electronics

MDPI

Article

An Analysis of 3D Steganography Techniques

Rohit Tanwar [1,*], Urmila Pilania [2], Mazdak Zamani [3,*] and Azizah Abdul Manaf [4]

[1] School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[2] Department of CST, Manav Rachna University, Faridabad 121004, India; urmila@mru.edu.in
[3] School of Business and Information Sciences, Felician University, Rutherford, NJ 07070, USA
[4] Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia; azizahmanaf18@gmail.com
* Correspondence: rohit.tanwar.cse@gmail.com (R.T.); ZamaniM@felician.edu (M.Z.)

Abstract: Steganography has become a preferred technique these days to successfully hide secret messages. Various research has been done in the past to justify and analyze suitable types of cover file, such as images, audio, videos, etc. Advancement in the image-processing domain has opened various possibilities of using three-dimensional (3D) images as cover files. In this paper, a systematic study of the research work done on 3D steganography in the last fifteen years has been carried out. The study is divided into different sections based on the types of algorithms used, additional security features, evaluation parameters, etc. Moreover, certain steganalysis techniques that are applicable for 3D steganography are also discussed.

Keywords: 3D steganography; 3D steganalysis; imperceptibility; concealing capacity; robustness; structure similarity index measure

Citation: Tanwar, R.; Pilania, U.; Zamani, M.; Manaf, A.A. An Analysis of 3D Steganography Techniques. *Electronics* **2021**, *10*, 2357. https://doi.org/10.3390/electronics10192357

Academic Editors: Tony Jan, Deepak Puthal, Mukesh Prasad and Anca Ralescu

Received: 28 August 2021
Accepted: 22 September 2021
Published: 27 September 2021

1. Introduction

Steganography plays a significant role in secret information transmission and has garnered considerable attention from scholars for years. A variety of options are in practice for the use of different types of multimedia files as cover. Recently, 3D objects have been gaining popularity as they provide a good opportunity for multimedia content. The features of 3D objects are prompting researchers towards 3D steganography, away from traditional digital multimedia files such as text, image, inaudible frequency, and video in their native forms [1]. The 3D multimedia files can hide a large amount of secret data. These objects also keep the secret data safer from unintentional hackers by concealing secret information inside hidden faces. Because of the good visual quality of the stego file, the chances of detection of the secret information in the 3D objects are reduced [2].

Multimedia files in 3D are playing a significant role in numerous standard applications, such as cutting-edge machinery, computer-generated reality, and 3D photogravure. These 3D multimedia files also have applications in education, entertainment, games, business, video conferencing, marketing and advertisement, etc. The 3D data concealing technique started in the late 90s when entertainers and 3D visuals inventors desired to impose their exclusive rights on material. Subsequently, several 3D data-concealing techniques have been developed by academicians and researchers. Currently, 3D images are getting popular as compared to other 3D multimedia files because of their intrinsic properties [3–5].

In this paper, a systematic study of 3D steganography research work carried out in the last 1.5 decades has been done. The research has been analyzed on the basis of the type of cover file, publication trend, and steganalysis perspective; and numerous works from related areas have been studied, which are focused on audio, image, and video steganography, as well as watermarking [6–51]. Moreover, the key features of the relevant research have been categorized and listed in tabular forms. The key observations and findings are listed in the later sections, which will be helpful in future research in a similar domain.

2. 3D Steganography in Different Domains

Here in this section, steganography is divided into mainly two sections, based on the domain used to hide the secret data. These two domains are the spatial and transform domains. In the spatial domain, bits of the cover files are replaced by bits of secret data [52,53]. Spatial domain techniques are simple and carry a great concealing capacity. These techniques can be easily exposed against signal-processing attacks. Meanwhile, transform domain techniques are complex and provide high security against attacks. Transform domain techniques find some complex regions in which to embed secret data first, and then conceal secret data inside those complex regions [54]. So, these techniques result in better security and good visual quality of the stego file. Some of the spatial as well as transform domain techniques are shown in Figure 1 and explained in detail:

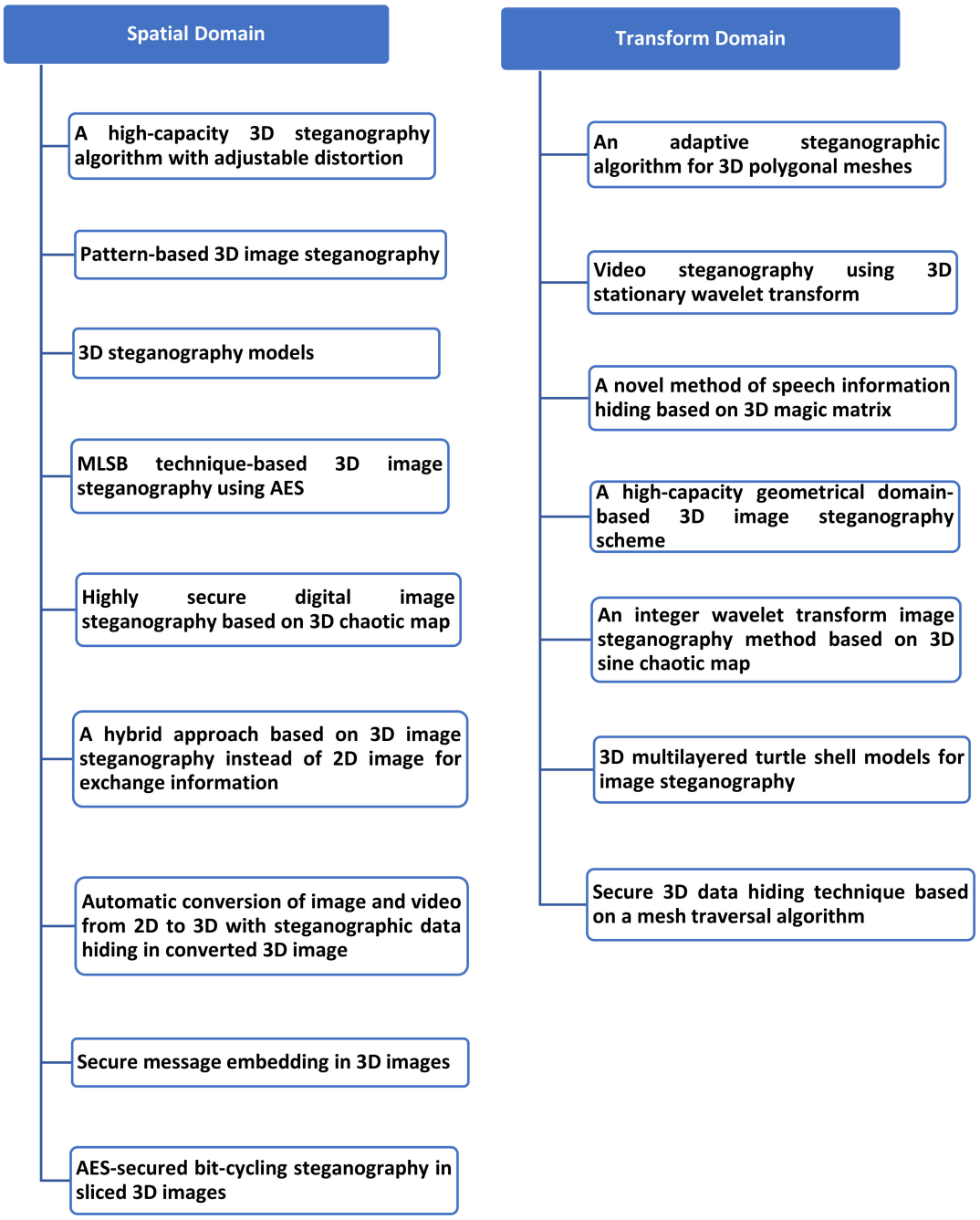

Figure 1. Different domains of 3D steganography.

Most of the existing 3D steganography techniques work in the spatial domain as shown in Figure 2. Spatial domain techniques allow the substitution of secret information on the pixels of the carrier file. However, transform domain techniques work on the frequency as well as the time-domain of the carrier file. Transform domain techniques first find the complex region in the cover file to embed the secret data. Concealing secret data inside complex regions results in more robustness against operations such as cropping, clipping, translation, scaling, etc.

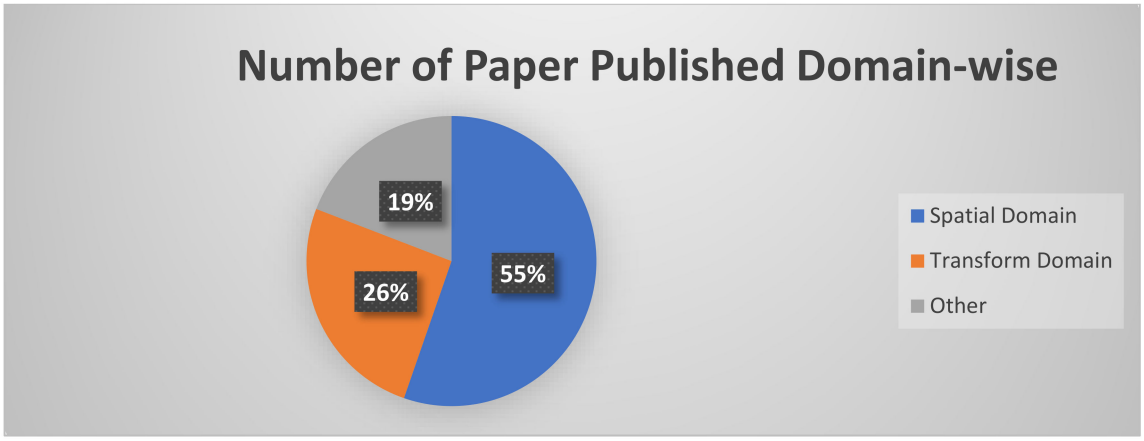

Figure 2. Categorization based on domain.

2.1. 3D Steganography in Spatial Domain

A review of nine spatial domain steganography techniques was done in this section. These techniques were reviewed based on features such as carrier files, the method used to conceal the secret information, their performance evaluations, etc. Spatial domain 3D steganography is getting popular among researchers because of its large embedding capacity and simplicity [55]. The nine spatial domain-based steganography techniques are explained as follows:

Steganography is gaining more and more attention from researchers these days. With the growth of communications systems and transmission technologies, online transmission of private information has also been increased. So, the security of private information has become an important issue. Steganography can provide high security, imperceptibility, large concealing capacity, and robustness against attacks. The high-capacity steganography technique was proposed using buffer space with the help of a shifting strategy as shown in Figure 3. Pre-processing of the 3D carrier file is needed for extra security and to hide a larger amount of secret information. Concealing of secret information was done in the spatial domain.

The carrier file is divided into many portions of equal size in sequence. Buffer space is chosen for storing the portioned carrier file. Finally, secret information is concealed inside these portioned components by shifting them among the intervals. As all the alterations are needed to be done in buffer space only, there should be less disturbance in the stego file compared to other existing techniques. The relationship between PSNR and embedding capacity (EC) was also calculated by the authors. Average PSNR was calculated as 133 dB and average EC was calculated as 92.9%. However, the proposed technique is robust against different attacks such as scaling, rotation, translation, clipping, and cropping, etc. Also, it has a high concealing capacity and good visual quality of the stego file [56].

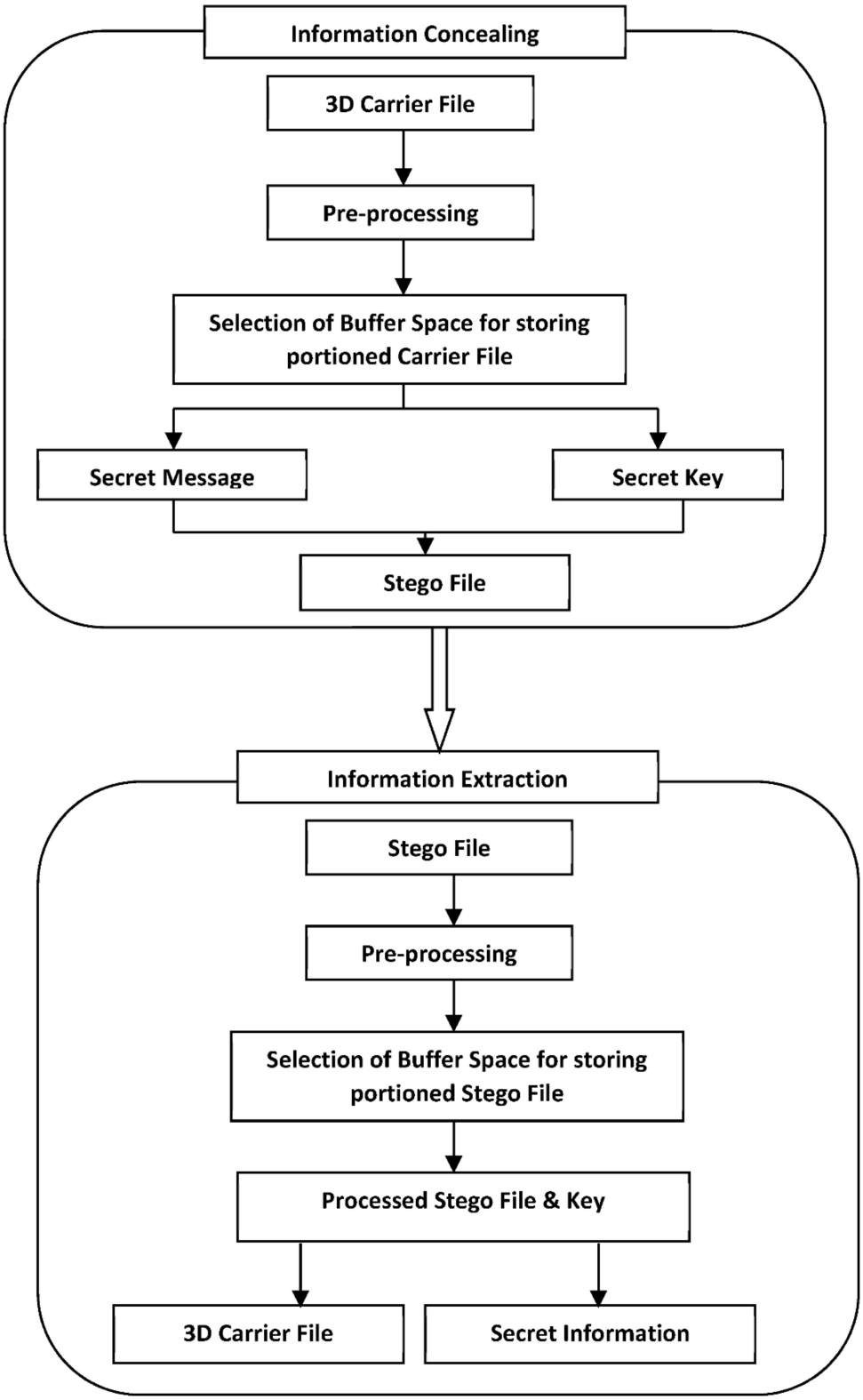

Figure 3. Technique of 3D steganography using buffer space [56].

The 3D cover file uses the entire three axes for concealing secret information on the suitable region of interest, which results in great robustness. A key is optional for the embedding and extraction of secret data. A different key can be used whenever the process of concealing and extraction takes place. Information concealing was done in the spatial domain by the authors using LSB substitution. Concealing secret data in the spatial domain

is simple and easy. Sometimes, however, secret information can be detected with the help of signal-processing attacks, as well as steganalysis techniques. Spatial domain techniques can be used directly without identifying the region of interest. Figure 4 represents both the concealing and extraction of secret information inside the 3D carrier file.

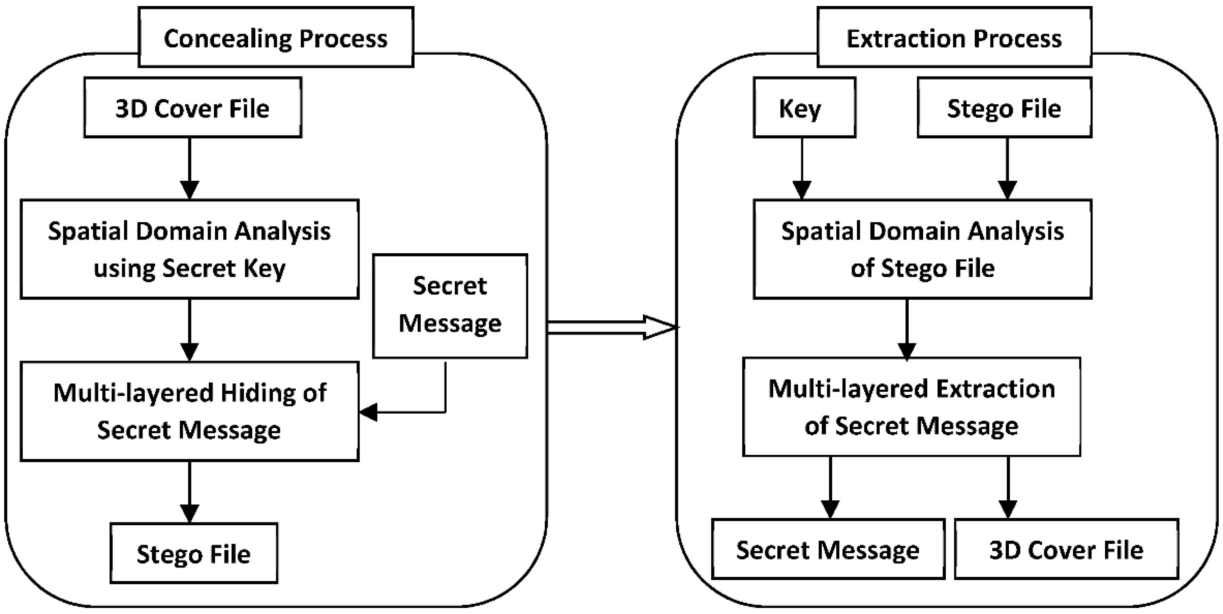

Figure 4. Multilayer data hiding using LSB [57].

In the proposed paper, multilayer data hiding is performed by the authors. The given file is converted to the multilayered version by the direct accumulation of additional layers. In the multilayer concealing process, two-state region subsets are prearranged in an interleaved style for every layer. Moreover, slight alteration is done in state regions of even layers which are moved to the right by two. The direction of shifting is bidirectional for a given vertex. Using the above-defined rule, vertices are shifted inward and rearward in the half interval of a state region when the secret information is concealed by using the LSB technique. By using the proposed technique, concealing capacity is improved due to the multilayer concept as well as 3D cover files. It is robust because the 3D carrier file visual quality of the stego file is good [57].

In the proposed paper, a key was produced by the secret message. Then this produced stego key was used to embed the secret data inside the carrier file. The proposed technique worked in the spatial domain for embedding the secret data. It had the following parts: secret data selection, generation of a stego key, formulation of a triangular mesh, concealing of secret message, and extraction of the secret message. The secret message was first converted to ASCII and then into binary format.

The binary form was divided into three parts, and zeroes were added as extra padding. These three parts were converted into decimal forms. From each part minimum and maximum were calculated. Then these calculated values were normalized, and the normalized values were used to find the median. This normalized value was then used in the selection of the stego key. Figure 5 explains the complete process of LSB steganography in the spatial domain.

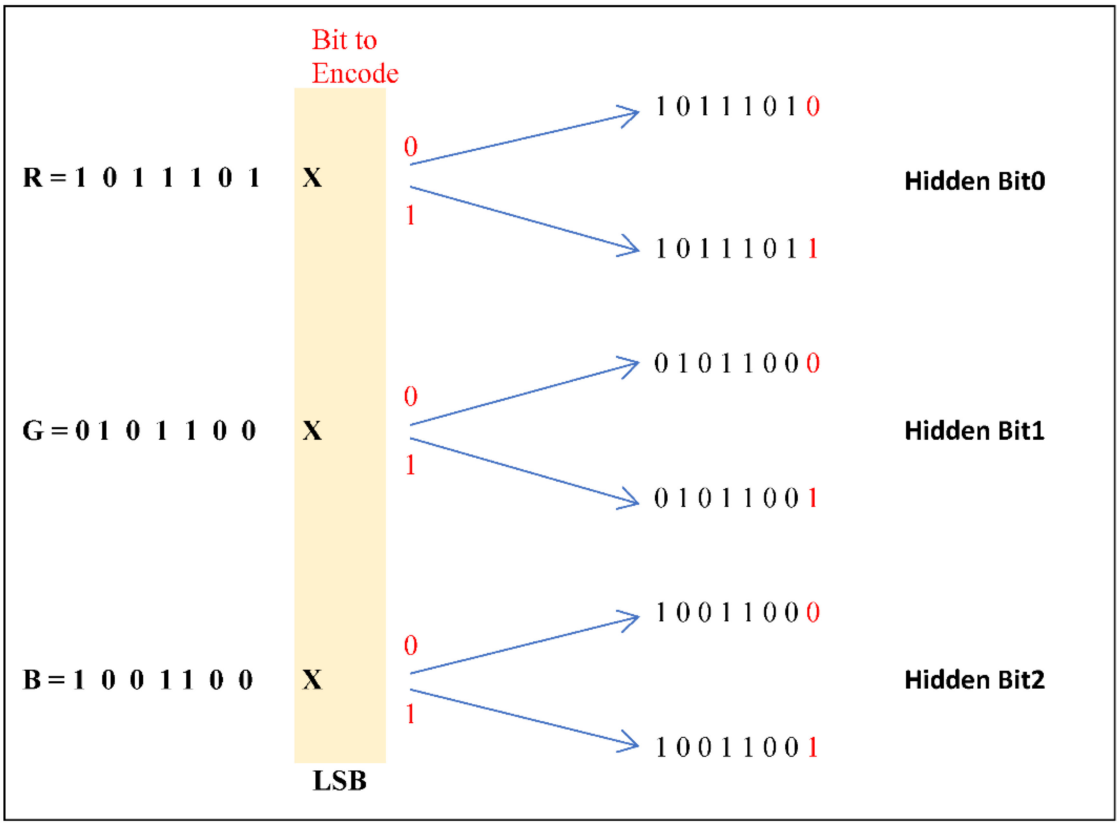

Figure 5. Steganography using the LSB technique [58].

The initial large triangle was decomposed into smaller triangles to find a large number of vertices. By dividing the side of the triangle into two equal parts, it was divided into many smaller triangles. These triangles were then used to embed secret data. With the help of the stego key, secret data was hidden in vertices in a clockwise direction using the LSB technique. The technique substitutes the two least significant bits of the vertex with secret data bits. For extraction of the secret message again, the stego key was generated with the help of the concealed part. The proposed technique was blind steganography, so no cover file was produced. The quality of research work was evaluated with the help of parameters: MSE, PSNR, bit error rate (BER), and normalized Hausdorff distance (NHD), etc. The concealing capacity of the proposed work was found to be good in several bits. The average PSNR value for the research work was calculated as 55 dB. The average MSE was calculated as 0.148 for the work. The average BER was calculated as 2.25 for the proposed work. Normalized Hausdorff distances were calculated as 6.17 for the proposed work [58].

Chaotic maps are iterative functions that are discrete. These maps are used to privately secure secret information. Chaotic maps have their applications in mathematics, science, computers, finance, etc. In the paper, 3D chaotic maps were proposed by the authors for the secret key. Secret messages and carrier files were taken in the form of an image. After hiding the secret message, JPEG compression was applied to the secret message. LSB was used to conceal secret information over the least significant bits of the carrier file.

Figure 6 represents the complete concealing and extraction process. Chaotic map primary keys were input and formed a flag matrix for grouping certain pixels of carrier image. One by one, secret message bits were taken and generated the carrier image chaotic pixel. The process was repeated until all the conditions held. The chosen bit of the secret message was concealed in the generated carrier image chaotic pixel of LSB, and this pixel was tagged. If the chosen pixel was the last pixel, the process was stopped process and the stego image produced; otherwise, the next bit of secret message was chosen. For checking the quality of the proposed research work visual test, a Chi-square test, PSNR, structure similarity index matrix (SSIM), and a Nist test were performed by the authors.

The proposed research work was found to be good compared to other existing techniques. The average value of PSNR, SSIM, and the Nist test was calculated as 55, 0.9986, and 0.82 respectively [59].

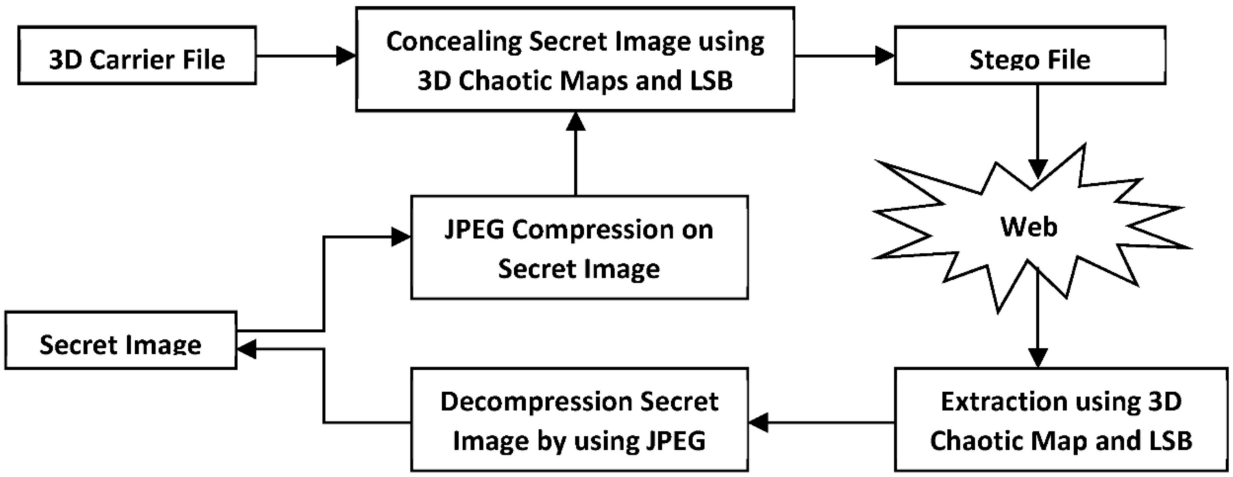

Figure 6. 3D Steganography using chaotic map and the LSB technique [59].

In the proposed paper, again 3D mesh triangles were used to conceal secret information. These 3D mesh triangles are very much suitable to conceal secret information. 3D objects can be very well-visualized to find the suitable region of interest. The AES algorithm was applied to the secret message to encrypt it into some unreadable form. AES is the standard algorithm with a different size key set. Encryption, along with steganography, improves the security of the proposed algorithm. For concealing secret information most significant bit (MSB) was used by the authors.

Figure 7 shows MSB substitution of secret information with complete details. The main proposed method consisted of a selection of 3D carrier images, encryption using AES, concealing of secret information using MSB, decryption, and extraction of secret information. Additionally, the discrete wavelet transform (DWT) technique was applied to secret information to compress it and improve concealing capacity. MSB provides more safety to the secret data by increasing the complexity of the detection of secret information. The experimental results of the proposed techniques prove their robustness as well as greater concealing capacity [60].

Steganography has its applications in various fields such as medical, business, science, military, and education. As a carrier file, 3D images are finding very much popularity on social networking sites. The 3D images provide large exposure for finding complex regions in which to embed secret data. In the proposed paper, encryption was combined with steganography to improve security levels. For encrypting the secret information, a symmetric algorithm was applied on RGB images. For concealing the secret information, a pseudo-random number generator was used. Pixels chosen by the random number generator are substituted by the secret information. Figure 8 shows the complete process of concealing and extracting secret information.

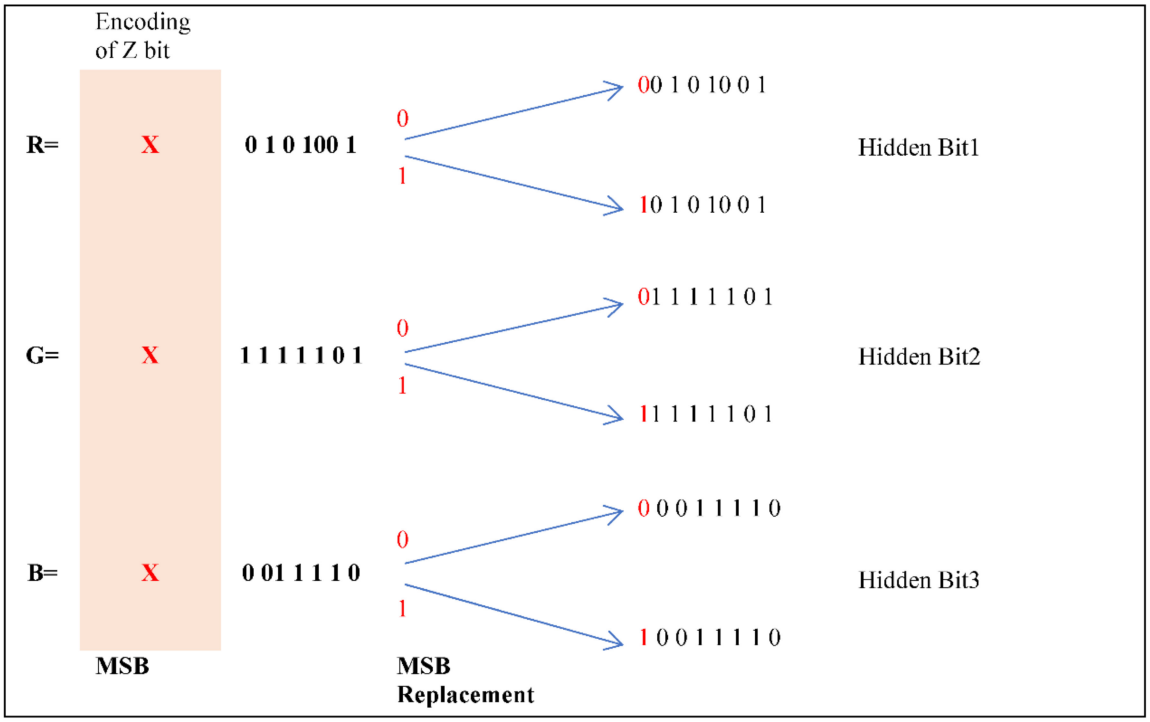

Figure 7. 3D Steganography using the MSB technique [60].

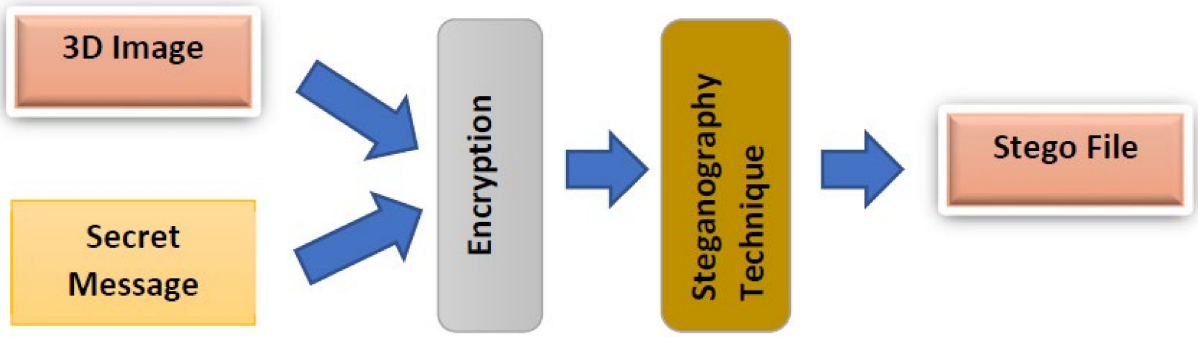

Figure 8. 3D image steganography with encryption [61].

For concealing secret information, the spatial domain substitution method was used by the authors. For decoding secret information, the reverse process of concealing was used by the authors. The proposed research work has to conceal a capacity of approximately 256 bits in the carrier file. A PSNR value was calculated approximately equal to 30 dB. The MSE for the work was found to be in the range of 0 to 1. The stego file created has a very good quality almost equal to the original file. The proposed work was implemented in MATLAB. Security provided by the proposed technique was better than the existing techniques. It was robust against image-processing attacks [61].

Initially, the video file was taken as the carrier file by the authors in this paper. Then the video file was converted into multiple frames, and the frames into images. In a second, 24 frames are processed to convert into images. The 2D to 3D video conversion was done to conceal the secret information. By converting the input files into 3D, the security of online information transmission was enhanced. For conversion into 3D, the file pixels of the image were studied in-depth, based on transformation. The depth of the 3D image was calculated by applying nearest-neighbor regression. For calculating the depth of the image, the following points were used: color, location of object, motion, brightness, etc. Finally, the depth of all the points calculated were combined to find the median. Median filtering

across depth fields is known as depth fusion. The output of the depth fusion process of removing variation is known as depth smoothening.

Figure 9 shows the complete process of concealing and extracting secret information. After reading and analyzing data, the input image edges were detected by using the nearest neighbor depth learning algorithm. The algorithm also helps to find the boundary points for concealing secret information. Secret information was taken in the form of text. The steganography process then conceals secret information by applying a spatial domain-based method. The resultant stego file has a good visual quality almost equal to the original carrier file. For the extraction of secret information, a reverse process was used. Simulation of the research work proved its quality [62].

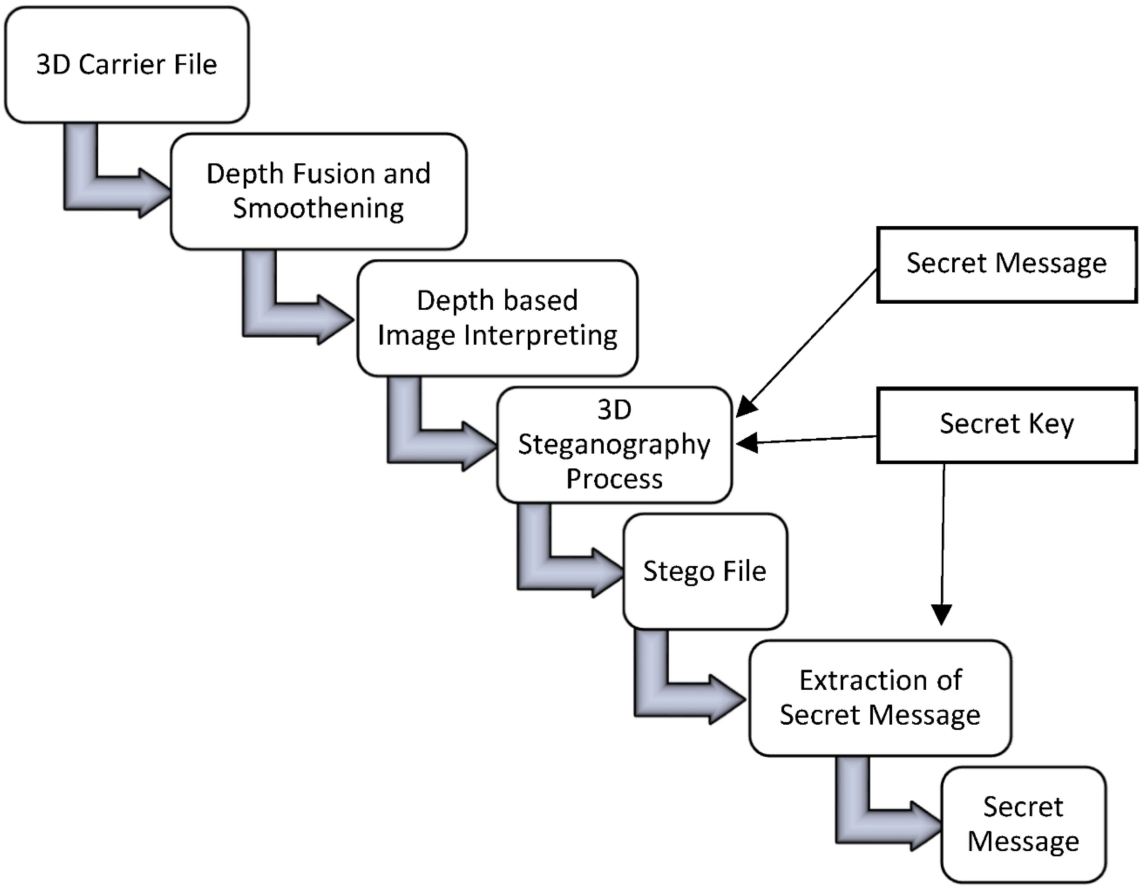

Figure 9. 3D steganography using nearest-neighbor depth calculation [62].

Three different methods of 3D image steganography have been proposed, which are geometric domain-based steganography, topological domain-based steganography, and representation-based steganography. The 3D images are decomposed into multiple layers of 2D images resulting in improved concealing capacity. Proposed research work was done into four parts: encryption using AES-128; encoding; steganography; and finally, jamming. AES-128 was applied to a secret message to encrypt it. After encryption, encoding of the secret information was done using a recurrence code with a recurrence key N. N was any integer value that helps to reduce the distortion in the carrier file. The size of the encoded and encrypted secret information was checked as to whether or not it was suitable to conceal that information in the carrier file. The proposed research work is also shown in Figure 10 as follows.

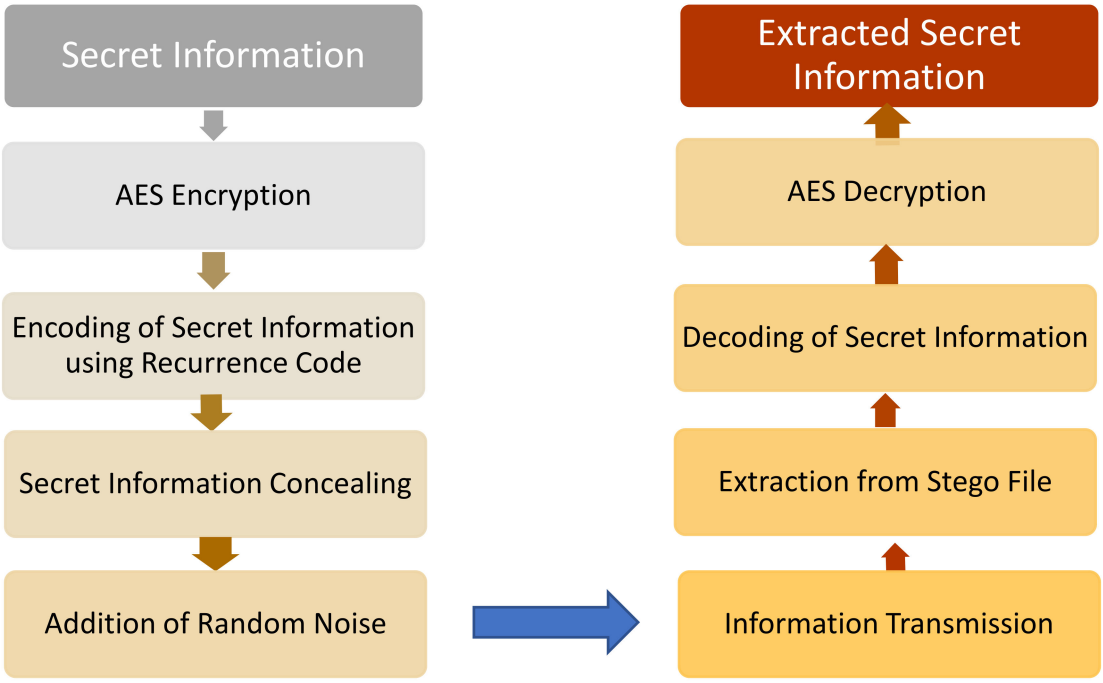

Figure 10. 3D steganography technique using recurrence code [63].

The 3D carrier file was thus selected according to the size of secret information to be concealed. The 3D carrier file was divided into frames that carry red, green, and blue color components. Concealment of the secret information was done in the blue component of the carrier file. The human visual system is less susceptible to alteration in the blue color components. LSB was applied to the blue component to hide the secret information. LSB results in a high concealing capacity and low visual distortion in the carrier file. Proposed research work was implemented using the Wolfram Mathematica tool. The quality of research work was measured in terms of concealing capacity, MSE, and PSNR. Average MSE was calculated as 0.30 and PSNR as 53 dB. The average concealing time was calculated approximately equal to 500 s [63].

In the case of cryptography, secret information is scrambled to some unreadable form. However, in the case of steganography, secret data is embedded inside the carrier file. In the case of cryptography, because of the visibility of the secret information, there is a chance of exposure. In steganography, however, the existence of the secret information is hidden from the third party, so there are fewer chances of the exposure of the secret information. Online use of 3D images these days results in high concealing capacity. The visual quality of the 3D stego file also results in improved quality, because of the exploration of complex regions. The process of secret information concealment using the LSB technique is shown in Figure 11.

The paper proposes two-layer security using AES at the first level and LSB steganography technique at the second level. The 3D image was converted into a 2D image first and then secret information was concealed inside the sliced parts. Using AES, a 128-bit key was generated to encrypt the secret information. After encryption, the secret information was concealed using the LSB technique. Concealment of the secret information was done inside the selected bits. The selection of bits was done using an arithmetic sequence. An arithmetic sequence finds the common difference between consecutive bits by setting common differences for the complete sequence. Selected bits are replaced by bits of secret information. The quality of research work was calculated in terms of MSE, PSNR, MSSIM, mean absolute error (MAE), and entropy. Simulation of the work proved that the proposed research work has good concealing capacity, good visual quality, and robustness against attacks. Average PSNR was calculated as 51 dB, MSE was 0.498, MSSIM was 0.9704, and MAE was calculated as 0.9704 for the research work [64].

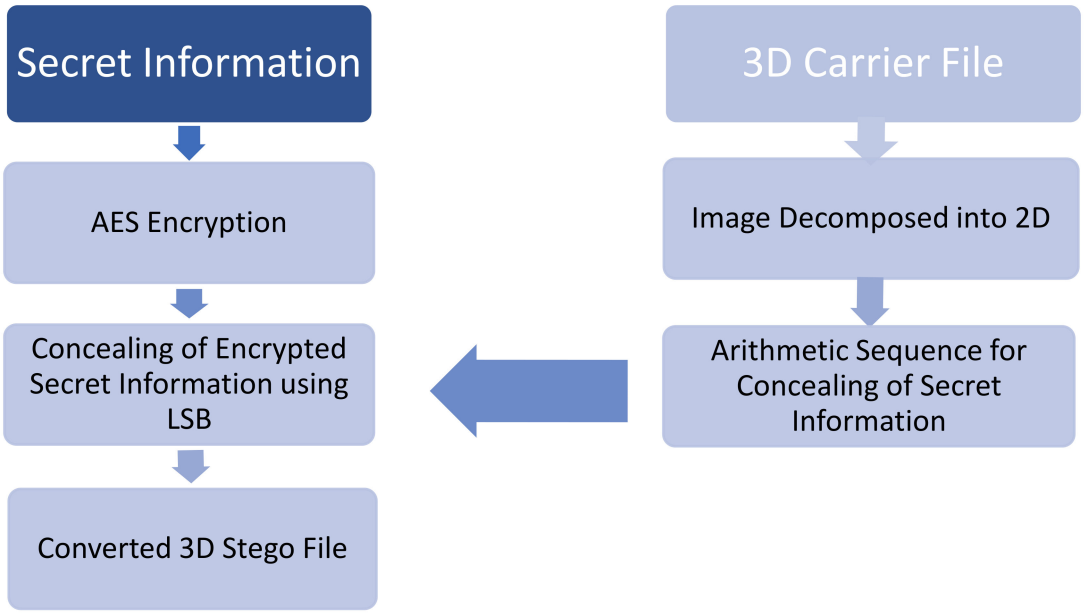

Figure 11. 3D steganography using LSB with arithmetic sequence [64].

2.2. 3D Steganography in the Transform Domain

In this research, various transform domain-based 3D steganography techniques were studied in detail. Transform domain-based techniques are robust and time-consuming ways to conceal and extract secret information [65]. These techniques were explored based on the carrier file used, the technique used to conceal secret information, and evaluation parameters, etc.

Because of the growth of the internet, the security of data transmission is becoming an important issue in everyone's life. Methods of 3D steganography provide secure ways to transmit information without the knowledge of a third party Demand for 3D multimedia files is increasing day by day.

In the proposed paper, 3D polygon meshes were used to hide a secret message. Adaptive minimum distortion estimation (AMDE) was applied to attain and preserve shape features such as edges, vertices, and origin, etc. Concealment of secret information was done by finding the correlation between neighbor vertices. Secret key, hash function, and diffusion techniques were also combined to provide more security. Figure 12 shows the process of concealing and extracting the secret information.

For pre-processing, principal component analysis (PCA) was applied to the polygon to decompose it into smaller polygons. PCA first produces a vertex body table (VBT), which provides a relation between a vertex and polygon. Another table generated by PCA is the polygon neighbor table (PNT), which provides the relation for connections between polygon and its neighbor. The whole process of pre-processing was very complex and time-consuming. In reducing complexity and search time, VBT helps by eliminating some of the candidate polygons. The AMDE procedure helps to conceal at least three bits in a vertex, resulting in improved concealing capacity. Message adaptation estimation (MAE) helps to find the suitable region of interest by avoiding several vertex positions, resulting in greater imperceptibility of the concealed material. Minimal distortion distance estimation (MDDE) calculates the distance between the vertices to reduce the noise. MDDE helps to improve the robustness of the proposed technique. Robustness was checked against different signal-processing attacks, such as rotation, scaling, translation, cropping, and clipping. The value calculated for research work in terms of evaluation parameters was EC = 522834 bit, time consumed = 1.16 s, and distortion = 5.69×10^{-6} [66].

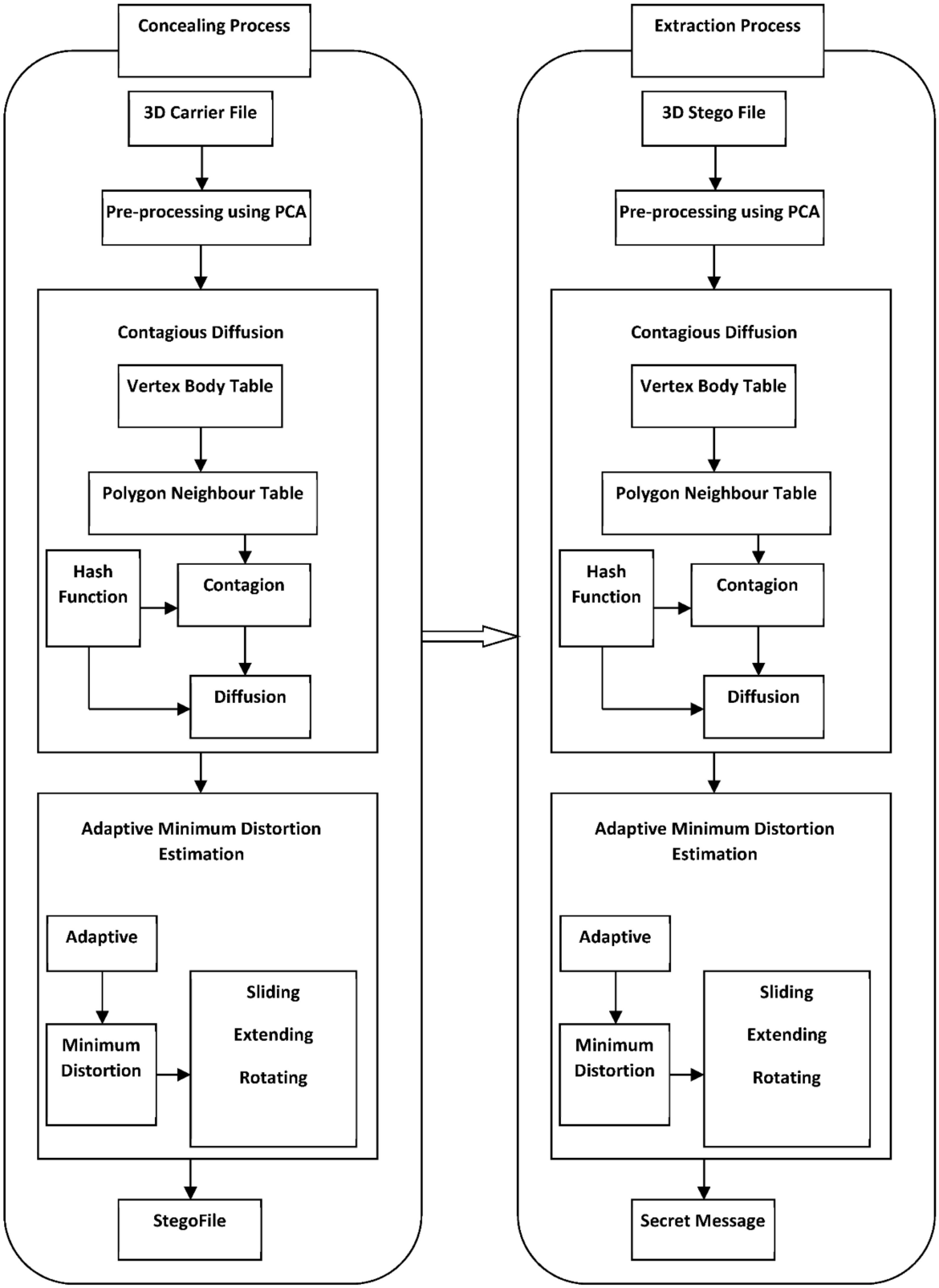

Figure 12. 3D steganography using a 3D polygon [66].

Video files are getting popular these days because of their applications on social networking sites. However, information security is becoming a major issue due to the popularity of digital multimedia files. Many security techniques are available, such as cryptography, watermarking, steganography, etc.

The authors in this work have proposed the use of 3D steganography using stationary wavelet transform (SWT). The proposed technique works in the time and frequency domains, both resulting in improved security and robustness. SWT detected motion among different video frames. Then, later on, the detect motion frames were decomposed using wavelet transform. The 3D SWT divided signals up into two levels to provide more security to secret information. The first signal was divided into four sub-bands: LL, LH, HL, and HH. Then, again, the LL component was decomposed into four sub-bands. Figure 13 shows the complete proposed research work.

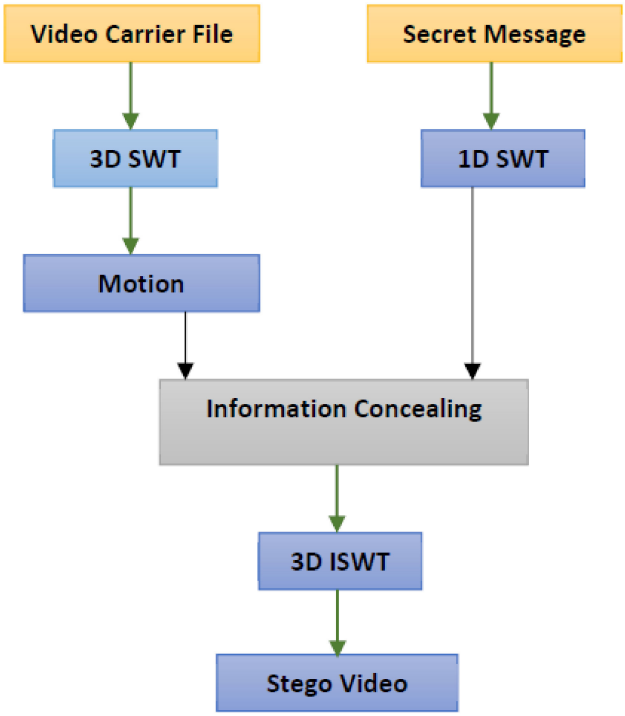

Figure 13. 3D steganography using SWT [67].

We applied 1D SWT onto secret images to decompose them into L and H components. Then L components were concealed inside HHH components using 3D SWT on the carrier file. Wavelet fusion was used to merge the carrier component and secret information component. Secret information retrieval is the reverse process of information concealing. On the stego file, SWT was applied to detect motion among video frames. These processes of motion detection help to find the frames that carry secret information. Then, inverse SWT was used to extract secret information from the carrier file. Performance metrics such as MSE, PSNR, and SSIM were applied to check the quality of the proposed work. Average PSNR was calculated as 37.8 dB and average SSIM was found to be 98.02 for the research work [67].

However, extending the concept of steganography, the carrier file was taken as the audio in the proposed paper. The concept of the 3D magic matrix was used to hide the secret information. The low bitrate codec G723.1 was used as a carrier file in the proposed research work. G723.1 is a widely used audio file in the communication media over the web. The concealing of secret information was done using a line spectral pair (LSP) index. First, the framing of the G723.1 signal was done, and then LSP analysis and linear prediction coefficients (LPC) quantization were done. The best suitable numbers for information hiding were separated by the aforementioned process for concealing secret information. Figure 14 shows the concealing and extraction process as follows.

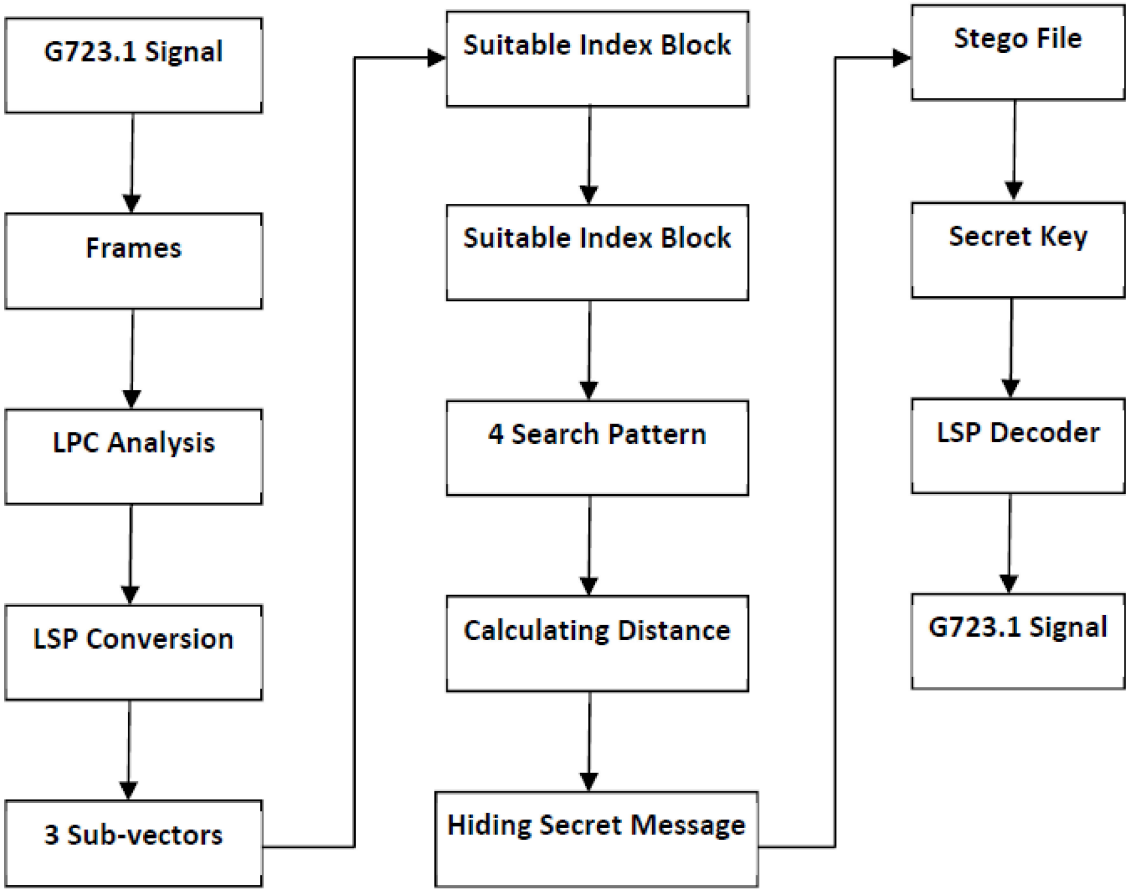

Figure 14. 3D steganography using sudoku matrix [68].

The 3D sudoku matrix has more space and complex points as compared to the 2D sudoku matrix. The 3D matrix provides an exploration of complex points based on three parameters such as length, breadth, and height. It carries a 9×9 matrix with 9, 3×3 sub-matrices. There are 81 cells on one surface, including a total of six surfaces. The authors suggested four searching patterns to find the matched index code word. Euclidean distance was used to find the distance or relationship between two neighbor code words. The codeword with the smallest distance was chosen for the second code index. Then the second code indexes were quantized based on the value of secret information to be concealed.

Retrieval of secret information was relatively simple as compared to the concealing process. It simply requires the secret key and the stego file created. Simulation of the work proved that the proposed research work carries the concealing capacity of 200 bps. Perceptual evaluation of speech quality (PESQ) was also carried out to check the quality of the resultant stego file. Then signal-to-noise ratio (SNR) was carried out for the subjective test of the visual quality of the proposed work. The average PESQ for the work was calculated as 3.6, and embedding capacity was found to be 200 bits/s [68].

During the last few years, excessive growth in the field of information transmission has been observed. Steganography is the art and science of concealing secret information in such a way that no one apart from the sender and receiver can know the existence of the secret data. In the proposed work, Blowfish encryption, along with geometric domain-based steganography, are combined for 3D objects. The 3D image steganography conceals secret information inside the vertices, edges, and faces of the defined object. As a large number of vertices, edges, and faces are available in 3D objects, 3D image steganography is gaining popularity over 2D image steganography.. The 3D steganography works in all the domains, such as the spatial domain, transform domain, geometric domain, topological domain, and representation domain. The basic idea behind the geometric domain is the

representation of the object. Because of the wide variety of faces, vertices, and edges for concealment, the capacity of 3D image steganography is very large compared to the 2D steganography techniques.

In the proposed research work, 3D image steganography technique was proposed on polygon models as shown in Figure 15. The secret message was first encrypted with the Blowfish algorithm to improve the security of the research work. After that, the polygon was modified according to the bit value of the secret information. The secret information was concealed inside the 4th and 5th decimal points of the vertex. If the bit to be concealed is 1, then the 4th or 5th decimal points were replaced by the odd value from 1 to 9 randomly. On the other hand, if the information bit to be concealed is 0, then the 4th or 5th decimal points were replaced by even values from 2 to 8 randomly.

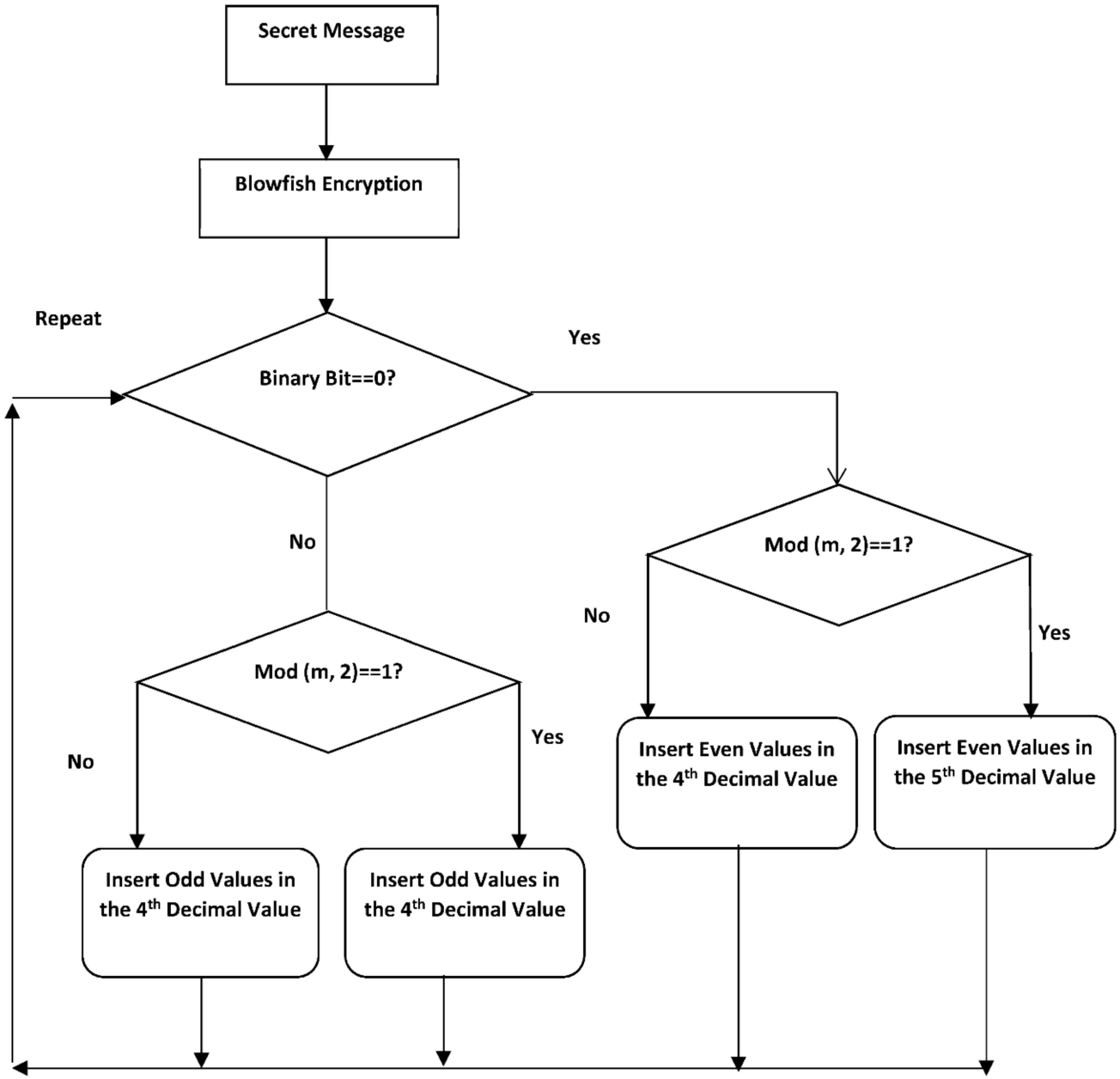

Figure 15. 3D steganography in transform domain using the 3D polygon model [69].

For retrieval of the secret information, the reverse process of concealing was applied. For extraction of secret information, every 4th and 5th bit of the stego file was examined. If

the 4th or 5th bit was found to be an even number that means '0' was extracted from the stego file. In the case that the 4th or 5th bit was calculated as an odd number, that means '1' was the extracted secret information from the stego file. The performance of the research work was calculated with the help of performance metrics. The simulation results proved the high concealing capacity and good visual quality of the research work. The average concealing capacity was found to be 1,249,800 bits, MSE was found to be 0.355×10^{-6} and, the total time taken for the process was found to be 63.7 s [69].

In the paper adaptive 3D steganography has been proposed based on 3D sine chaotic maps as shown in Figure 16. A 3D carrier file of size N × P × K and secure information with size l × m was taken. IWT was applied on a 2D carrier file to decompose it into LL, LH, HL, and HH. The extracted LL sub-band was blocked with 3 phases and divided into 16 × 16 blocks. After that block-wise permutation was done in phase 4, the permuted blocks were put into the matrix. Then in the next phase, the 3D sine chaotic map key was applied to produce random number decimal numbers. The random number generated helps to convert secret information into an integer number. Now in phase 6, the generated integer number was used as a coordinate of the matrix to conceal the secret information. In phase 7, inverse processes were applied to extract the secret information.

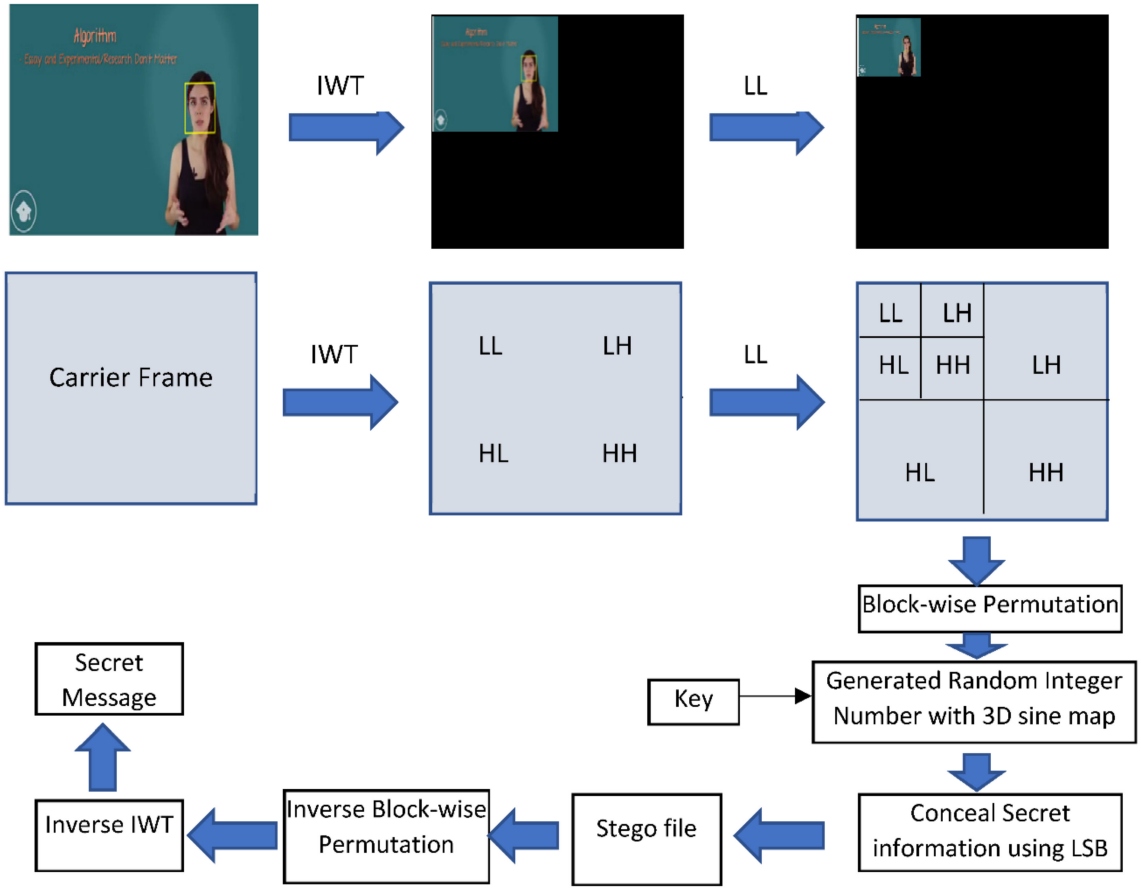

Figure 16. 3D steganography using IWT [70].

To check the performance of the research work, MSE and PSNR were calculated. Different attacks such as rotation, resize, sharpen, blur, Gaussian noise, and many more attacks were also applied. The aforementioned attacks NCC, PSNR, BER, and SSIM were calculated, which were found to be 0.9784, 53.76, 0.0145, and 0.9997 respectively. Histogram and space key analysis were also done to check the quality of research work [70].

Due to the availability of lots of smart devices and internet connections online transmission of secret information is gaining a lot of popularity. Because of the increasing popularity of online transmission of private information security is also become the main

concern these days. 3D image steganography has an opportunity to save secret private information on the web. Information-concealing techniques are divided into compression, frequency, and spatial domain. The 3D turtle shell technique was used in this paper to embed secret data, as shown in Figure 17. Concealing secret information in turtle shells results in great concealing capacity. The quality of the stego file produced was found to be good.

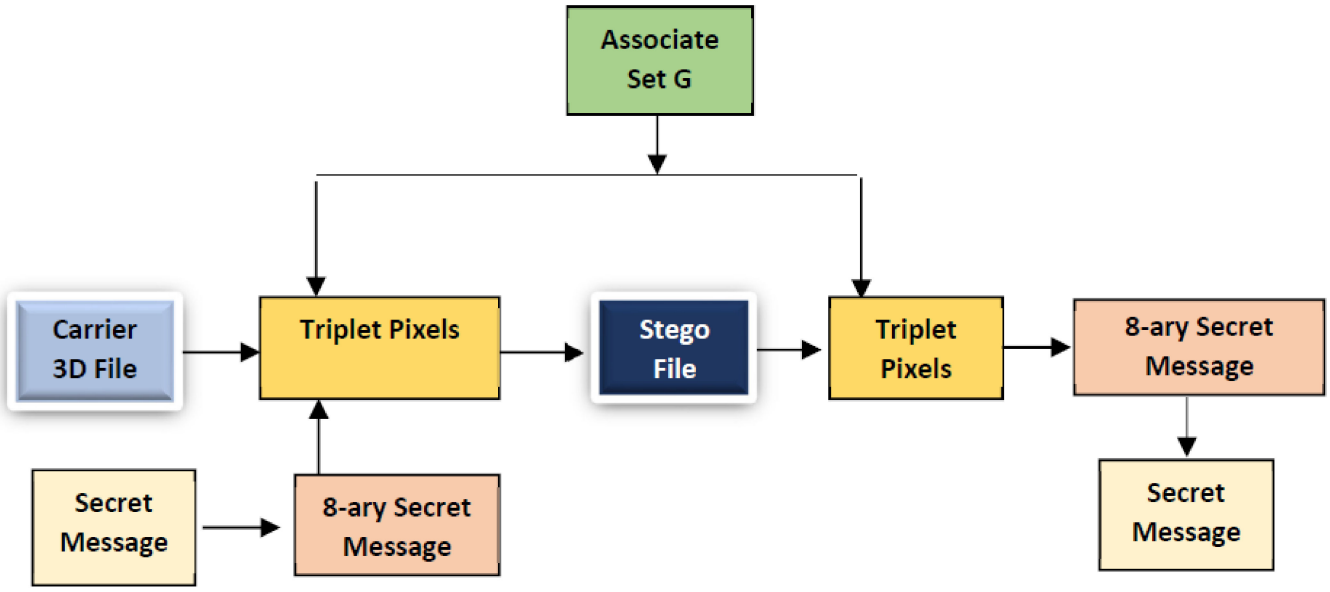

Figure 17. Turtle shell 3D steganography technique [71].

Pixels of 3D carrier files were decomposed into size M × N and secret information was converted into 8-ary secret digits. An M × N matrix, having size 256 × 256, was rearranged consisting of the number of hexagonal objects and these hexagonal objects were known as turtle shells. These turtle shells were divided into special and regular objects. Associated set G was calculated by applying the following three rules. For finding regular elements if M (p_i, p_{i+1}) was a back digit in the turtle shell, then the associated set G will have all digits in the turtle shell. Otherwise, if M (p_i, p_{i+1}) was an edge digit concerned in at least one turtle shell then the associated set G was a group of all digits belonging to the concerned turtle shells. In the case of the special element if M (p_i, p_{i+1}) is not involved in any turtle shell, then associated set G is the group of all digits in its adjacent 3 × 3 submatrices. To conceal the processed 8-ary secret information, grey-level values were chosen from the carrier file pixel pairs.

By applying the abovementioned rules, associated set G was obtained and the cover pair was modified to (p'_i, p'_{i+1}). In the case of multiple solutions, the solution having the shortest distance was selected, which resulted in minor modifications in the carrier file. The abovementioned rule was not suitable for all the cases. These rules were also difficult to design, as in the carrier file a large set of hexagonal objects were produced. It was very difficult to select the same pair of hexagonal objects. For simplification of the mentioned rules, algebraic expressions were applied to find the relationships between neighboring pairs of hexagonal objects. The experiment was performed in MATLAB because of its popularity. Research work was evaluated based on the parameters PSNR, SSIM, concealing capacity, and complexity. The average PSNR value was calculated as 48 dB, average MSE was found to be 0.632, embedding capacity was found to be 1.3 bits/s, and SSIM was found to be 0.9804 [71].

The 3D mesh triangle steganography technique could be applied in the spatial as well as in the transform domain. In spatial domain techniques, bits of carrier file are substituted with the bits of secret message. For concealing secret information, vertices and edges were chosen by the researcher in the mesh triangles as shown in Figure 18. The spatial domain

could be further categorized as geometrical, topological, and representational domains. In the proposed research work, the shortest distance between the adjacent vertices was calculated by applying the Dijkstra algorithm. The algorithm would produce the same traversal path every time. The algorithm was based on the breadth first search and initially, all the vertices were marked unvisited.

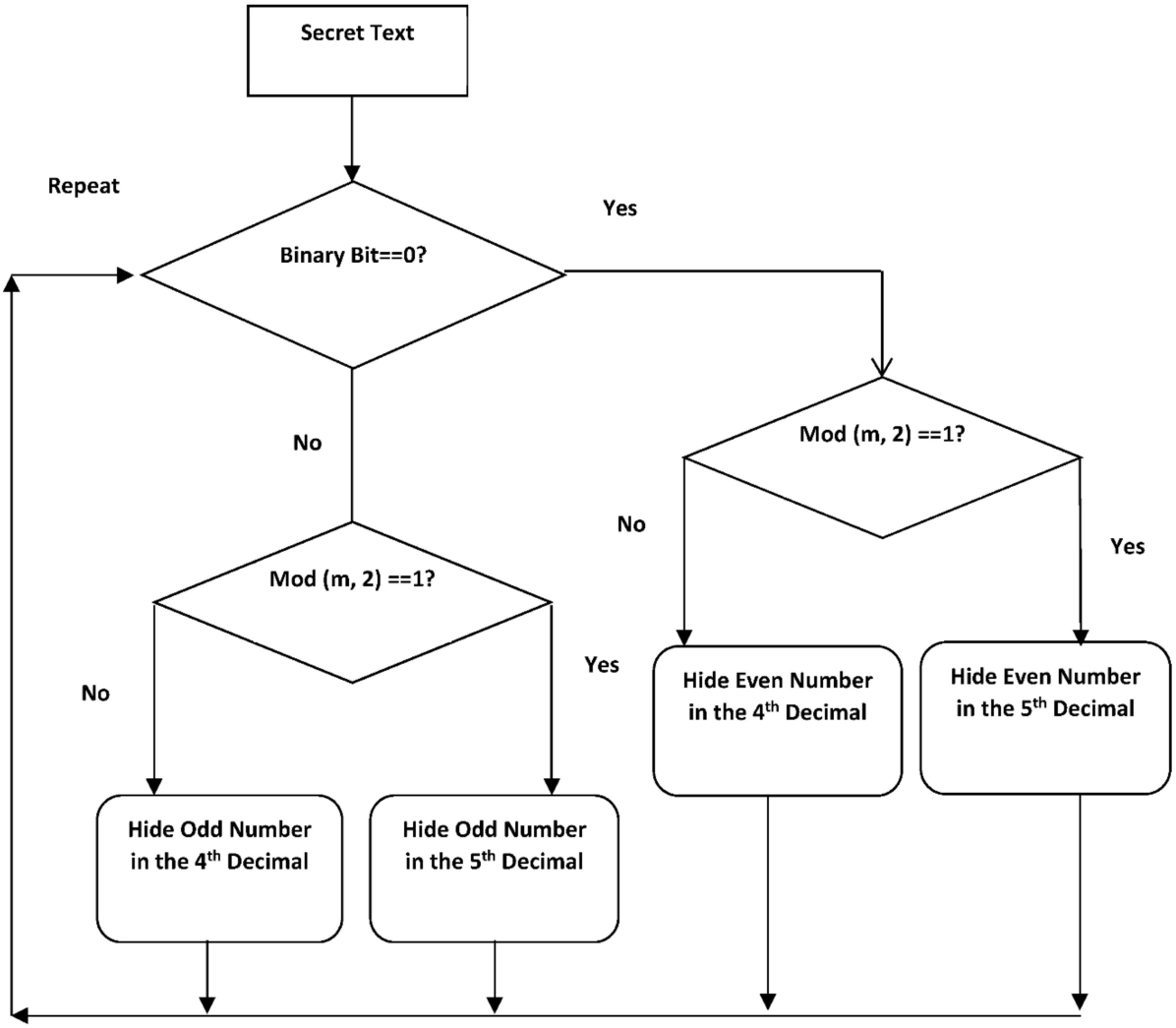

Figure 18. 3D steganography using mesh triangle [72].

The center of gravity of the 3D carrier file was calculated and then the distance between all the vertices was also computed. The vertex having minimum distance from the center was chosen as the source vertex. It was marked as visited in the traversal list. All the remaining adjacent vertices were added to the queue. Again, the distances of all the adjacent vertices were calculated from the chosen vertex. The vertex with the minimum distance was added to the traversal list, and so on—the whole process repeated until all the vertices were traversed. After finding the traversal order for all the vertices, the process of concealing secret information started. The traversal list was then looped back and due to the concealment of secret information, a slight modification in the carrier 3D file takes place.

If the secret information that was to be concealed is '0', then the 4th or 5th digit of a vertex after the decimal was altered by an even number between 1 to 9. Moreover, if the secret information bit that needs to be concealed is '1' then the 4th or 5th bit of the vertex after the decimal was altered by an odd number between 1 to 9. The 3D triangular mesh was then reconstructed using altered vertices and sent to the third party through the web. On the receiver side, a reverse process was performed by the recipient. Again, the traversal

order was calculated by the recipient to extract the secret information. The output of the algorithm was looped back, and the 4th and 5th decimal digits after the decimal point were retrieved. For the retrieved list, every odd number was updated by '1', and every even number was updated by '0'. The performance of the research work was evaluated using concealing capacity, PSNR, MSE, SSIM, and NHD. Average PSNR was calculated as 85.07 dB, MSE was calculated as 1.647×10^{-7}, NHD was calculated as 2.07×10^{22126}, and embedding capacity was calculated as 48,312 bits [72].

3. Analyzing Research Trends in 3D Steganography

For the last two decades, researchers and academicians have been working on 3D carrier files instead of 2D carrier files. The 3D carrier files can be explored in three dimensions because that researcher has more options to conceal secret information. The proposed paper is reviewed: year-wise, based on carrier file, based on the domain in which the secret information is concealed, and evaluation parameters, etc. In the proposed paper, it has been concluded that most of the work was done by researchers on images in the spatial domain. Images are popular in social media these days. Therefore, concealing secret information inside images can be delivered to the destination without the knowledge of any third party.

3.1. Research Papers Publications Year Wise

Figure 19 shows the papers published in a year. The maximum number of papers reviewed belongs to the year 2018. The minimum numbers of papers reviewed are from the years 2012, 2014, and 2021. All the papers reviewed carry some pros and cons associated with them, as discussed in Table 1 also.

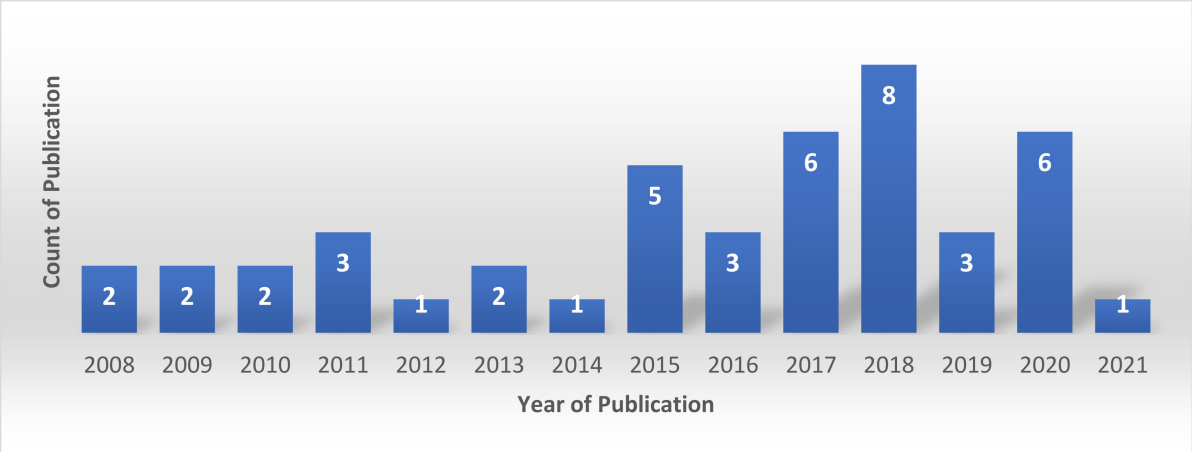

Figure 19. Count of publications (year-wise).

3.2. Choosing the Type of Carrier File

Figure 20 shows the number of papers reviewed, based on the carrier file used. Text and audio steganography techniques are the least used by researchers. These techniques have low concealing capacity, less imperceptibility, and are not robust against attacks. Image and video steganography techniques ensure no detection of secret information to the hackers. Because of their large concealing capacity and good visual quality of stego files, these techniques are most commonly used by the researchers.

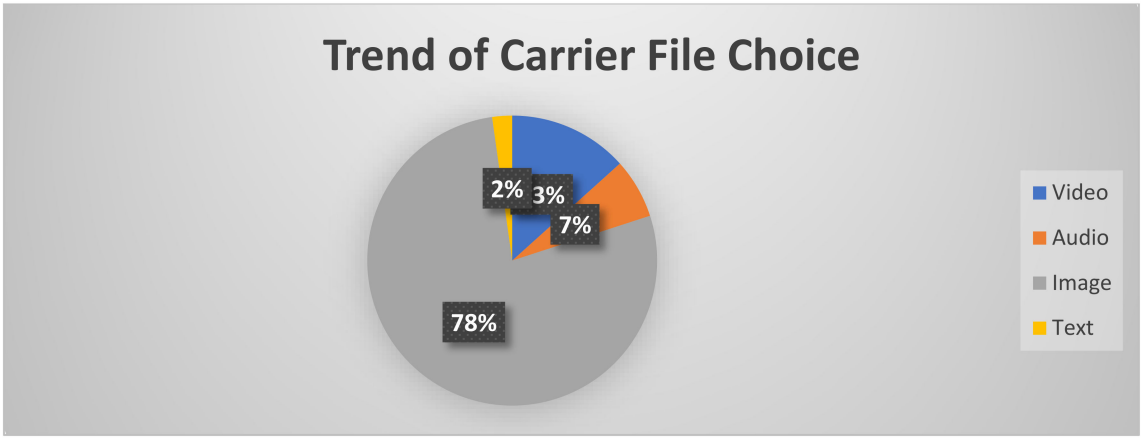

Figure 20. Types of carrier file used.

3.3. Attainment of Evaluation Parameters

Figure 21 represents the review of papers based on the evaluation parameters. Evaluation parameters include PSNR, MSE, SSIM, NCC, CC, NHD, MSSIM, entropy, histogram, MAE, and many more. All these parameters help to find the quality of the work. Quality of research work can be measured in terms of concealing capacity, imperceptibility, and robustness against attacks. Concealing capacity is the amount of secret data that can be concealed in a carrier file. Imperceptibility is the visual quality of the stego file—high imperceptibility means less chance of detection of secret information. Robustness is the ability of the stego file to avoid exposure of secret information against different types of attacks.

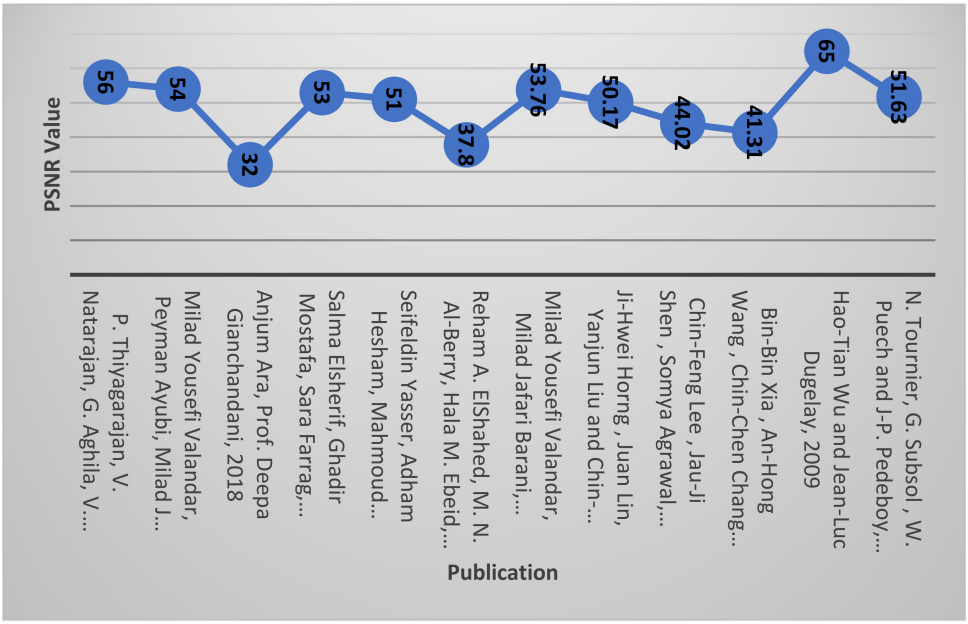

Figure 21. PSNR analysis.

Figure 21 shows the PSNR values of the paper studied. PSNR analyzes the visual quality of the 3D stego file.

PSNR values greater than 30 dB mean that the stego files have good visual quality. The higher the value of PSNR, the lower is the chance of detection of the secret information. PSNR measures the imperceptibility as well as the robustness of the stego file.

Figure 22 shows the graph for the MSE values for the papers reviewed. MSE represents the error present between the original and stego carrier file. The lower the value of MSE,

the lower is the chance of detection of the secret information. So, it is also used to measure the quality of the stego file as well as robustness against different types of signal-processing attacks.

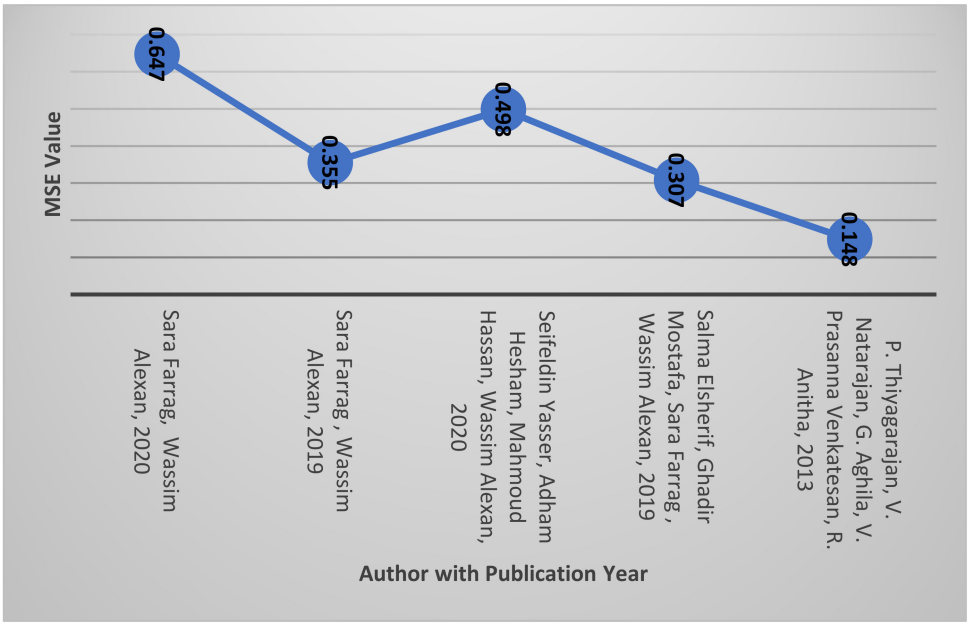

Figure 22. MSE analysis.

Figure 23 represents the value of SSIM for the various papers reviewed. SSIM compares the structure of the original and the stego file to find the dissimilarity.

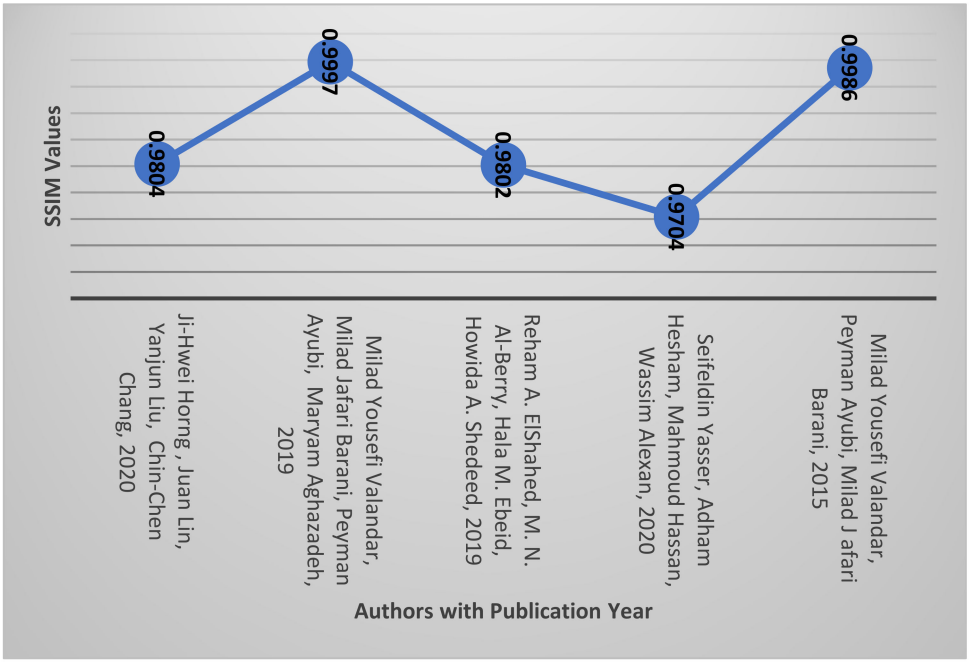

Figure 23. SSIM Analysis.

The value of SSIM varies between 0 and 1. A value of 1 represents very good quality of a 3D stego file, and 0 signifies poor quality. SSIM performs better than both MSE and PSNR in terms of quality checking. SSIM can efficiently check the quality and robustness of the stego file. Figure 24 represents the amount of secret information concealed for the reviewed papers. Concealing capacity is the amount of secret information that can be

concealed in the cover file without the knowledge of a third party. It is measured in the number of secret bits concealed per unit of time. On concealing a large amount of secret information, imperceptibility as well robustness can become compromised, resulting in exposure of the secret information.

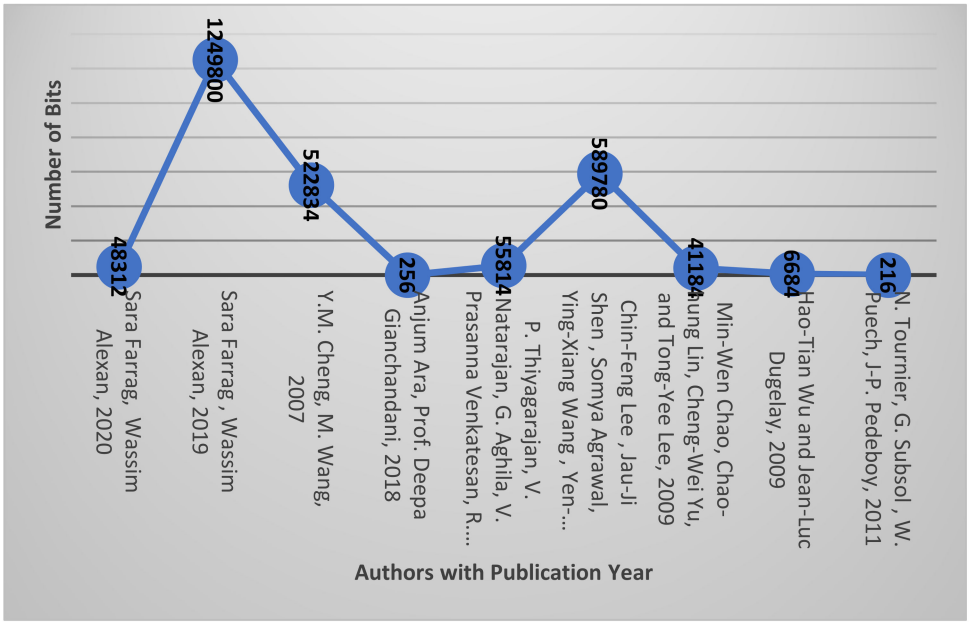

Figure 24. Analysis of concealing capacity.

Figure 25 shows the total time taken by the technique for concealment and retrieval of the secret information. Concealing time is the amount of time required to hide the secret information in the 3D cover file. Retrieval time is the amount of time required to retrieve the secret information from the 3D stego file. Some of the reviewed techniques performed very well in terms of time.

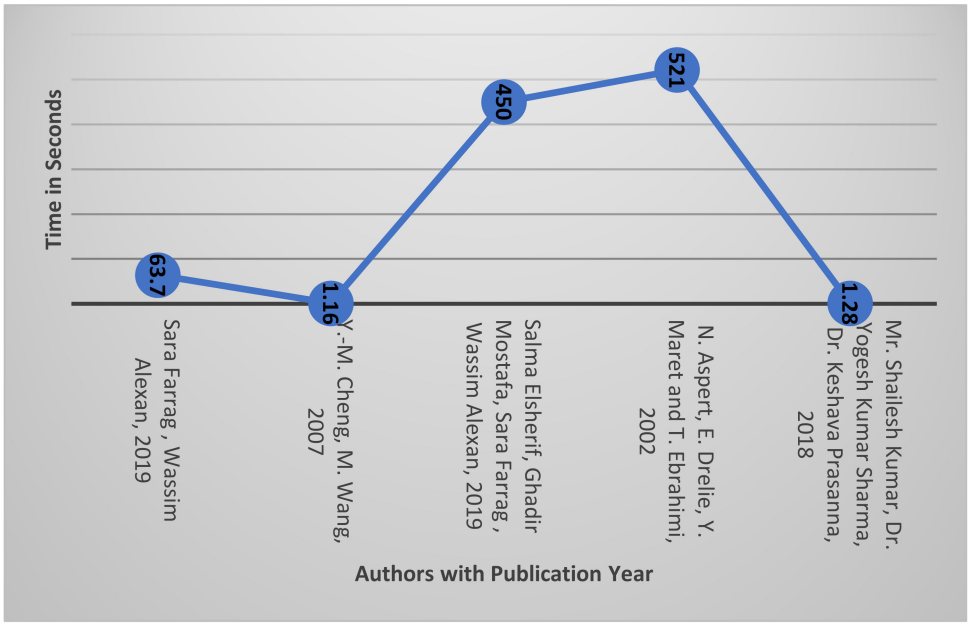

Figure 25. Concealment and retrieval time analysis.

3.4. 3D Steganography Technology Preferences

The relevant literature on 3D steganography from the year 2008 to 2021 has been considered for analysis. The researchers have explored different techniques of varying nature to implement 3D steganography in different domains. The intention of achieving high capacity and greater robustness has also led to interdisciplinary work. In this section, the research work done in the aforesaid duration is categorized on the basis of the steganography methods being focused on. Table 1 summarizes the work done based on LSB techniques and their modified versions. Being simple to implement and easy to understand, LSB remained the preferred choice of researchers to implement 3D steganography. Similarly, Table 2 lists the work based on 3D polygon methods; whereas Table 3 summarizes the 3D steganography work that exploited DCT or wavelet transforms. Table 4 discusses the basic features and additional security provisions in 3D steganography research based on different 3D models. Table 5 enlists the other techniques that could not be placed in the first three tables.

Table 1. 3D steganography using LSB and its variants.

Publication	Author, Year	Additional Technique	Method Used	Key Features
High Secure Digital Image Steganography Based On 3D Chaotic Map [59]	Milad Yousefi Valandar, Peyman Ayubi, and Milad Jafari Barani, 2015	Chaotic Map, JPEG Compression	LSB	Chaotic maps were used by the authors to conceal secret data inside 3D images. Three variables were used to find the pixel positions for concealing secret information. The RGB model was used for the color image, which acts as a carrier. The key used in this paper determines the robustness of the proposed work.
MLSB-Technique-Based 3D Image Steganography Using AES Algorithm [60]	Nandhini, Nivetha, Nirmala, and Poornima, 2016	AES	Modified LSB	Modified least significant bit (MLSB) was used to conceal secret information in 3D images. The concealing capacity of the technique was found to be large as compared to LSB. AES encryption was used for additional security.
Hiding of Text in a 3D Image Ising Steganography [73]	Chandraleka, Ankita Singh, and Astha Mehta, 2017	RSA, MD5	LSB	For encryption, the RSA algorithm along with MD5 was used. LSB conceals encrypted secret information in the carrier file. The concealing capacity of the research work was found to be very high but at the same time, imperceptibility got compromised.
Study of 3D Barcode with Steganography for Data Hiding [74]	Megha S M, and Chethana, 2018	Encryption	LSB on 3D bar codes	The carrier file changed from 3D images to 3D barcodes for concealing secret information. In bar codes, the third dimension acts as the color component. Encryption was applied to the secret data first to provide a double level of security. Then the encrypted data was concealed inside 3D bar codes.
An Efficient Approach Based on 3D Image Steganography for Security of Visual Contents [75]	Navendu Kumar and Dr. Deepak Kourav, 2018	Pseudorandom number generator	LSB	Experimental results showed that 256 bits of secret data could be concealed inside the carrier without degrading the visual quality of 3D images.

Table 1. *Cont.*

Publication	Author, Year	Additional Technique	Method Used	Key Features
A Hybrid Approach Based on 3D Image Steganography Instead of 2D Image for Exchange Information [61]	Anjum Ara and Deepa Gianchandani, 2018	Encryption	LSB	The proposed technique was able to conceal 256 bits of secret data into random bits of carrier file without affecting the quality of the stego file. The proposed technique was robust against scaling, rotation, cropping, and translation attacks.
Secure Message Embedding in 3D Images [63]	Salma Elsherif, Ghadir Mostafa, Sara Farrag, and Wassim Alexan, 2019	AES-128	LSB	The AES-128 encryption technique was applied to secret information. Scrambled secret information was concealed using the LSB technique in 3D images.
AES-Secured Bit-Cycling Steganography in Sliced 3D Images [64]	Seifeldin Yasser, AdhamHesham, Mahmoud Hassan and Wassim Alexan, 2020	AES Encryption	LSB	AES encryption scrambled secret information, and then this converted secret information was concealed by using LSB techniques.
A Comparative Study Among Different Mathematical Sequences in 3D Image Steganography [76]	Wassim Alexan, Mazen El Beheiry and Omar Gamal–Eldin, 2020	AES-128	LSB	The encrypted secret information was concealed using LSB substitution. The experiment was done to calculate image fidelity, image distance, normalized cross-correlation (NCC), PSNR, MSE, mean structural similarity index measurement (MSSIM), and etc.

Table 2. 3D steganography using the 3D polygon technique.

Publication	Author, Year	Additional Technique	Method Used	Key Features
An Adaptive Steganographic Algorithm for 3D Polygonal Meshes [66]	Yu-Ming Cheng and Chung-Ming Wang, 2008	-	3D Polygonal Meshes	The secret information was concealed inside a 3D polygon mesh. The authors calculated the correlation between neighboring polygons to find the smoothness. Rough surfaces were capable of storing a great amount of secret data as well as being robust against attacks.
A High-Capacity 3D Steganography Algorithm [77]	Min-Wen Chao, Chao-hung Lin, Cheng-Wei Lu, and Tong-Yee Lee, 2009	-	3D Polygon Model	The number of layers was used to hide secret information. The simulation proved that the proposed technique performs better with a large number of layers in the carrier file. The number of layers explored in the mentioned paper varies from 9 to 13.
A Novel High-Capacity 3D Steganographic Algorithm [78]	Meng-Tsan Li, Nien-Ching Huang and Chung-Ming Wang, 2011	-	3D Polygon Model	A total 9.6 million bits of secret data were concealed inside 14004 vertices of the 3D polygon model. Secret information was concealed in two steps. At first, the secret information was divided into many parts, then these parts of secret information were encoded using a random model produced on a unit sphere. In the second step, encoded information was concealed on the surface of the 3D polygon model.

Table 2. *Cont.*

Publication	Author, Year	Additional Technique	Method Used	Key Features
A High-Capacity Geometrical Domain-Based 3D Image Steganography Scheme [69]	Sara Farrag and WassimAlexan, 2019	Blowfish Encryption	3D Polygon Model	Blowfish encryption was applied to secret information to convert it into scrambled form. A 3D polygon was used to conceal the secret information by using triangular meshes. The proposed work was robust against scaling, translation, cropping, clipping, etc.

Table 3. 3D steganography using DCT/WT.

Publication	Author, Year	Additional Technique	Method Used	Key Features
3D Data Hiding for Enhancement and Indexation on Multimedia Medical Data [2]	Tournier, Subsol, Puech and Pedeboy, 2011	-	DCT-DWT	Sensitive patient information was concealed inside 3D images. The transform domain was used by the authors to hide secret information.
A 3D Video Watermark Embedding Technology in DCT-CS Domain [79]	Longfei Cai, Huimin Zhao, Jun Cai, and Li Zhu, 2015	-	DCT-CS Domain	The DCT-CS (discrete cosine transform-compressed sensing) technique was applied to the 3D video to conceal the secret information. Secret information was taken as fingerprint images.
Combining and Steganography of 3D Face Textures [80]	Mohsen Moradi and Mohammad-Reza Rafsanjani-Sadeghi, 2017	-	DWT, SVD	The 3D image steganography was implemented using the DWT-SVD technique. Faces in 3D were chosen for hiding secret information. As human faces have most of the useful information in low-frequency components and high-frequency components, they could be used for embedding secret information. Face texture was examined by the author and then in that texture, secret data was hidden.
Video Steganography using 3D Stationary Wavelet Transform [67]	El-Shahed, Al-Berry, and Ebeid, Shedeed, 2018	-	3D Stationary Wavelet Transform	The 3D Stationary Wavelet Transform (SWT) technique was used for concealing secret data into video frames. The performance of the proposed work was tested on different formats of video files as well as different formats of secret data. The PSNR value of the proposed work was calculated as 40 db.

Table 4. 3D steganography using different 3D models.

Publication	Author, Year	Additional Technique	Method Used	Key Features
An Image Steganography Scheme Using 3D-Sudoku [81]	Bin-Bin Xia, An-Hong Wang, Chin-Chen Chang, and Li Liu, 2016	-	3D-Sudoku	The carrier file is used in the form of 3D sudoku. A cyclic moving algorithm was applied to build the 3D sudoku. On concealing secret information inside the carrier of 3D sudoku, some bits are modified. These modified bits of the coordinated sudoku were then used to extract the secret data.

Table 4. *Cont.*

Publication	Author, Year	Additional Technique	Method Used	Key Features
A High-Capacity 3D Steganography Algorithm With Adjustable Distortion [56]	Nannan Li, JiangbeiHu, Riming Sun, Shengfa Wang and Zhongxuan Luo, 2017	-	3D Model	For concealing secret information, the author used a shifting strategy that results in low distortion. Depending upon the value of the threshold, the amount of secret information that can be concealed was calculated.
Rethinking the High-Capacity 3D Steganography: Increasing its Resistance to Steganalysis [82]	Zhenyu Li, Sebastien Beugnon, William Puech, and Adrian Bors, 2017	-	3D Model	Hamiltonian path quantization was applied on 3D images to conceal secret information. The proposed technique was robust enough for different signal-processing attacks.
Data Hiding Method Based on 3D Magic Cube [83]	Chin Feng Lee, Jau-Ji Shen, Somya Agrawal, Ying-Xiang Wang, and Yen-His Lee, 2020	-	3D Magic Cube	A magic cube technique was applied to embed the secret data in the proposed paper. In 4 pixels, 9 bits of secret information were embedded by the authors. A secret key was also used to improve the security against different attacks. Concealing capacity was calculated as 2.25 bpp and PSNR as 44 dB for the research work.
3D Multilayered Turtle Shell Models for Image Steganography [71]	Ji-Hwei Horng, Juan Lin, Yanjun Liu and Chin-Chen Chang, 2020	-	3D Turtle Shell Model	A new model named 3D turtle shell models was used by the author to conceal the secret information. Quality of work was checked with the help of performance metrics PSNR and SSIM.
Secure 3D Data-Hiding Technique Based on a Mesh Traversal Algorithm [72]	Sara Farrag and Wassim Alexan, 2020	-	3D Mesh Model	Reversible data concealing can separate both carrier and secret information at the receiver side. A 3D mesh model was used to conceal secret information using a traversal algorithm. Based on the distance between neighbor vertices, secret information was concealed in the proposed paper. The smaller the distance between vertices, the lower the chance of detection of the secret information.

Table 5. 3D steganography using miscellaneous approaches.

Publication	Author, Year	Additional Technique	Method Used	Key Features
3D Steganography Models [57]	Mihai Dupac and Nicolae Constantinescu, 2008	Symmetric Encryption	Grayscale Height Map	Symmetric encryption along with steganography in a grayscale height map was proposed.
Steganography in 3D Geometries and Images by Adjacent Bin Mapping [84]	Hao-Tian Wu and Jean-Luc Dugelay, 2009	-	Adjacent Bin Mapping	Secret information was concealed in 3D shapes by mapping the coordinates of two adjacent bins in pseudorandom order. The quality of the stego file was measured by histogram tail. The simulation of the work showed that high-order statistics of the carrier file were conserved, while small disturbance was observed.

Table 5. *Cont.*

Publication	Author, Year	Additional Technique	Method Used	Key Features
Lossless 3D Steganography Based on MST and Connectivity Modification [85]	Pamat, Puech, Druon, and Pedeboy, 2010	-	Minimum Spanning Tree	A minimum spanning tree was used to conceal secret information. The 3D images allow information concealment without shifting the location of vertices in the three dimensions. The concealing of secret information was done by altering the connectivity of boundaries in the particular areas built of quadruples. After concealing the secret information, the boundaries of the object are seen to be the same.
Mesh Discriminative Features for 3D Steganalysis [86]	Ying Yang and Ioannis Ivrissimtzis, 2013	-	Supervised Learning	Triangle meshes were used in this work to conceal the secret information; supervised learning was applied on triangle meshes with the help of discriminative feature vectors.
Pattern-Based 3D Image Steganography [58]	Thiyagarajan, Natarajan, Aghila, and Prasanna Venkatesan Anitha, 2013	-	Pattern-based Triangle Mesh Algorithm in Spatial Domain	An adaptive 3D symmetrical model was proposed by the authors on triangle meshes. The first triangle mesh was reconstructed using the proposed algorithm, which works in the spatial domain on patterns of 3D images. In the modified triangle meshes, up to 9 bits of secret data were concealed.
Automatic Conversion of Image and Video from 2D to 3D with Steganographic Data Hiding in Converted 3D Image [62]	Sariga N P, and Sajitha A S, 2015	-	Global Nearest-Neighbor Depth Learning	The 3D video was converted into images. Then these converted images were used to hide the secret data. For the conversion procedure, the global nearest-neighbor technique was used. LSB was used to hide the secret data inside converted 3D images.
Information Steganography within 3D Images Using Residue Number System [87]	Azin Azizifard, Mohammad Qermezkon, and Reza Farshidi, 2015	-	Residue Number System	Information concealing was done using the residue number system (RNS). RNS represents integer numbers by their modulo co-prime pairs. Then, 3D images provide more detail to conceal the secret information.
A 3D Steganalytic Algorithm and Steganalysis-Resistant Watermarking [88]	Ying Yang, Ruggero Pintus, Holly Rushmeier and Ioannis Ivrissimtzis, 2016	-	Gaussian distribution	Proposed research work was done by exploring the Gaussian distribution. The mean and variance of the watermark and original carrier image were calculated to measure the quality of the proposed research work. T-test and histogram analysis was also done to check the visual quality as well as robustness of the work.
3D Steganography using the Extended Local Feature Set [89]	ZhenyuLi, DaofuGong, Fenlin Liu, and Adrian G. Bors, 2017	-	Extended Local Features Set	The research work proposed 3D steganography using edge vectors. Cartesian and Laplacian coordinate systems were used to calculate the suitable region for concealing secret information.
Distortion Design for Secure Adaptive 3D Mesh Steganography [90]	Hang Zhou, Kejiang Chen, Weiming Zhang, Yuanzhi Yao and Nenghai Yu, 2018	-	Syndrome Trellis Codes	In this research work, the author concealed secret information in a non-adaptive way that is robust against attacks rather than in 3D meshes. By using syndrome trellis codes (STCs), local areas of vertices were calculated and then secret information was concealed.

Table 5. *Cont.*

Publication	Author, Year	Additional Technique	Method Used	Key Features
A Novel Method of Speech Information Hiding Based on 3DMagic Matrix [68]	Zhong-Liang Yang, Xue-Shun Peng, Yong-Feng Huang and Chin-Chen Chang, 2018	-	Line Spectrum Pair	Audio steganography on the 3D magic matrix was performed by using a line spectrum pair (LSP) of the inaudible frequency. Redundant data bits of low inaudible frequencies were chosen for concealing secret information. LPS works on several vector quantization features of audio.
An Integer Wavelet Transform Image Steganography Method Based on 3D Sine Chaotic Map [70]	Milad Yousefi Valandar, Milad Jafari Barani, Peyman Ayubi, and Maryam Aghazadeh, 2019	-	3D Sine Chaotic Map	3D steganography was performed by authors using a sine chaotic map. Sine chaotic map calculates the secret key for finding the suitable region of interest. Every time, a new key was generated to find the region of interest. Randomness improves the security of the proposed work.

The various works discussed here reveals that researchers have not relied upon 3D steganography solely; rather employed additional layers of security such as encryption, etc. Figure 26 shows that LSB is the preferred technology for implementing 3D steganography over other types of steganography.

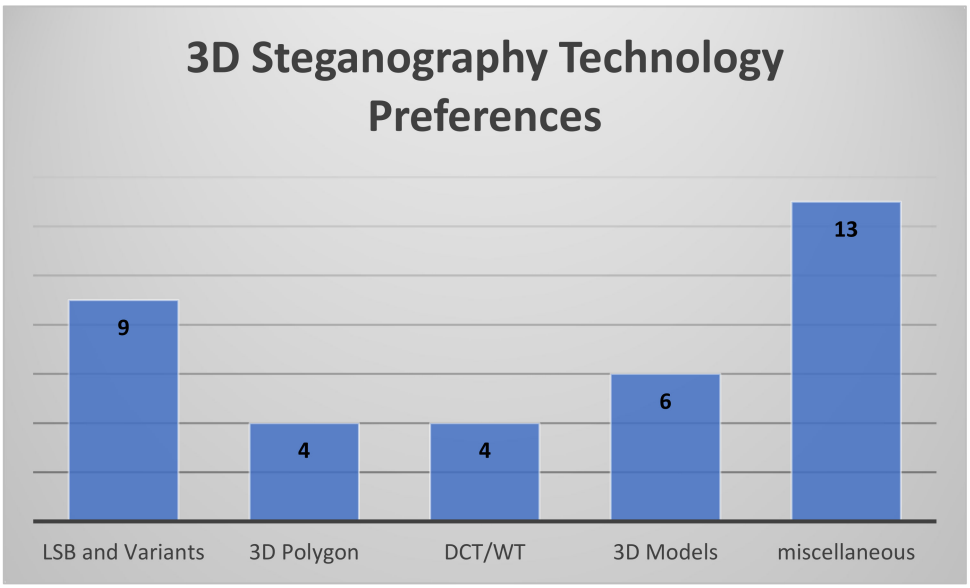

Figure 26. 3D steganography technology preferences.

4. Steganalysis of 3D Steganography

3D steganalysis uses machine-learning algorithms to distinguish stego files from carrier files. These techniques carry out many training and testing phases to expose secret information. These techniques came into existence in the late 2010s. After that, many different and more robust 3D steganalysis techniques have been implemented by researchers. The objective of these techniques is to gather adequate evidence for the existence of concealed information to break the security [91]. These techniques have many applications in computer forensics, cyber warfare, tracking criminal activities on the web, and assembly evidence for investigations specifically in the case of antisocial elements [92]. These techniques also improve the security of 3D steganography techniques and tools by assessing and recognizing their weaknesses.

3D mesh steganalysis techniques find the set of vertices and local curvature for exposure of secret information. In this technique, the first disturbance needs to be calculated. Disturbances can be calculated in terms of mean, inconsistency, skewness, and kurtosis. Both the original 3D cover and the stego file are compared to find the mismatch or disturbance among the two files. Then a machine classifier can be used to find the statistical properties of the two files. The quadratic discriminator and the FLD ensembles are finally applied to identify whether secret data was embedded in a 3D cover file or not [93]. It is very challenging for 3D steganalysis to find hidden secret information. For exposure of secret information, steganalysis techniques work on very small changes in 3D original and stego files. A variety of local features are analyzed to find the difference between the two files. The statistical properties of both files are checked with the help of experiments, such as machine learning algorithms. These algorithms include quadratic discriminate, Fisher linear discriminate (FLD) ensemble, and the support vector machine (SVM). These machine-learning algorithms train the data set and analyze the statistical properties to find the differences between two files [94].

3D steganalysis techniques are mainly divided into signature steganalysis and statistical steganalysis. This categorization is created based on whether the signature of the 3D steganography technique or the statistics of the image are used to perceive the existence of concealed information in the carrier file. Based on these two properties of carrier files, these techniques are future divided into subparts [95]. The categorization of 3D steganalysis techniques is given in Figure 27. 3D steganalysis provides two main types of analysis: visual analysis and statistical analysis. Visual analysis detects secret information with human eyes or through the computer in which bit planes of carrier files are analyzed independently for any uncommon alteration in appearance that could signify the existence of secret information.

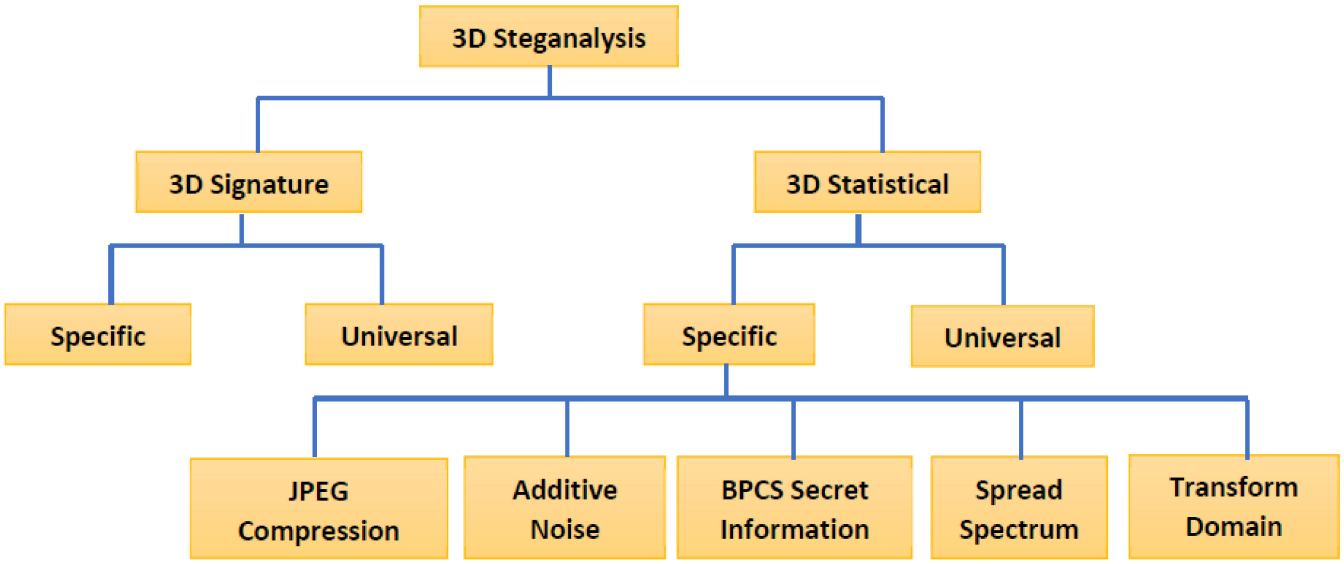

Figure 27. Categorization of 3D steganalysis techniques [96].

The statistical analysis deals with the detection of alteration in statistical features of the stego file initiated by steganography techniques. Steganalysis can also be divided into universal and specific steganalysis techniques. Universal steganalysis techniques can detect secret information in stego files concealed by any steganography technique and specific steganalysis techniques are complex techniques and work with some specific steganography techniques.

4.1. 3D Signature Steganalysis

Concealing secret information inside any digital media using the 3D steganography technique involves variations in media properties that might introduce unusual appear-

ances, degradation in carrier files, and patterns. These unusual appearances might act as signatures to detect the existence of concealed information. Attacks on these anomalies are simple and provide good results when the secret information is concealed successively. It is hard to detect secret information when it is concealed in video frames taking random locations [97].

- Universal steganalysis: This technique can find the concealed information embedded through any of the 3D steganography techniques. Spatial domain steganography techniques are easily detected by steganalysis techniques. But secret information concealed through the transform domain steganography technique is more robust and difficult to detect by steganalysis technique.
- Specific steganalysis: These techniques are designed for some specific steganography techniques. Stego images created through steganography techniques are compared by taking their histogram. When histograms generated for original and stego images are not the same, then chances of detection of secret information increase.

4.2. 3D Statistical Steganalysis

Steganography conceals secret information in any type of digital carrier. The statistics of the carrier file may be altered because of information concealing. The 3D statistical steganalysis method analyzes these altered statistics of carrier files for detecting the secret concealed information. This steganalysis is found to be more powerful than signature steganalysis. These techniques are evaluated mathematically, and mathematical calculations are more accurate as compared to visual perception [98].

- **BPCS steganography steganalysis:** This technique is efficient to identify the presence of secret information in the carrier file. It can easily identify secret information in both spatial and transform domains. It is concluded that a statistical characteristic known as isotropy is modified after concealing secret information through BPCS-steganography. This modification is known as steganalysis. Histograms, the Chi-square test, entropy, correlation coefficient, MSE, and hypothesis, etc., are used to detect the presence of secret information [99].
- **JPEG compression steganalysis:** Because of their ideal characteristics, JPEG images are extensively used on the internet, so they are also used in most of the 3D steganography techniques for concealing secret information. When secret information is concealed using the DCT technique, it is found that the quantized DCT coefficients of JPEG images allocate evenly in zeros in carrier images. Chi-square measurements of the stego image are produced and a variation equation is applied to conclude the existence of secret information [100].
- **Transform domain steganalysis:** From histogram exploration, it is concluded that the histogram of the carrier image is flatter than the stego image. A stego image is quantitatively analyzed by its spectrum and energy difference with that of the carrier image. From this experiment, it is concluded that the energy difference for stego images is greater than carrier images. The threshold value is also calculated to check whether secret information exists or not [101].
- **Additive noise steganalysis:** This is a 3D steganalysis scheme of binary images, which are concealed by reversing pixels with boundaries. This steganalysis scheme depends on the correlation between compression rate and information concealing rate. As and when more secret information is concealed inside the carrier image, more compression is required. This compression rate is then used for differentiating the statistical properties of carrier and stego images [102].
- **Spread spectrum steganalysis:** When secret information is concealed using a spread spectrum then this 3D steganalysis technique is used to find the existence of secret information. The carrier image is initially re-established using a spatial filter. After that spread, the spectrum procedure is applied on the carrier image many times and modification of low-frequency coefficients in every DCT block is assessed. The same

procedure is used on a stego image with its modifications produced. The differences between these two images detects the existence of secret information [103–106].

5. Observations and Findings

The study of relevant literature on 3D steganography in approximately the past 15 years has laid down certain interesting observations. These points are helpful for future research in this domain. The observations are listed as follows:

- Image file remained the preferred choice for cover file in most of the research work. The scope of exploring other types of multimedia files as cover in 3D steganography is still open.
- Most of the researchers relied upon conventional cryptography techniques for additional security. It adds to the computational requirement of the method.
- The PSNR attainment in 3D steganography is lesser as compared to image and video steganography. It shows the further scope of improvement as PSNR is a measure of robustness, which is an essential requirement of steganography.
- An attempt to increase embedding capacity results in compromised robustness as witnessed from MSE and PSNR attainments. A balance between these two parameters remains an open question.
- Majority of the research utilized LSB or its variants to implement 3D steganography. However, there are many other techniques of steganography with their inherent benefits that are unexplored in this context.
- People have started using machine learning in 3D steganography; however, its use is still in the infancy period.

6. Conclusions

A systematic study of 3D steganography techniques has been carried out. The study reveals that 3D steganography is dominantly implemented in the transform domain, where robustness was the prime objective; however, the spatial domain 3D steganography techniques dominated to achieve high capacity. LSB technique was dominantly used as the main embedding algorithm. A lot of attempts using hybrid approaches have also been done to improve the robustness; however, the capacity remained a question there. Most of the researchers have used an image as a cover file and very few go for audio and video. Spatial domain techniques are found to be less complex as compared to transform domain techniques, but they are easy to detect comparatively. Steganalysis can be done based on various properties such as histogram analysis, entropy change, changes in the statistical properties of the image, compression rate, change in the format of image and threshold value of the image, etc. Many steganalysis tools also exist that can detect the presence of secret information but not the contents. There is a scope of future research in this domain to find the balance among complexity, robustness, and capacity.

Author Contributions: Methodology, R.T.; Investigation, U.P.; Validation, M.Z.; Writing—review & editing, A.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rana, M.; Tanwar, R. Genetic Algorithm in Audio Steganography. *Int. J. Eng. Trends Technol.* **2014**, *13*, 29–34. [CrossRef]
2. Tournier, N.; Subsol, G.; Puech, W.; Pedeboy, J.-P. 3D Data Hiding for Enhancement and Indexation on Multimedia Medical Data. In Proceedings of the 2nd International Workshop on Medical Image Analysis and Description for Diagnosis Systems, Rome, Italy, 28–29 January 2011; pp. 43–51. [CrossRef]
3. Huang, H.Y.; Yang, C.H.; Hsu, W.H. A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation. *IEEE Trans. Inf. Forensics Secur.* **2021**, *5*, 625–637. [CrossRef]
4. Aspert, N.; Drelie, E.; Maret, Y.; Ebrahimi, T. Steganography for Three-Dimensional Polygonal Meshes. *Int. Symp. Opt. Sci. Technol.* **2002**, *4790*, 211–219. [CrossRef]

5. Girdhar, A.; Kumar, V. Comprehensive survey of 3D image steganography techniques. *IET Image Process.* **2018**, *12*, 1–10. [CrossRef]
6. Zamani, M.; Manaf, A.B.A. Genetic algorithm for fragile audio watermarking. *Telecommun. Syst.* **2015**, *59*, 291–304. [CrossRef]
7. Chaeikar, S.S.; Zamani, M.; Manaf, A.B.A.; Zeki, A.M. PSW statistical LSB image steganalysis. *Multimed. Tools Appl.* **2018**, *77*, 1–31. [CrossRef]
8. Zamani, M.; Manaf, A.A.; Ahmad, R. Current Problems of Substitution Technique of Audio Steganography. In Proceedings of the International Conference on Artificial Intelligence and Pattern Recognition, Orlando, FL, USA, 13–16 July 2009.
9. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Wide Smooth Region Photos Statistical Steganalysis. *J. Next Gener. Inf. Technol.* **2013**, *4*, 43–56.
10. Zamani, M.; Manaf, A.A.; Ahmad, R. Genetic Algorithm as an Approach to Resolve the Problems of Substitution Techniques of Audio Steganography. In Proceedings of the International Conference on Genetic and Evolutionary Methods, Las Vegas, NV, USA, 13–16 July 2009.
11. Araghi, T.K.; Manaf, A.B.A.; Zamani, M.; Araghi, S.K. A Survey on Digital Image Watermarking Techniques in Spatial and Transform Domains. *Int. J. Adv. Image Process. Tech.* **2016**, *3*, 6–10.
12. Zamani, M.; Manaf, A.A.; Ahmad, R. Knots of Substitution Techniques of Audio Steganography. In Proceedings of the International Conference on Telecom Technology and Applications, Manila, Philippines, 6–8 June 2009.
13. Arab, F.; Abdullah, S.M.; Hashim, S.Z.M.; Manaf, A.A.; Zamani, M. A robust video watermarking technique for the tamper detection of surveillance systems. *Multimed. Tools Appl.* **2016**, *75*, 10855–10885. [CrossRef]
14. Zamani, M.; Manaf, A.A.; Ahmad, R.; Jaryani, F.; Taherdoost, H.; Zeki, A. A Secure Audio Steganography Approach. In Proceedings of the 4th International Conference for Internet Technology and Secured Transactions, London, UK, 9–12 November 2009.
15. Arab, F.; Zamani, M. VW16E: A Robust Video Watermarking Technique Using Simulated Blocks. In *Multimedia Forensics and Security*; Springer: Berlin/Heidelberg, Germany, 2017; Volume 115, pp. 193–221.
16. Zamani, M.; Manaf, A.A.; Ahmad, R.; Zeki, A.; Abdullah, S. A Genetic-Algorithm-Based Approach for Audio Steganography. *World Acad. Sci. Eng. Technol.* **2009**, *30*, 355–358.
17. Arab, F.; Zamani, M. VW16F: A Robust Video Watermarking Using Simulated Block Based Spatial Domain Technique. In Proceedings of the International Conference on Security and Management, Athens, Greece, 12–15 July 2018.
18. Zamani, M.; Manaf, A.A.; Ahmad, R.; Zeki, A.; Magalingam, P. A Novel Approach for Audio Watermarking. In Proceedings of the Fifth International Conference on Information Assurance and Security, Xian, China, 18–20 August 2009.
19. Abdullah, S.; Manaf, A.A.; Zamani, M. Capacity and Quality Improvement in Reversible Image Watermarking Approach. In Proceedings of the International Conference on Networked Computing and Advanced Information Management, Seoul, Korea, 16–18 August 2010.
20. Zamani, M.; Ahmad, R.; Manaf, A.A.; Zeki, A. An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography. In Proceedings of the International Conference on Computer Science and Information Technology, Beijing, China, 8–11 August 2009.
21. Zamani, M.; Taherdoost, H.; Manaf, A.A.; Ahmad, R.; Zeki, A. An Artificial-Intelligence-Based Approach for Audio Steganography. *MASAUM J. Open Probl. Sci. Eng.* **2009**, *1*, 64–68.
22. Abdullah, S.; Manaf, A.A.; Zamani, M. Recursive Reversible Image Watermarking Using Enhancement of Difference Expansion Technique. *J. Inf. Secur. Res.* **2010**, *1*, 64–70.
23. Zamani, M.; Manaf, A.A. Azizah's Method to Measure the Efficiency of Steganography Techniques. In Proceedings of the 2nd International Conference on Information and Multimedia Technology, Hong Kong, China, 28–30 December 2010.
24. Zamani, M.; Manaf, A.A.; Ahmad, R.; Jaryani, F.; Taherdoost, H.; Chaeikar, S.S.; Zeidanloo, H.R. A Novel Approach for Genetic Audio Watermarking. *J. Inf. Assur. Secur.* **2010**, *5*, 102–111.
25. Zeki, A.; Abdul, M.; Zamani, M. Bit-Plane Model: Theory and Implementation. In Proceedings of the Engineering Conference, Kuching, Malaysia, 14–15 April 2010.
26. Zamani, M.; Manaf, A.A.; Zeidanloo, H.R.; Shojae, C.S. Genetic Substitution-Based Audio Steganography for High-Capacity Applications. *Int. J. Internet Technol. Secur. Trans.* **2011**, *3*, 97–110. [CrossRef]
27. Zeki, A.; Manaf, A.; Ibrahim, A.A.; Zamani, M. A Robust Watermark Embedding In Smooth Areas. *Res. J. Inf. Technol.* **2011**, *3*, 123–131. [CrossRef]
28. Zamani, M.; Taherdoost, H.; Manaf, A.A.; Ahmad, R.; Zeki, A. Robust Audio Steganography via Genetic Algorithm. In Proceedings of the Third International Conference on Information & Communication Technologies, Karachi, Pakistan, 15–16 August 2009.
29. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. An Introduction to Image Steganography Techniques. In Proceedings of the International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, 26–28 November 2012.
30. Zamani, M.; Manaf, A.A.; Abdullah, S. Correlation between PSNR and Size Ratio in Audio Steganography Recent Researches in Communications. In Proceedings of the 11th international conference on Signal Processing, WSEAS, Cambridge, UK, 22–24 February 2012; Volume 2, pp. 82–87.
31. Altaay, A.J.; Sahib, S.B.; Zamani, M. Edgy Photos Statistical Steganalysis. *Adv. Inf. Sci. Serv. Sci.* **2013**, *5*, 35–48.

32. Zamani, M.; Manaf, A.A.; Abdullah, S. Efficient Embedding for Audio Steganography Models and Methods in Applied Sciences. *WSEAS* **2012**, *3*, 195–199.
33. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Determining the Threshold of Pixel Correlativity Analysis. *Int. J. Digit. Content Technol. Its Appl.* **2013**, *7*, 164–172.
34. Zamani, M.; Manaf, A.A.; Abdullah, S. An Overview on Audio Steganography Techniques. *Int. J. Digit. Content Technol. Its Appl.* **2012**, *6*, 107–122.
35. Altaay, A.A.J.; BinSahib, S.; Zamani, M. An Introduction to Watermarking Techniques Recent Advances in Electrical and Computer Engineering. *WSEAS* **2013**, *2*, 50–54.
36. Zamani, M.; Manaf, A.A.; Abdullah, S.; Chaeikar, S.S. Correlation between PSNR and Bit per Sample Rate in Audio Steganography Recent Researches in Communications. in Signals and Information Technology. *WSEAS* **2012**, *3*, 163–168.
37. Altaay, A.J.; Sahib, S.B.; Zamani, M. *Correlation Analysis of the Four Photo Themes in Five Layers Communications in Computer and Information Science*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 398, pp. 211–222.
38. Zamani, M.; Manaf, A.A.; Abdullah, S.; Chaeikar, S.S. *Mazdak Technique for PSNR Estimation in Audio Steganography Applied Mechanics and Materials*; Trans Tech Publications Inc.: Freienbach, Switzerland, 2012; Volume 229, pp. 2798–2803.
39. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Multimedia Data Hiding Evaluation Metrics. Recent Researches in Information Science and Applications. *WSEAS* **2013**, *2*, 29–34.
40. Zamani, M.; Manaf, A.A.; Daruis, R. Azizah Technique for Efficiency Measurement in Steganography. In Proceedings of the 8th International Conference on Information Science and Digital Content Technology, Jeju, South Korea, 26–28 June 2012.
41. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Partial Smooth Region Photos Statistical Steganalysis. *Int. J. Inf. Process. Manag.* **2013**, *4*, 130–143.
42. Zamani, M.; Manaf, A.A. Mazdak's Method for PSNR Estimation in Audio Steganography. In Proceedings of the International Conference on Computer and Computational Intelligence, Nanning, China, 25–26 December 2010.
43. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. *Pixel Correlation Behavior in Different Themes Communications in Computer and Information Science*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 398, pp. 223–234.
44. Zamani, M.; Manaf, A.A.; Ahmad, R.; Jaryani, F.; Chaeikar, S.S.; Zeidanloo, H.R. *Genetic Audio Watermarking Communications in Computer and Information Science*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 70, pp. 514–517.
45. Zamani, M.; Abdul Manaf, A.; Ahmad, R.; Jaryani, F.; Taherdoost, H.; Chaeikar, S.S.; Zeidanloo, R. Genetic Audio Steganography. *Int. J. Recent Trends Eng. Technol.* **2010**, *3*, 89–91.
46. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Statistical Steganalysis of Four Photo Themes before Embedding. In Proceedings of the International Conference on Advanced Computer Science Applications and Technologies, Sarawak, Malaysia, 23–24 December 2013.
47. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. Wide Flat Region Photos Statistical Steganalysis. *J. Converg. Inf. Technol.* **2013**, *8*, 1–14.
48. Aghbabaeyan, R.; Abdullah, S.; Zamani, M. Review of Digital Watermarking Techniques. In Proceedings of the 1st Technology Education and Science International Conference, Skudai, Malaysia, 29 November–1 December 2013.
49. Atoum, M.S.; Ibrahim, S.; Sulong, G.; Zamani, M. A New Method for Audio Steganography Using Message Integrity. *J. Converg. Inf. Technol.* **2013**, *8*, 35–44.
50. Dolatabadi, Z.S.S.; Manaf, A.A.; Zamani, M. Using Three Levels DWT to Increase Robustness against Geometrical Attacks. *Int. J. Adv. Comput. Technol.* **2013**, *5*, 86–104.
51. Tohidi, F.; Manaf, A.A.; Zamani, M.; Jamshidi, H. Improving the Capacity of Watermarking Techniques by Using Block Truncation Coding. *Int. J. Digit. Content Technol. Its Appl.* **2013**, *7*, 33–47.
52. Thanikaiselvan, V.; Arulmozhivarman, P. High security image steganography using IWT and graph theory. In Proceedings of the IEEE ICSIPA 2013—IEEE International Conference on Signal and Image Processing Applications, Melaka, Malaysia, 8–10 October 2013; pp. 337–342. [CrossRef]
53. Urmila, P.; Prinima, G. A Proposed Optimized Steganography Technique using ROI, IWT and SVD. *Int. J. Inf. Syst. Manag. Sci.* **2018**, 313–318.
54. Alyousuf, F.Q.A.; Din, R.; Qasim, A.J. Analysis review on spatial and transform domain technique in digital steganography. *Bull. Electr. Eng. Inform.* **2020**, *9*, 573–581. [CrossRef]
55. Cheddad, A.; Condell, J.; Curran, K.; Kevitt, P.M. Digital Image Steganography: Survey and Analysis of Current Methods Abbas. *Signal Process.* **2010**, *90*, 727–752. [CrossRef]
56. Li, N.; Hu, J.; Sun, R.; Wang, S.; Luo, Z. A High-Capacity 3D Steganography Algorithm with Adjustable Distortion. *IEEE Access* **2017**, *5*, 24457–24466. [CrossRef]
57. Dupac, M.; Constantinescu, N. 3D Steganography Models. *Ann. Univ. Craiova Math. Comp. Sci. Ser.* **2008**, *35*, 97–102.
58. Thiyagarajan, P.; Natarajan, V.; Aghila, G.; Venkatesan, V.P.; Anitha, R. Pattern based 3D image Steganography. *3D Res.* **2013**, *4*, 1–8. [CrossRef]
59. Valandar, M.Y.; Ayubi, P.; Barani, M.J. High secure digital image steganography based on 3D chaotic map. In Proceedings of the 2015 7th Conference on Information and Knowledge Technology (IKT), Urmia, Iran, 26–28 May 2015. [CrossRef]
60. Nandhini, E.; Nivetha, M.; Nirmala, S.; Poornima, R. MLSB Technique Based 3D Image Steganography Using AES Algorithm. *J. Recent Res. Eng. Technol.* **2016**, *3*, 2936.

61. Ara, A.; Gianchandani, D. A Hybrid Approach Based 3d Image Steganography Instead of 2d Image for Exchange Information. In Proceedings of the 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 15–16 October 2018; pp. 244–248. [CrossRef]
62. Sariga, N.P.; Sajitha, A.S. Steganographic data hiding in automatic converted 3D image from 2D and 2D to 3D video conversion. In Proceedings of the ICIIECS 2015—2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 27–32. [CrossRef]
63. Elsherif, S.; Mostafa, G.; Farrag, S.; Alexan, W. Secure Message Embedding in 3D Images. In Proceedings of the International conference on Innovative Trends in Computer Engineering ITCE 2019, Aswan, Egypt, 2–4 February 2019; pp. 117–123. [CrossRef]
64. Yasser, S.; Hesham, A.; Hassan, M.; Alexan, W. AES-secured Bit-cycling steganography in sliced 3D Images. In Proceedings of the International Conference on Innovative Trends in Communication and Computer Engineering ITCE 2020, Aswan, Egypt, 8–9 February 2020; pp. 313–317. [CrossRef]
65. Subhedar, M.S.; Mankar, V.H. Current status and key issues in image steganography: A survey. *Comput. Sci. Rev.* **2014**, *13–14*, 95–113. [CrossRef]
66. Tsai, Y.-Y. An adaptive steganographic algorithm for 3D polygonal models using vertex decimation. *Multimed. Tools Appl.* **2014**, *69*, 859–876. [CrossRef]
67. El-Shahed, R.A.; Al-Berry, M.N.; Ebeid, H.M.; Shedeed, H.A. Video Steganography using 3D Stationary Wavelet Transform. *SSRN Electron. J.* **2019**. [CrossRef]
68. Yang, Z.L.; Peng, X.S.; Huang, Y.F.; Chang, C.C. A novel method of speech information hiding based on 3D-magic matrix. *J. Internet Technol.* **2019**, *20*, 1167–1175. [CrossRef]
69. Farrag, S.; Alexan, W. A high capacity geometrical domain based 3d image steganography scheme. In Proceedings of the International Conference on Advanced Communication Technologies and Networking, CommNet 2019, Rabat, Morocco, 12–14 April 2019. [CrossRef]
70. Valandar, M.Y.; Barani, M.J.; Ayubi, P.; Aghazadeh, M. An integer wavelet transform image steganography method based on 3D sine chaotic map. *Multimed. Tools Appl.* **2019**, *78*, 9971–9989. [CrossRef]
71. Horng, J.-H.; Lin, J.; Liu, Y.; Chang, C.-C. 3D Multilayered Turtle Shell Models for Image Steganography. *Comput. Model. Eng. Sci.* **2020**, *125*, 879–906. [CrossRef]
72. Farrag, S.; Alexan, W. Secure 3D data hiding technique based on a mesh traversal algorithm. *Multimed. Tools Appl.* **2020**, *79*, 1–15. [CrossRef]
73. Singh, A.; Mehta, A. Hiding of text in a 3D image using steganography. *Int. J. Eng. Res. Comput. Sci. Eng.* **2017**, *4*, 59–62.
74. Megha, S.M.; Chethana, C. Study of 3D Barcode with Steganography for Data Hiding. *Int. Res. J. Eng. Technol.* **2018**, *5*, 250–254.
75. Kumar, N.; Kourav, D. An Efficient Approach based 3D Image Steganography for Security of Visual Contents. *Int. J. Innov. Trends Eng.* **2018**, *48*, 16–19.
76. Alexan, W.; Beheiry, M.E.; Gamal-Eldin, O. A Comparative Study Among Different Mathematical Sequences in 3D Image Steganography. *Int. J. Comput. Digit. Syst.* **2020**, *9*, 545–552. [CrossRef]
77. Chao, M.-W.; Lin, C.-H.; Yu, C.-W.; Lee, T.-Y. A High Capacity 3D Steganography Algorithm. *IEEE Trans. Vis. Comput. Graph.* **2008**, *15*, 274–284. [CrossRef]
78. Li, M.; Huang, N.; Wang, C. A Novel High Capacity 3D Steganographic Algorithm. *Int. J. Innov. Comput. Inf. Control.* **2011**, *7*, 4198.
79. Cai, L.; Zhao, H.; Cai, J.; Zhu, L. A 3-D Video Watermark Embedding Technology in DCT-CS Domain. *Int. J. Mach. Learn. Comput.* **2015**, *5*, 206–213. [CrossRef]
80. Moradi, M.; Sadeghi, M.-R. Combining and Steganography of 3D Face Textures. *arXiv* **2017**, arXiv:1702.01325.
81. Xia, B.B.; Wang, A.H.; Chang, C.C.; Liu, L. An image steganography scheme using 3D-Sudoku. *J. Inf. Hiding Multimed. Signal Process.* **2016**, *7*, 836–845.
82. Puech, W.; Bors, A.G. Rethinking the High Capacity 3D Steganography: Increasing its Resistance to Steganalysis. In Proceedings of the 2017 IEEE International Conference on Image Processing (ICIP), Beijing, China, 17–20 September 2017; pp. 510–514.
83. Lee, C.-F.; Shen, J.-J.; Agrawal, S.; Wang, Y.-X.; Lee, Y.-H. Data Hiding Method Based on 3D Magic Cube. *IEEE Access* **2020**, *8*, 39445–39453. [CrossRef]
84. Wu, H.-T.; Dugelay, J.-L. Steganography in 3D Geometries and Images by Adjacent Bin Mapping. *EURASIP J. Inf. Secur.* **2009**, *2009*, 317165. [CrossRef]
85. Amat, P.; Puech, W.; Druon, S.; Pedeboy, J. Lossless 3D steganography based on MST and connectivity modification. *Signal Process. Image Commun.* **2010**, *25*, 400–412. [CrossRef]
86. Yang, Y.; Ivrissimtzis, I. Mesh Discriminative Features for 3D Steganalysis. *BodyNets Int. Conf. Body Area Netw.* **2017**, *44*, 1–13. [CrossRef]
87. Azizifard, A.; Qermezkon, M.; Farshidi, R. *Information Steganography within 3D Images Using Residue Number System*; Islamic Azad University: Dezfoul, Iran, 2015.
88. Yang, Y.; Pintus, R.; Rushmeier, H.; Ivrissimtzis, I. A 3D Steganalytic Algorithm and Steganalysis-Resistant Watermarking. *IEEE Trans. Vis. Comput. Graph.* **2016**, *23*, 1002–1013. [CrossRef]
89. Li, Z.; Gong, D.; Liu, F.; Bors, A.G. 3D Steganalysis using the Extended Local Feature Set. In Proceedings of the 2018 25th IEEE International Conference on Image Processing, Athens, Greece, 7–10 October 2018; pp. 1683–1687. [CrossRef]

90. Zhou, H.; Chen, K.; Zhang, W.; Yao, Y.; Yu, N.-H. Distortion Design for Secure Adaptive 3-D Mesh Steganography. *IEEE Trans. Multimed.* **2019**, *21*, 1384–1398. [CrossRef]
91. Nissar, A.; Mir, A.H. Classification of steganalysis techniques: A study. *Digit. Signal Process.* **2010**, *20*, 1758–1770. [CrossRef]
92. Kharrazi, M.; Sencar, H.T.; Memon, N. Benchmarking steganographic and steganalysis techniques. In *Security, Steganography, Watermarking Multimed. Contents VII*; International Society for Optics and Photonics: Bellingham, WA, USA, 2005; Volume 5681, p. 252. [CrossRef]
93. Li, Z.; Bors, A.G. 3D mesh steganalysis using local shape features. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016. [CrossRef]
94. Li, Z.; Bors, A.G. Steganalysis of 3D objects using statistics of local feature sets. *Inf. Sci.* **2017**, *415–416*, 85–99. [CrossRef]
95. Yang, Y. Information Analysis for Steganography and Steganalysis in 3D Polygonal Meshes. 2013. Available online: http://etheses.dur.ac.uk/8492/ (accessed on 12 August 2021).
96. Sencar, H.T.; Kharrazi, M.; Memon, N. Performance study of common image steganography and steganalysis techniques. *J. Electron. Imaging* **2006**, *15*, 041104. [CrossRef]
97. Chandramouli, R.; Kharrazi, M.; Memon, N. Image Steganography and Steganalysis: Concepts and Practice. *Program. Lang. Syst.* **2004**, *2939*, 35–49. [CrossRef]
98. Karampidis, K.; Kavallieratou, E.; Papadourakis, G. A review of image steganalysis techniques for digital forensics. *J. Inf. Secur. Appl.* **2018**, *40*, 217–235. [CrossRef]
99. Christaline, J.A.; Ramesh, R.; Vaishali, D. Critical review of image steganalysis techniques. *Int. J. Adv. Intell. Paradig.* **2015**, *7*, 368–381. [CrossRef]
100. Mbadr, S.; Ismaial, G.; Khalil, A.H. A Review on Steganalysis Techniques: From Image Format Point of View. *Int. J. Comput. Appl.* **2014**, *102*, 11–19. [CrossRef]
101. Kaur, M.; Kaur, G. Review of Various Steganalysis Techniques. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 1744–1747.
102. Avcibas, I.; Memon, N.; Sankur, B. Steganalysis Using Image Quality Metrics. *IEEE Trans. Image Process.* **2003**, *12*, 221–229. [CrossRef]
103. Johnson, N.F.; Jajodia, S. Steganalysis: The investigation of hidden information. In Proceedings of the 1998 IEEE Information Technology Conference, Information Environment for the Future, Syracuse, NY, USA, 3 September 1998; pp. 113–116. [CrossRef]
104. Ding, X.; Xie, Y.; Li, P.; Cui, M.; Chen, J. Image Steganography Based on Artificial Immune in Mobile Edge Computing with Internet of Things. *IEEE Access* **2020**, *8*, 136186–136197. [CrossRef]
105. Dhawan, S.; Chakraborty, C.; Frnda, J.; Gupta, R.; Rana, A.K.; Pani, S.K. SSII: Secured and high-quality Steganography using Intelligent hybrid optimization algorithms for IoT. *IEEE Access* **2021**, *9*, 1. [CrossRef]
106. Bairagi, A.K.; Khondoker, R.; Islam, R. An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. *Inf. Secur. J. A Global Perspect.* **2016**, *25*, 197–212. [CrossRef]