capacity, R: Robustness, I: Imperceptibility

4. Results

This section presents a comprehensive landscape analysis for steganography-based cover selection techniques, encompassing a timeframe from 2010 to 2023 involving 44 articles. Figure 3 portrays the chronological distribution of published articles across four categories: image, audio, text, and video. These categories were defined based on the medium used for concealing the data. Consequently, the articles on image cover selection were recorded over 13 years (2010 to 2023). This outcome was consistent with the high number of image steganography-related articles [5]. In contrast, only one video-based cover selection was reported, as it is the most recently explored domain. Most articles focused on steganography techniques rather than cover selection, resulting in the inadequate identification of other specific trends.

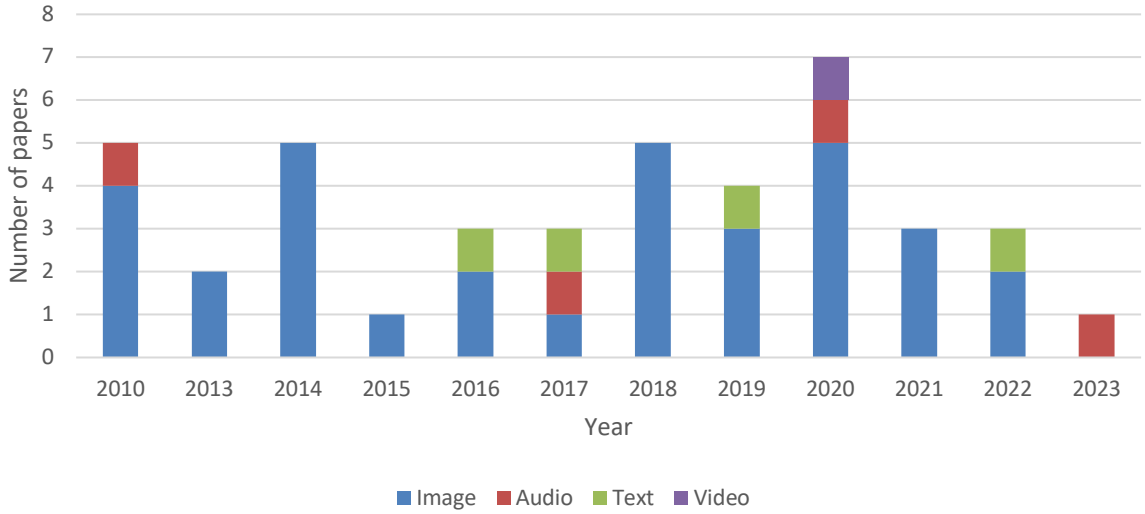

Fig. 3. The number of publications from 2010 to 2023

Figure 4 displays the cover medium distribution used in the selected articles. Among the 44 examined academic articles on cover selection, most research presented the usage of images. This observation was followed by audio, text, and video. The following process investigates the parameters used in the cover selection method corresponding to the cover types.

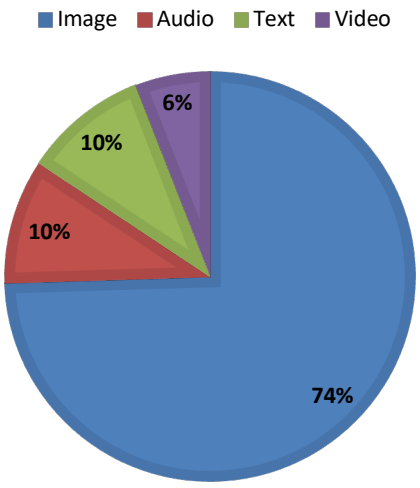

Fig. 4. The cover medium distribution

4.1 Image Medium

The image cover was the most significant and extensively researched cover type in steganography-based cover selection. The selection of cover images was frequently based on their pixel size, which directly influenced the capacity and perceptual impact of the steganographic process. Figure 5 depicts the distribution of cover image resolution, ranging from squared 256 px to 2048 px. The most prevalent pixel size for cover images was 512 px × 512 px, which was primarily used to achieve higher capacity [9]. Larger images were also advantageous due to their increased embedding capacity for concealing large data amounts. This finding contributed to the availability of numerous image datasets (such as BOSSBase), facilitating extensive experimentation and research in this field [10, 11]. Nonetheless, high-resolution images produced increased computational expenses, thus impeding the efficiency of data embedding and retrieval processes [12].

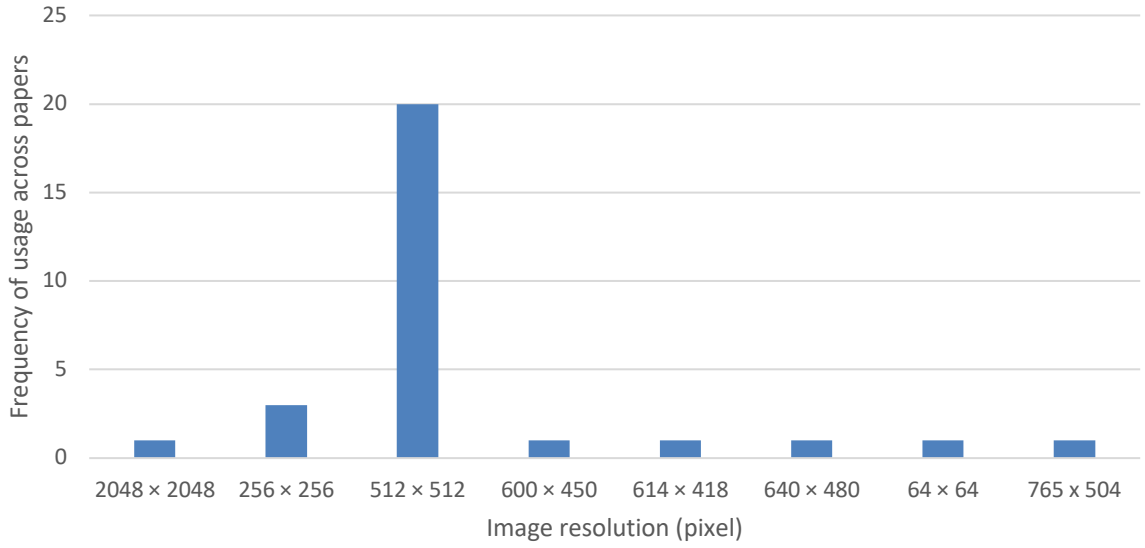

Fig. 5. The cover image resolution distribution used for cover selection

Most image cover selection-based articles mainly relied on the Joint Photographic Experts Group (JPEG) format [8, 11-16]. JPEG is a prevalent image compression technology renowned for its effectiveness in lowering file sizes while maintaining reasonable image quality. This format is often selected due to the well-balanced benefits between capacity and imperceptibility. The inherent lossy compression of this method introduced a certain distortion level, which aided in concealing embedded data. Thus, this technology was less likely to be detected by casual observers. On the contrary, specific articles selected grayscale cover images instead of color (RGB). This decision was taken to retain experimental consistency and control. Given that grayscale images contained only grey shades and no color information, researchers could simplify their experiments by eliminating color-related variables [13].

Figure 6 illustrates the frequency of parameters of the selected articles to determine a good cover image. The comprehensive list of image cover parameters is in the Appendix section due to its extensive length (see Appendix). The primary parameters for determining a good cover image were a cover image, message size, and cover blockiness heterogeneity. These parameters directly impacted the success of the steganographic process by affecting the concealed content within the overall visual context. The message size parameter was crucial in defining the capacity of the steganographic approach. Thus, balancing the message size with cover image characteristics was

necessary for achieving optimal data embedding without compromising the perceptual quality of the cover image. The cover blockiness heterogeneity was also a significant parameter, particularly in segmentation methods dividing the cover image into blocks for embedding data. Therefore, high blockiness heterogeneity allowed for strategically identifying places with unique textures or color patterns. Nevertheless, low heterogeneity suggested that the material was more consistent and required careful deliberation when selecting appropriate areas for hidden information [17].

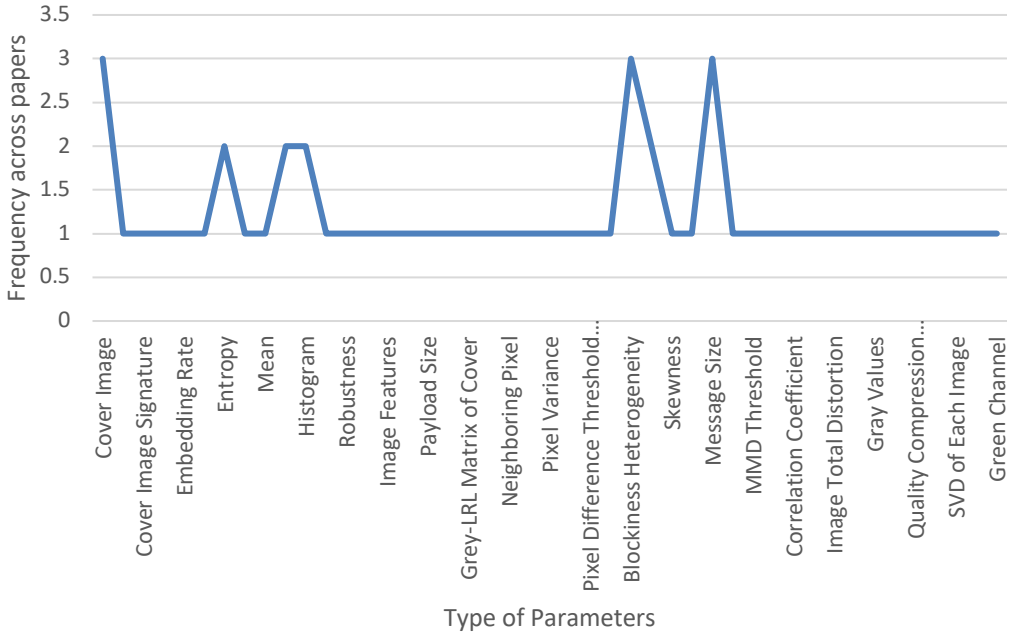

Fig. 6. The distribution of different parameters for image cover selection

This SLR determined the evaluation metrics employed in image cover selection-based articles (besides extracting parameters). Figure 7 illustrates the various metrics used to assess the cover selection output. The Peak-Signal-Noise Ratio (PSNR) was the dominant metric for evaluating image medium. Consequently, researchers applied PSNR as a benchmark to assess the effectiveness of their image cover selection approaches in maintaining image quality. When the results were compared to the PSNR of the original image, the distortion level caused by the embedding process was determined. Thus, PSNR was chosen as a reference metric for image mediums in this SLR. Table 7 summarizes the research articles involving the parameters used and their corresponding PSNR values.

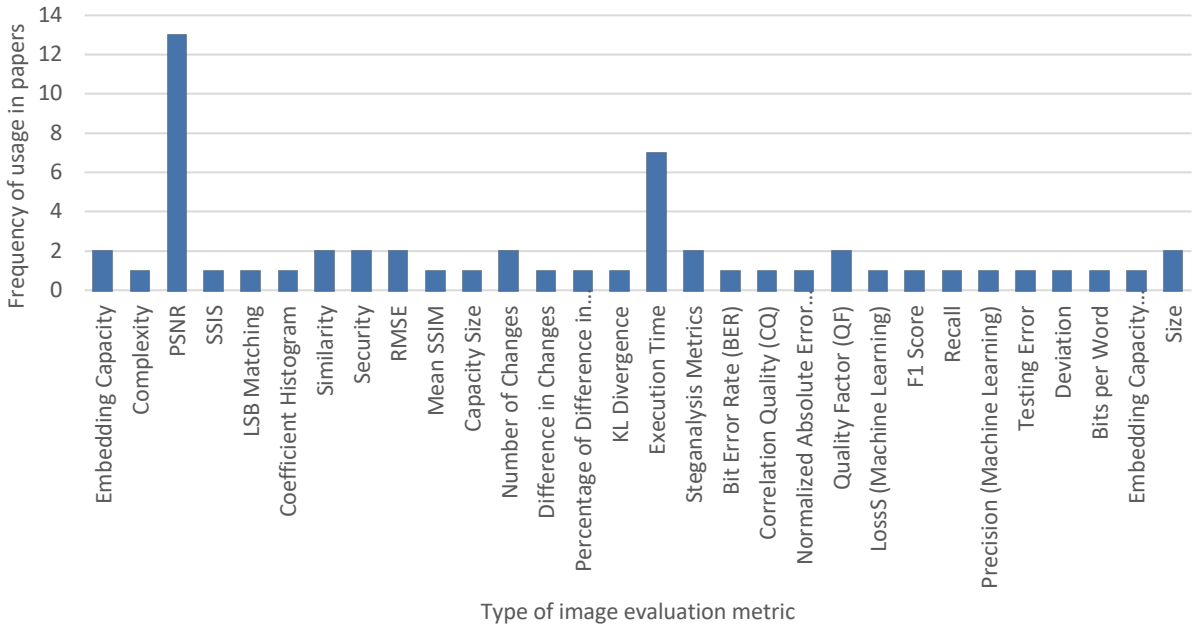

Fig. 7. The distribution of image evaluation metric in image medium cover selection

Table 7
Summary of existing research articles with parameters used and their average PSNR values

Author	Parameters	Mean of PSNR values (dB)
Sajedi & Jamzad [18]	• Cover Image • Signature	43.00
Sajedi & Jamzad [19]	• Embedding Rate • Coefficient Value	38.00
El Abbadi [20]	• Entropy • Capacity • Mean • Variance • Histogram • Energy • Robustness • Expected Secrecy	34.00
Subhedar & Mankar [21]	• Cover Image , Contrast	43.00
Amin Seyyedi & Ivanov [22]	• Cover Image Content	42.36
Umamaheswari & Sumathi [23]	• Pixel Difference Threshold Value	35.02
Evsutin *et al.,* [15]	• Compression Complexity • Blockiness Heterogeneity • Deviation	45.37
Molato & Gerardo [24]	• Cover Skewness • Cover Kurtosis	48.46
Hajduk & Levicky [25]	• Message Size • Number of Changes	54.6
Subhedar & Mankar [26]	• Message Size	50.24
Abed *et al.,* [8]	• Pixel Intensity • Entropy • Histogram	48.00
Shah & Bichkar [27]	• Message Characteristic	51.14
Subhedar [17]	• Gray Values • Blockiness Heterogeneity	54.55

The higher PSNR value implied superior signal quality due to the PSNR calculation measuring the distortion of the image after the secret message was embedded. A study by Subhedar [17] documented two prominent PSNR values considering gray values and blockiness heterogeneity as parameters. Similarly, Hajduk and Levicky [25] considered message size and number of changes as parameters. The number of modifications utilized as parameters served a function comparable to the PSNR measure, which was employed to quantify the distortion level in the stego output image. Thus, a good stego output image should consider cover image blockiness heterogeneity, secret message size, and cover size. Gray values should also be considered if the grayscale image was used as the cover.

4.2 Audio Medium

Limited academic articles regarding the audio cover selection were observed compared to the image cover. This outcome was attributed to steganography initially focused on digital images, whereas audio research began later [28]. Nonetheless, audio-based carrier mediums enabled the hiding of significant amounts of data due to their greater capacity [29]. The imperceptible modification of audio signals also guaranteed the preservation of the original characteristics of the host message [30]. Therefore, these factors contributed to the effectiveness of audio steganography in protecting privacy and enhancing data security. Figure 8 displays the audio frequency distribution for the audio cover selection, which presents the ability of steganographic techniques to adjust to different audio frequencies when choosing a cover. Typically, a higher Hertz value indicates a greater capacity for coverage. As such, audio-based cover selection should consider audio frequency due to its influence on the capacity and imperceptibility of the hidden message. Trade-offs also existed between imperceptibility and capacity, capacity and robustness, and imperceptibility and robustness [2]. These factors required balancing when designing steganographic systems that were efficient and adaptable.

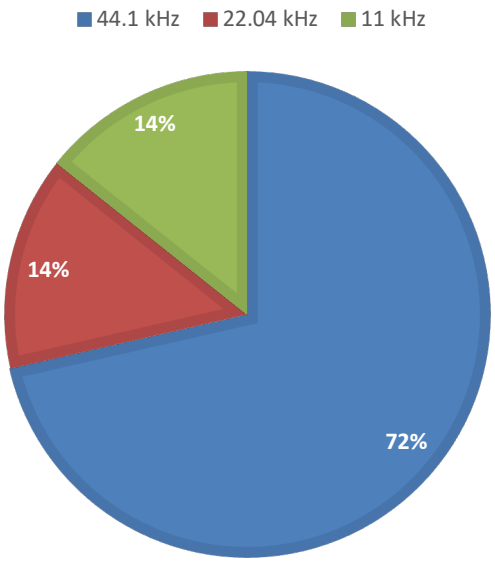

Fig. 8. The distribution of audio frequency used for the audio cover selection

Figure 9 depicts the audio cover parameters employed in previous articles. The audio cover parameter could be classified into two distinct categories: subject and object features. Subject parameters were the hidden message-related parameters, while object parameters were the audio

cover. The subject parameter remained fixed, which is the message size, while object parameter varied such as audio size, audio bps, and many more. Therefore, the capacity of the cover should be considered when deciding on a suitable message size (two factors were interconnected). The cover size parameter was the most common object parameter used in determining and selecting a cover for a secret message [2, 3, 28, 31]. The cover size of the audio was also considered to produce an excellent audio capacity of audio stego.

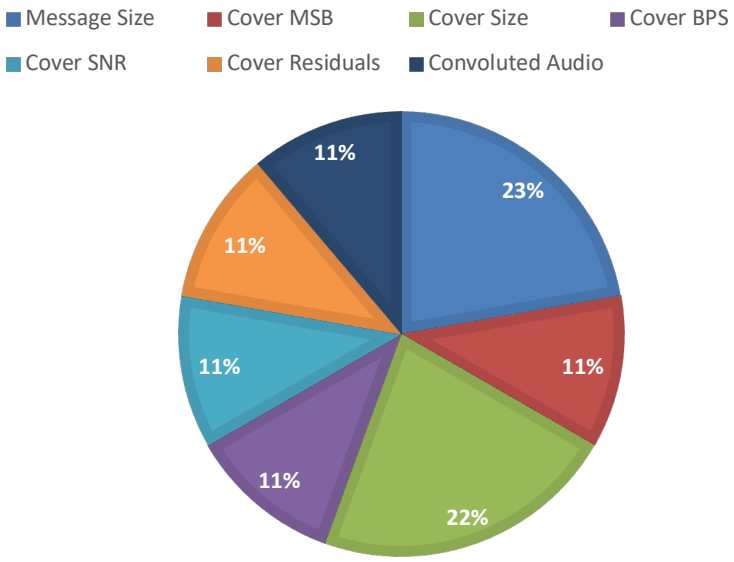

Fig. 9. The distribution of parameters of audio cover selection

The cover size should be considered when working with audio steganography to maximize the audio capacity during the steganographic processes [3]. Considering the significant cover size, the embedded data could be directly affected. Thus, increasing the cover size allowed for more substantial space to conceal the hidden message, which improved the steganographic capacity of the audio medium. Overall, the cover size was vital in determining the efficiency and effectiveness of audio steganography, rendering it the most used parameter that required careful consideration. The parameter solution [audioindex, bps] could also address the feature dependency while navigating the cover size parameter [2]. This parameter enabled precise identification of the index or position within the audio dataset. Simultaneously, the effective embedding rate (bits per second) could be determined.

The evaluation metrics used in audio cover selection-based articles were identified. Two broad categories were applied for these metrics: calculating and non-calculating metrics. Figure 10 presents the metric distributions of steganography-based audio cover selection. The metric calculations involved quantitative measurements to assess specific aspects of a system or process. These metrics utilized mathematical calculations or algorithms to generate numerical values that provided insights into the performance, quality, or characteristics of the experiments. Table 8 tabulates a few components of the calculating metrics in this SLR. Alternatively, non-calculating metrics were qualitative or subjective measurements used to assess various attributes of a system or process. Compared to calculating metrics, non-calculating metrics did not involve mathematical computations to derive numerical values but used human perception and observations. The non-calculating metrics for audio cover selection are listed as follows

I. Listening Test
II. Objective Test

Previous articles on cover selection denoted that PSNR was the most common metric used to measure the imperceptibility of a stego output file in an audio medium [2, 3, 28, 31]. Therefore, previous articles established a new correlation between the number of parameters and SNR (see Table 9).

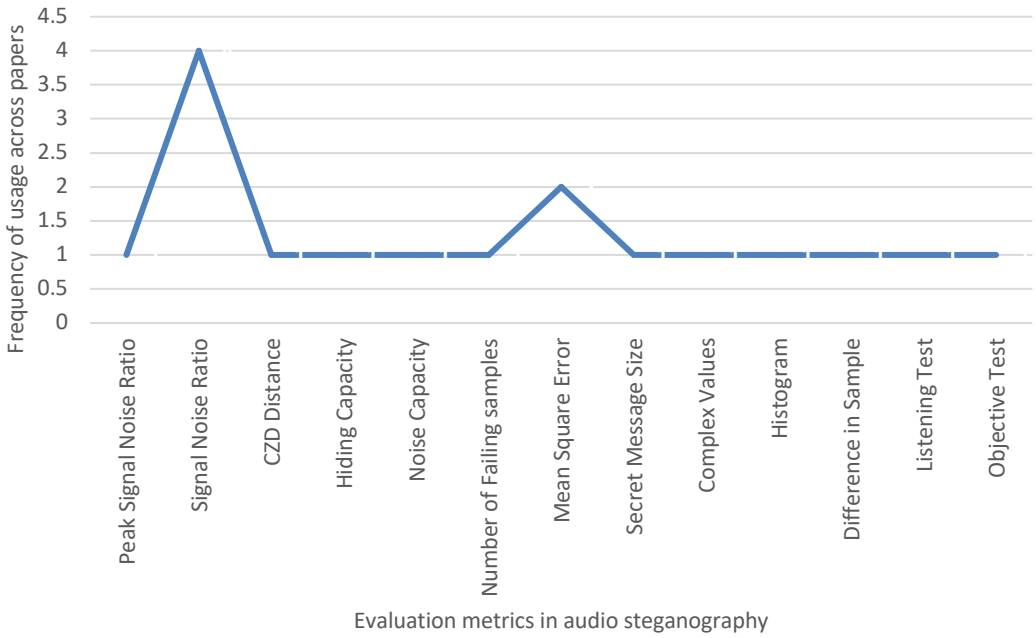

Fig. 10. The distribution of evaluation metrics used in audio steganography cover selection

Table 8
Summary of definition for audio evaluation metrics and its description

Definition	Description
Signal Noise Ratio	Measures the ratio of signal strength to noise
Peak Signal Noise Ratio	Evaluates the peak signal-to-noise ratio for signal quality assessment
CZD Distance	Quantifies the Czekanowski Distance
Hiding Capacity	Determines the maximum capacity for data hiding
Noise Capacity	Measures the capacity for embedding data within noise
Number of Failing samples	Counts instances of samples failing a specific criterion
Mean Square Error	Calculates the mean squared difference between original and distorted data
Difference in Sample	Evaluates the disparity between sample values

Table 9 represents a collection of research articles using specific parameters in their steganographic processes. These processes were integrated with their corresponding mean Signal-to-Noise Ratio (SNR) values. The SNR is a critical metric for assessing the perceptual quality of steganographic results, in which higher SNR values imply superior quality and imperceptibility. Noor Azam *et al.,* [2] evaluated four parameters and obtained the highest mean SNR value of 75.36 dB. The study suggested exceptional imperceptibility. On the contrary, Kekre *et al.,* [3] documented a single parameter, which produced a competitive but slightly lower mean SNR value of 49.89 dB.

Typically, audio steganography relies on the "audio bps" (bits per second) to determine the capacity of the stego output. The "number of covers" denotes the cover variety, while "message size" determines the content and capacity. Furthermore, the "solution" [(audioindex, bps)] allows fine-tuning to balance capacity and audio quality. These parameters enhanced the ability of the steganographic algorithm to make well-informed decisions on cover choices, optimizing steganography results. Consequently, these findings demonstrated the significance of

comprehensive parameter selection and analysis in steganography. The imperceptibility of the hidden information was improved when several factors were included, thus highlighting the crucial role of parameter choice in steganographic practices.

Table 9
Summary of previous studies with their corresponding parameters and SNR values

Author	Parameters	Mean of SNR (dB)
Nasrullah *et al.,* [31]	• Message size • Cover size • Cover SNR	49.25
Ali *et al.,* [28]	• Message size • Cover size • All cover size	54.10
Kekre *et al.,* [3]	• Most Significant Bit (MSB) of the data (either 1MSB or 2MSB)	49.89
Noor Azam *et al.,* [2]	• Number of covers • Message size • Audio bps • Solution [audioindex, bps]	75.36

4.3 Text Medium

Text medium can embed secret messages within the text, rendering them imperceptible to human visual perception [32]. Given that Indian and Chinese languages possess feature-codable characters and flexible grammar structures, this approach effectively enhances the concealment of the messages [33, 34]. The secret message is generally chosen as the subject, while the cover medium is selected as the object. In contrast, the approach to text medium is different [33-37]. A text-based medium involves selecting covers that slightly differ from other media forms. This difference results from the hidden message functioning as the object at certain times, while the text covers serve as the pre-existing subject. In some instances, the primary information to be concealed is the secret message (object), and the text covers (subject) are generated in advance to facilitate the hiding of the message. Hence, distinctive methods for concealing information are introduced based on the adaptive embedding of the generated covers.

Several distinct methods of adaptive embedding are observed on a generated cover as follows

I. Markov chain text pattern generated cover [36]: This method leveraged Markov chain text patterns to create the cover text closely approximating natural language patterns. Therefore, utilizing natural language in steganography improved the undetectability of the hidden content. The cover selection process was primarily based on the ability of the technique to accommodate the desired message size, ensuring that the hidden message could be effectively embedded within the cover text. An essential benefit of this method involved its high capacity, suggesting that substantial messages could be effectively hidden while preserving the cover text quality.

II. Neural-based poetry generated cover [34]: This distinct method comprised poems created using neural-based techniques. The strategy centered on secret information within quatrain lines of the generated poetry, highlighting the structured and rhythmic nature of quatrain verses. This method applied naturalness as an important metric, signifying the close resemblance of the generated poetry to the genuine poetry while contributing to the imperceptibility of the embedded information. The approach was mainly acknowledged for its high embedding rate, signifying its capacity to hide significant data within the poetry. Thus, this method was suitable for high-capacity steganography.

III. Document letter generated cover: A study by El Rahman [35] investigated document letters as a steganography-based cover medium. The study utilized a word length and white space-based approach to embed secret information within these letters. Consequently, this process was suitable for text-based steganography using evaluation metrics based on preservation, robustness, and capacity improvement.

IV. Social media post as cover: A study by Zhang *et al.,* [37] involved systematically collecting a large volume of social media postings (10,731,668 posts) to serve as the cover text, emphasizing the scale of the cover medium. Zhang *et al.,* [37] achieved high capacity in behavioral steganography, indicating its ability to conceal a substantial message proficiently within social media posts. A carrier selection with timestamp modulation was employed, contributing to the effectiveness of the steganographic process. Therefore, this technique was recognized for its higher capacity, signifying its capability to hide significant information within the cover text.

Table 10 summarizes the evaluation metrics used for text steganography. Each technique offered distinct methods for assessing the quality of the stego output. Interestingly, no common metrics were observed measuring the effectiveness of the processes. Compared to other steganography types (image or audio) involving common metrics (PSNR or SNR) for consistent evaluation, text steganography demonstrated an insufficient universal set of metrics due to its diverse approaches.

Table 10
Summary of definition for text steganography evaluation metrics and its description

Definition	Description
Bit per Words (BPW)	Measures steganographic efficiency by calculating the average bits needed to hide one unit of linguistic information
Embed Capacity	Measures the maximum hidden message that can be concealed within a cover medium
Naturalness	Assesses how closely the Artificial Intelligence (AI)-generated cover is to the human-generated cover
Jaro-Winkler Metric	Measures the similarity between two strings using the Jaro-Winkler distance

4.4 Video Medium

The popularity of video steganography is increasing due to its effective embedding of a significant amount of information and its robustness, rendering it valuable for secure communication. Comparatively, audio and image steganography have lower embedding capacity and robustness, respectively [38]. Although video steganography is effective, several challenges have been observed. Video steganography necessitates high computational power and can be detected through steganalysis attacks [39]. Only three articles regarding video steganography have also been observed, implying that it remains unexplored [40-42]. A study by Dasgupta *et al.,* [40] reported steganography with optimal imperceptibility by employing the genetic algorithm (GA). The study focused on frames with a 320 × 320 resolution while thoroughly examining time and space complexity. Several evaluation metrics (PSNR, MSE, and image fidelity) were also included in the study, emphasizing the importance of maintaining high-quality stego output frames.

Another study by Wang *et al.,* [41] introduced using the high efficiency video coding (HEVC) standard in 2019, which was effective in steganography-based cover selection. The study also selected 23 YUV color spaces alongside the HEVC as the cover medium for video-based steganography. Thus, video compression techniques could be adapted for information hiding. Meanwhile, Cao *et al.,* [42] presented an efficient video steganography technique based on H.264 advanced video coding (AVC) in YUV format. The study investigated Intra Prediction Mode (IPM)

modifications while highlighting the importance of maintaining security and video quality in steganography. Additionally, the evaluation metrics used in the study were PSNR and Accuracy Rate (AR) for quality and security assessment, respectively. Table 11 summarizes evaluation metrics used for video steganography. These metrics provided a more comprehensive and specialized set of criteria for evaluating the effectiveness and impact of video steganography techniques. The metrics addressed the various difficulties of video mediums as a means of covert data transmission. No common metrics were also observed to measure the effectiveness between techniques in one medium.

Table 11
Summary of definition for video steganography evaluation metrics and its description

Definition	Description
Jaro-Winkler Metric	Measures the similarity between the two pictured using the Jaro-Winkler distance
Bjontegaard Delta Bitrate (BDBR)	Quantifies the rate-distortion trade-off in video coding
Bjontegaard Delta Structural Similarity Index (BD-SSIM)	Evaluate structural similarity between images.
Intra-Prediction Mode (IPM)	Refers to the calibration of Intra Prediction Modes in video coding
Time Complexity Analysis	Assesses the computational time required for a specific operation
Space Complexity Analysis	Analyzes the memory or storage space required for a specific task

4.5 Additional Findings

This SLR provided a concise overview of similar evaluation metrics for analyzing images, audio, text, and video. Figure 11 displays a Venn diagram to summarize commonalities and differences in evaluation metrics used across mediums, in which the evaluation metric samples were applied in different mediums. Consequently, similar metrics were observed in other mediums, such as PSNR in image and audio covers. The Jaco-Wrinkler metric was also utilized in text and video covers while embedding capacity was used in image and text covers. Overall, this SLR contributed valuable steganography-based insights by examining the correlation between parameters, metrics, and the efficiency of cover selection techniques across different mediums.

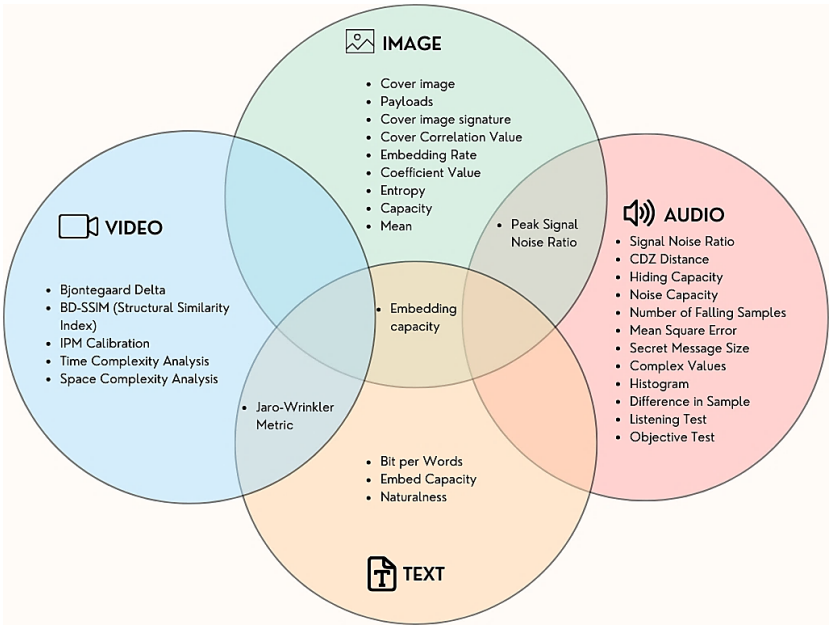

Fig. 11. A Venn diagram of evaluation metric sample used across different medium

5. Conclusions

This review conducted an SLR to identify relevant articles and address the specified RQs. Four categories were used to categorize the selected articles: image, audio, text, and video. The outcomes demonstrated that using parameters was heavily dependent on the category type. Nevertheless, certain categories (images) possessed more evaluation parameters. Various evaluation metrics were also employed to evaluate the performance of cover selection methods for different mediums. These metrics were used to determine the robustness, imperceptibility, and capacity of their approaches. Consequently, PSNR and SNR were widely employed for evaluating audio and images. This observation was attributed to the significant efficiencies of PSNR and SNR in their respective mediums for assessing perceptual quality and clarity. Despite PSNR and SNR serving as established metrics for images and audio, insufficient standardized metrics for text and video indicate a need for tailored evaluation criteria. Therefore, this SLR addressed the diverse requirements of cover selection by highlighting the variations in which no universally applicable evaluation method was proposed.

Cover selection could be daunting and require substantial time and resources when managing numerous datasets. Thus, this SLR provided a definitive framework for future researchers to improve cover selection through ML algorithms, significantly improving the selection process. The ML methods could also expedite and enhance the precision of cover selection by examining and acquiring knowledge from various datasets. Researchers could employ ML to investigate automated techniques that adapt well to the unique qualities of different media and messages. This advancement represents progress in the domain of steganography.

Acknowledgement
This research was funded by the Ministry of Higher Education (MOHE) Malaysia under the Fundamental Research Grant Scheme (FRGS/1/2020/ICT02/USIM/02/1). The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and MOHE for the support and facilities provided.

References

[1] Sedighi, Vahid, Rémi Cogranne, and Jessica Fridrich. "Content-adaptive steganography by minimizing statistical detectability." *IEEE Transactions on Information Forensics and Security* 11, no. 2 (2015): 221-234. https://doi.org/10.1109/tifs.2015.2486744

[2] Azam, Muhammad Harith Noor, Farida Hazwani Mohd Ridzuan, and M. Norazizi Sham Mohd Sayuti. "Optimized Cover Selection for Audio Steganography Using Multi-Objective Evolutionary Algorithm." *Journal of Information and Communication Technology* 22, no. 2 (2023): 255-282. https://doi.org/10.32890/jict2023.22.2.5

[3] Kekre, Hemant B., Archana Athawale, B. Swarnalata Rao, and Uttara Athawale. "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding." In 2010 3rd International Conference on Emerging Trends in Engineering and Technology, pp. 196-201. IEEE, 2010. https://doi.org/10.1109/icetet.2010.118

[4] Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet computing 5, no. 3 (2001): 75-80. https://doi.org/10.1109/4236.935180

[5] AlSabhany, Ahmed A., Ahmed Hussain Ali, Farida Ridzuan, A. H. Azni, and Mohd Rosmadi Mokhtar. "Digital audio steganography: Systematic review, classification, and analysis of the current state of the art." Computer Science Review 38 (2020): 100316. https://doi.org/10.1016/j.cosrev.2020.100316

[6] Majeed, Mohammed Abdul, Rossilawati Sulaiman, Zarina Shukur, and Mohammad Kamrul Hasan. "A review on text steganography techniques." Mathematics 9, no. 21 (2021): 2829. https://doi.org/10.3390/math9212829

[7] Vimal, Jithu. "Literature review on audio steganographic techniques." International Journal of Engineering Trends and Technology 11, no. 5 (2014): 246-248. https://doi.org/10.14445/22315381/ijett-v11p247

[8] Subhedar, Mansi S., and Vijay H. Mankar. "Current Status and Key Issues in Image Steganography: A Survey." Computer science review 13 (2014): 95-113. https://doi.org/10.1016/j.cosrev.2014.09.001

[9] Laishram, Debina, and Themrichon Tuithung. "A survey on digital image steganography: current trends and challenges." In proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT), pp. 26-27. 2018. https://doi.org/10.2139/ssrn.3171494

[10] Abed, Sa'ed, Suood Abdulaziz Al-Roomi, and Mohammad Al-Shayeji. "Efficient cover image selection based on spatial block analysis and DCT embedding." EURASIP Journal on Image and Video Processing 2019, no. 1 (2019): 87. https://doi.org/10.1186/s13640-019-0486-8

[11] Wang, Zichi, Guorui Feng, Liquan Shen, and Xinpeng Zhang. "Cover selection for steganography using image similarity." IEEE Transactions on Dependable and Secure Computing (2022). https://doi.org/10.1109/tdsc.2022.3181039

[12] Ren, Weixiang, Yibo Xu, Liming Zhai, Lina Wang, and Ju Jia. "Fast carrier selection of JPEG steganography appropriate for application." Tsinghua Science and Technology 25, no. 5 (2020): 614-624. https://doi.org/10.26599/tst.2019.9010069

[13] Sajedi, Hedieh, and Mansour Jamzad. "BSS: Boosted steganography scheme with cover image preprocessing." Expert systems with Applications 37, no. 12 (2010): 7703-7710. https://doi.org/10.1016/j.eswa.2010.04.071

[14] Li, Bin, Ming Wang, Xiaolong Li, Shunquan Tan, and Jiwu Huang. "A strategy of clustering modification directions in spatial image steganography." IEEE Transactions on Information Forensics and Security 10, no. 9 (2015): 1905-1917. https://doi.org/10.1109/tifs.2015.2434600

[15] Evsutin, Oleg, Anna Kokurina, and Roman Meshcheryakov. "Approach to the selection of the best cover image for information embedding in JPEG images based on the principles of the optimality." Journal of Decision Systems 27, no. sup1 (2018): 256-264. https://doi.org/10.1080/12460125.2018.1460163

[16] Nazari, Sara, and Mohammad Shahram Moin. "Cover selection steganography via run length matrix and human visual system." (2013): 131-138.

[17] Subhedar, Mansi S. "Cover selection technique for secure transform domain image steganography." Iran Journal of Computer Science 4, no. 4 (2021): 241-252. https://doi.org/10.1007/s42044-020-00077-9

[18] Sajedi, Hedieh, and Mansour Jamzad. "Evolutionary rule generation for signature-based cover selection steganography." Neural Network World 3, no. 10 (2009): 297-316.

[19] Sajedi, Hedieh, and Mansour Jamzad. "Using contourlet transform and cover selection for secure steganography." International Journal of Information Security 9 (2010): 337-352. https://doi.org/10.1007/s10207-010-0112-3

[20] El Abbadi, Nidhal K. "Cover optimization for image in image steganography." International Journal of Computer Science Issues (IJCSI) 10, no. 1 (2013): 556.

[21] Subhedar, Mansi S., and Vijay H. Mankar. "Performance evaluation of image steganography based on cover selection and contourlet transform." In 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, pp. 172-177. IEEE, 2013. https://doi.org/10.1109/cube.2013.39

[22] Seyyedi, Seyyed Amin, and Nick Ivanov. "Statistical Image Classification for Image Steganographic Techniques." International Journal of Image, Graphics and Signal Processing 6, no. 8 (2014): 19-24. https://doi.org/10.5815/ijigsp.2014.08.03

[23] Umamaheswari, G., and C. P. Sumathi. "Pixel selection based on the difference between secret message and cover image pixel for efficient information hiding." In 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1-5. IEEE, 2016. https://doi.org/10.1109/isco.2016.7726877

[24] Molato, Mark Rennel D., and Bobby D. Gerardo. "Cover image selection technique for secured LSB-based image steganography." In Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence, pp. 1-6. 2018. https://doi.org/10.1145/3302425.3302456

[25] Hajduk, Vladimir, and Dusan Levicky. "Cover selection steganography with intra-image scanning." In 2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA), pp. 1-4. IEEE, 2018. https://doi.org/10.1109/radioelek.2018.8376370

[26] Subhedar, Mansi S., and Vijay H. Mankar. "Curvelet transform and cover selection for secure steganography." Multimedia Tools and Applications 77, no. 7 (2018): 8115-8138. https://doi.org/10.1007/s11042-017-4706-x

[27] Shah, Pratik D., and Rajankumar S. Bichkar. "Genetic algorithm based approach to select suitable cover image for image steganography." In 2020 International Conference for Emerging Technology (INCET), pp. 1-5. IEEE, 2020. https://doi.org/10.1109/incet49848.2020.9154032

[28] Ali, Ahmed Hussain, Mohd Rosmadi Mokhtar, and Loay Edwar George. "Enhancing The Hiding Capacity of Audio Steganography Based on Block Mapping." Journal of Theoretical & Applied Information Technology 95, no. 8 (2017): 1441-1448.

[29] Singh, Kamred Udham. "A survey on audio steganography approaches." International Journal of Computer Applications 95, no. 14 (2014). https://doi.org/10.5120/16660-6640
[30] Balgurgi, Pooja P., and Sonal K. Jagtap. "Audio steganography used for secure data transmission." In Proceedings of international conference on advances in computing, pp. 699-706. Springer India, 2012. https://doi.org/10.1007/978-81-322-0740-5_83
[31] Nassrullah, Hussein A., Wameedh Nazar Flayyih, and Mohammed A. Nasrullah. "Enhancement of LSB Audio Steganography Based on Carrier and Message Characteristics." J. Inf. Hiding Multim. Signal Process. 11, no. 3 (2020): 126-137.
[32] Bhavana, S., and K. L. Sudha. "Text Steganography using LSB insertion method along with Chaos Theory." International Journal of Computer Science, Engineering and Applications 2, no. 2 (2012): 145. https://doi.org/10.5121/ijcsea.2012.2212
[33] Changder, S., S. Das, and D. Ghosh. "Text steganography through Indian languages using feature coding method." In 2010 2nd International Conference on Computer Technology and Development, pp. 501-505. IEEE, 2010. https://doi.org/10.1109/icctd.2010.5645849
[34] Luo, Yubo, and Yongfeng Huang. "Text steganography with high embedding rate: Using recurrent neural networks to generate chinese classic poetry." In Proceedings of the 5th ACM workshop on information hiding and multimedia security, pp. 99-104. 2017. https://doi.org/10.1145/3082031.3083240
[35] El Rahman, Sahar A. "Text steganography approaches using similarity of English font styles." International Journal of Software Innovation (IJSI) 7, no. 3 (2019): 29-50. https://doi.org/10.4018/ijsi.2019070102
[36] Shniperov, Alexey Nikolaevich, and K. A. Nikitina. "A text steganography method based on Markov chains." Automatic Control and Computer Sciences 50 (2016): 802-808. https://doi.org/10.3103/S0146411616080174
[37] Zhang, Mingliang, Zhenyu Li, Pei Zhang, Yi Zhang, and Xiangyang Luo. "A novel high-capacity behavioral steganographic method combining timestamp modulation and carrier selection based on social networks." Symmetry 14, no. 1 (2022): 111. https://doi.org/10.3390/sym14010111
[38] Dalal, Mukesh, and Mamta Juneja. "A survey on information hiding using video steganography." Artificial Intelligence Review 54, no. 8 (2021): 5831-5895. https://doi.org/10.1007/s10462-021-09968-0
[39] Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa GM Mostafa. "Video steganography: a comprehensive review." Multimedia tools and applications 74 (2015): 7063-7094. https://doi.org/10.1007/s11042-014-1952-z
[40] Dasgupta, Kousik, Jyotsna Kumar Mondal, and Paramartha Dutta. "Optimized video steganography using genetic algorithm (GA)." Procedia Technology 10 (2013): 131-137. https://doi.org/10.1016/j.protcy.2013.12.345
[41] Wang, Jie, Xiaoqing Jia, Xiangui Kang, and Yun-Qing Shi. "A cover selection HEVC video steganography based on intra prediction mode." IEEE access 7 (2019): 119393-119402. https://doi.org/10.1109/access.2019.2936614
[42] Cao, Mingyuan, Lihua Tian, and Chen Li. "A secure video steganography based on the intra-prediction mode (IPM) for H264." Sensors 20, no. 18 (2020): 5242. https://doi.org/10.3390/s20185242
[43] Sun, Yifeng, and Fenlin Liu. "Selecting cover for image steganography by correlation coefficient." In 2010 Second International Workshop on Education Technology and Computer Science, vol. 2, pp. 159-162. IEEE, 2010. https://doi.org/10.1109/etcs.2010.33
[44] Yuan, Junying, and Haishan Chen. "Embedding suitability adaptive cover selection for image steganography." In 2014 International Conference on e-Education, e-Business and Information Management (ICEEIM 2014), pp. 36-39. Atlantis Press, 2014. https://doi.org/10.2991/iceeim-14.2014.11
[45] Jalili, Zahra, Hedieh Sajedi, and Maryam Hasanzadeh. "Image cover selection for steganography based on run length matrix." The Modares Journal of Electrical Engineering 14, no. 3 (2014): 48-55.
[46] Wu, Songtao, Yan Liu, Shenghua Zhong, and Yang Liu. "What makes the stego image undetectable?." In Proceedings of the 7th international conference on Internet multimedia computing and service, pp. 1-6. 2015. https://doi.org/10.1145/2808492.2808539
[47] Hajduk, Vladimír, and Dušan Levický. "Accelerated cover selection steganography." In 2017 27th International Conference Radioelektronika (RADIOELEKTRONIKA), pp. 1-4. IEEE, 2017. https://doi.org/10.1109/RADIOELEK.2017.7937591
[48] Zhong, Nan, Zhenxing Qian, Zichi Wang, Xinpeng Zhang, and Xiaolong Li. "Batch steganography via generative network." IEEE Transactions on Circuits and Systems for Video Technology 31, no. 1 (2020): 88-97. https://doi.org/10.1109/tcsvt.2020.2974884
[49] Hamid, Nagham, Balasem Salem Sumait, Bilal Ibrahim Bakri, and Osamah Al-Qershi. "Enhancing visual quality of spatial image steganography using SqueezeNet deep learning network." Multimedia Tools and Applications 80, no. 28 (2021): 36093-36109. https://doi.org/10.1007/s11042-021-11315-y

[50] Wang, Zichi, Xinpeng Zhang, and Zhaoxia Yin. "Joint cover-selection and payload-allocation by steganographic distortion optimization." IEEE Signal Processing Letters 25, no. 10 (2018): 1530-1534. https://doi.org/10.1109/lsp.2018.2865888

[51] Wang, Zichi, and Xinpeng Zhang. "Secure cover selection for steganography." IEEE Access 7 (2019): 57857-57867. https://doi.org/10.1109/ACCESS.2019.2914226

[52] Wang, Zichi, Shujun Li, and Xinpeng Zhang. "Towards improved steganalysis: When cover selection is used in steganography." IEEE Access 7 (2019): 168914-168921. https://doi.org/10.1109/ACCESS.2019.2955113

[53] Chen, Menghua, Peisong He, and Jiayong Liu. "Hltd-csa: Cover selection algorithm based on hybrid local texture descriptor for color image steganography." Journal of Visual Communication and Image Representation 89 (2022): 103646. https://doi.org/10.1016/j.jvcir.2022.103646

[54] Zhang, Xueyuan, Rangding Wang, Li Dong, Diqun Yan, Yuzhen Lin, and Jie Wang. "Towards Designing an Effective Complexity Indicator for Audio Steganography." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020. https://doi.org/10.1109/icc40277.2020.9148992