Survey of 2D &3D Image Steganography Techniques for Data Security System

[1]Ranjan Kumar Mandal, [2]Dr. Nikhil Ranjan,[3]Dr. Bharti Chourasia

[1]ME Scholar, [2]Associate Professor, [3]Associate Professor & HOD,

[1&2&3]Department of Electronics & Communication,

[1&2&3]RKDF Institute of Science & Technology, SRK University, Bhopal, India.

Abstract : Image steganography refers to hiding information i.e. text, images or audio files in another image or video files. The current project aims to use steganography for an image with another image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique. This examination displays an outline of different three-dimensional (3D) picture steganography methods from overview perspective. This paper exhibit scientific categorization of 3D picture steganography systems and distinguish the ongoing advances in this field. Steganalysis and assaults on 3D picture steganography calculations have likewise been examined. 3D picture steganography strategies in all the three spaces: geometrical, topological and portrayal areas have been contemplated and thought about among each other on different parameters, for example, inserting limit, reversibility and reaction towards assaults. A few difficulties which restrain the advancement of 3D steganography calculations have been recognized. This investigation finishes up with some valuable discoveries at last**.**

IndexTerms **- Image Processing, Image, 2D, 3D, Steganography.**

I. Introduction

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[3]

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned both with concealing the fact that a secret message is being sent and its contents.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change. Due to advancements in digital communication, sending a secure message where intruders from every nook and corner of the world are present is a challenging task. Various methods have been developed for secure communication such as cryptography and information hiding. The former one converts messages into a form which is incomprehensible for human beings. It also requires a key for bringing it back to the understandable form. The key is already available to the destined receiver and hence no one except him/her can make out the message. However, the problem with cryptography is the jumbled (encrypted) representation of message which can create sufficient suspicion in eavesdropper's mind that something of interest is being carried away. The intruder might hamper its contents. Hence, the destined receiver is not able to fetch the correct message. On the other hand, the latter one hides the secret information in such a way that it remains invisible to human eye. In this case, the secret information is placed inside an innocuous looking file in such a way that the presence of information goes undetectable. It is an effective and secure communication method as the communication takes place without being sensed by anyone.

Figure 1 shows some methods for securing confidential information. Information hiding is done by watermarking or steganography. Both differ from each other in terms of carrying capacity and objective to be achieved. Watermarking has low carrying capacity and the main objective is attaching the payload in a carrier in the most robust manner. Whereas, steganography has high carrying capacity and the main objective is to make the embedded message as imperceptible as possible [1].

For unsecure communication channel, steganography is a better method than cryptography. In this technique, the secret information is embedded inside a host (cover) file such as audio, video, text or image and the resulting output file (known as stego-file) is perceptually similar to the host file. The quality of steganography algorithm is dependent upon the imperceptibility of hidden message inside the host file, robustness of the approach of being able to carry secret message safely to the destined receiver and capacity of carrying message at least a quarter size of host file.

If the host file is an image, then steganography is named as image steganography. It is important to understand the difference between two-dimensional (2D) image steganography and 3D image steganography.

Modern steganography entered the world in 1985 with the advent of personal computers being applied to classical steganography problems. Development following that was very slow, but has since taken off, going by the large number of steganography software available:

- Concealing messages within the lowest bits of noisy images or sound files. A survey and evaluation of relevant literature/techniques on the topic of digital image steganography can be found here.[8]
- Concealing data within encrypted data or within random data. The message to conceal is encrypted, then used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates cipher texts that look perfectly random without the private key).
- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a cipher text-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.

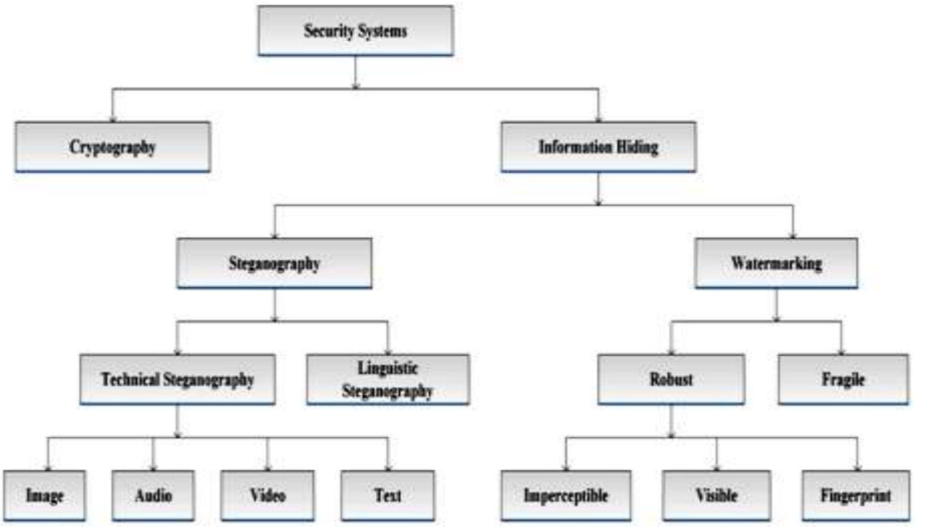

Figure 1: Methods for securing confidential information

Many 2D image steganography algorithms have been developed [2]. 3D image steganography algorithms due to some inherent challenges are quite less in number. However, 2D image steganography techniques have less carrying capacity than 3D image steganography. Survey of various 2D image steganography techniques has been done [2, 3]. However, to the best of our knowledge, a comprehensive survey of 3D image steganography techniques is not available till date. This motivates us to initiate this survey, in which various 3D image steganography techniques have been reviewed.

The goal of this paper is to survey the fundamental concepts and techniques in 3D image steganography. The references will be made to fundamental concepts and techniques arising from 3D image steganography in the image processing communities. This paper includes researchers in image analysis, information hiding and security communities.

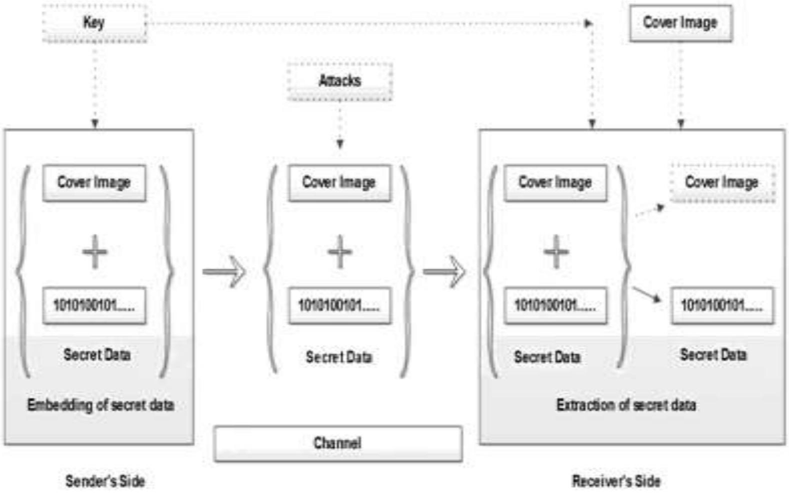

Figure 2: Generalized view of steganographic system

II. MAIN COMPONENTS OF IMAGE STEGANOGRAPHY SYSTEM

3D image steganography system requires a 3D image model as a cover object and secret binary message. Steganography system consists of two main procedures: embedding and extraction procedures. These procedures may or may not require a secret key. A 3D object consists of points represented in three coordinates. Steganography algorithms work at manipulating these points in such a way that the changes are invisible to human eye. The manipulations are done in order to embed the secret data bits inside the points of 3D image model. The basic components of a steganography system are depicted in Fig. 2. The embedding procedure takes two inputs, i.e. a cover image and secret message; and generates a stego-image. Stego image may be subjected to attacks while it is being transferred from sender to receiver. The extraction process may require cover image. Some extraction processes do not need cover image. Thus, these are termed as blind extraction. The extraction process may yield the exact cover image in addition to the secret data. Such a steganography is termed as reversible steganography as information hiding has no effect on cover image and hence is reversible.

3D image steganography has become an area of interest for research ever since the support for 3D image models from software and hardware arose. Due to large data points in the 3D image model than a 2D image, the carrying capacity of the 3D image model is much more. Hence, 3D image steganography techniques have been centered on utilizing the optimal embedding capacity of the 3D image model.

III. BACKGROUND

A. G. Benedict, et al., [1] Steganography is the way toward concealing a mystery message inside a conventional message and removing it at its goal. Picture steganography is one of the most widely recognized and secure types of steganography accessible today. Conventional steganography methods utilize a solitary spread picture to install the mystery information which has barely any security inadequacies. In this manner, bunch steganography has been embraced which stores information on different pictures. In this work, a novel methodology is proposed for cutting the mystery information and putting away it on numerous spread pictures.

M. C. Kasapbaşi et al., [2] In this investigation, another spatial space turbulent steganography conspire is introduced using additionally new fractal stream encryption calculation to stow away Huffman encoded and packed Turkish writings. The examination makes out of four principle stages. Right off the bat, an example of Turkish newswork feature writer corpus is assembled to get not just the frequencies of letters including exceptional Turkish characters yet additionally accentuations, spaces, newlines, citations, and so on. Because of the primary stage, a static Huffman encoding word reference is acquired for 102 experienced characters.

X. Xie et al., [3] In this examination, the creators propose a Vague control succession \lpar(n,n) mystery picture sharing plan dependent on code division multiplexing. The mystery information are decoded into n have pictures to produce n meaningful offers utilizing n encoding codes. Any two of encoding codes are symmetrical to one another. On the off chance that and just if with n shares together, the mystery information can be recovered effectively, and the host pictures can be recouped totally.

D. Hu, et al.,[4] In this letter, it is characterize another cost work that utilizes nonnegative lattice factorization to foresee the picture pixels and uses the common conditions among the pixels to compute the expenses. it is available a novel cost work in which the residuals are not determined through convolution with steady channels. Test results show that our strategy beats the best in class MiPOD, spatial all inclusive wavelet relative twisting, wavelet got loads, and HUGO-BD strategies in opposing steganalysis dependent on the spatial rich model and is marginally better than the high-pass, low-pass, low-pass technique.

E. Emad, et al., [5] This work proposes a safe steganography calculation that shrouds a bitstream of the mystery text into the least critical bits (LSBs) of the estimation coefficients of the whole number wavelet change (IWT) of grayscale pictures just as every segment of shading pictures to shape stego-pictures. The installing and extricating periods of the proposed steganography calculations are performed utilizing the MATLAB programming.

X. Zhang, et al.,[6] To accomplish picture steganography, the mystery data is changed over into a double grouping and divided into sections, and the picture whose component succession equivalents to the mystery data fragments is picked as the spread picture as indicated by the record. From that point forward, all spread pictures are sent to the recipient. In the entire procedure, no change is done to the first pictures. Exploratory outcomes and investigation show that the proposed calculation can oppose the location of existing steganalysis calculations, and has better power against regular picture preparing and better capacity to oppose steganalysis contrasted and the current coverless picture steganography calculations.

W. Zhou, et al.,[7] In this work, it is propose a novel cost reassignment rule, which is applied to not one but rather a group of existing contortion capacities. it is find that the costs appointed on certain pixels by a few steganographic strategies might be totally different despite the fact that these techniques exhibit close security levels. it is call such pixels "questionable pixel". Exploratory outcomes show that steganalysis highlights are not touchy to dubious pixels; in this manner, these pixels are appropriate to convey more payloads. it is name this standard the disputable pixels earlier (CPP) rule.

B. Debnath et al., [8] The proposed QCA encoder/decoder circuit is reasonable for reversible registering. To set up this, the warmth vitality dispersal by the proposed encoder/decoder circuit is assessed. The estimation shows that the encoder/decoder circuit has exceptionally low vitality dissemination. Single missing/extra cell-based deformity examination is likewise investigated in this investigation. Dependability of the circuit is tried against various temperatures. Execution and testing of the circuit are accomplished utilizing QCADesigner apparatus. MATLAB is utilized to create the contribution to the proposed circuit.

F. Wang, et al., [9] As of late, Lee and Tsai proposed another validation strategy for greyscale report pictures utilizing the convenient system designs group picture; be that as it may, their technique can't avoid the self-replacement assault, the equivalent position-replacement assault, or the cut-off assault. Besides, those assaults can be finished by the famous picture altering programming Adobe Photoshop. Thusly, the creators proposed a security-improved verification conspire dependent on Lee and Tsai's technique. The creators' proposed conspire utilizes three random parallel groupings to randomize the paired form of a given greyscale archive picture, and subsequently conquers the security defects referenced previously.

W. Zhang, et al., [10] With the prominence of redistributing information to the cloud, it is indispensable to ensure the security of information and empower the cloud server to effortlessly deal with the information simultaneously. Under such requests, reversible information stowing away in encoded pictures (RDH-EI) pulls in an ever increasing number of specialists' consideration. In this work, it is propose a novel system for RDH-EI dependent on reversible picture change (RIT). Not the same as all past encryption-based systems, in which the ciphertexts may pull in the documentation of the inquisitive cloud, RIT-based structure permits the client to change the substance of unique picture into the substance of another objective picture with a similar size.

R. Jain, et al., [11] This work investigations these systems and presents a compression among them to discover the best strategy for computerized shading Image compression. The aim of this work is to be find out the best approach for growing better approach for advanced color Image compression with least loss in Image quality.

J. H. J. Yin, et al., [12] Web of Things (IoT) is a typical thing (object) in this day and age, which fills in as a major aspect of our standard life exercises. In spite of the fact that it benefits the private locale in a few different ways, different difficulties, for example, information secrecy and protection are made. In actuality, the network is concerned what data may spill out by means of IoT.

IV. CHALLENGES

Developing a steganography algorithm for 3D mesh has some inherent challenges and thus leading to less number of algorithms than 2D images. A few of them, as identified in [3, 5] have been put up below:

(i)Sampling of 3D object is not regular as is the case with 1D/2D geometric representations. For instance, a 2D image can be seen as a 2D array of pixel values; but similar sampling cannot be applied on 3D object. This makes techniques like DCT, DWT and so on which make use of regularly sampled data, even more difficult to be applied.

(ii)Same mesh model can be represented in a number of ways, i.e 3D mesh, NURBS surface and so on. 3D mesh itself can be stored in a number of formats. For all the practical applications, files stored in these formats are interchangeable. However, steganography algorithms are designed for a particular type of format. Thus, a standardized steganography algorithm which works on all types of 3D image models is a big challenging task.

(iii)Embedding of secret data is done on the pixel values in 2D images and in case of 3D meshes; it is done on vertices and faces. Unlike pixel values, vertices and faces are subjected to many intentional or non-intentional changes while in transmission (e.g. rotation, uniform scaling of 3D meshes, cropping etc). Also the number of attacks to 3D stego model outnumbers the attacks that can be carried on the 2D stego image. Thus, the extraction of secret data should take into account all these changes and manipulation of 3D mesh may be required before the actual extraction can take place.

(iv)Unlike 2D image where data can be picked by following either the row or the column order, there is no order sequence of 3D data in 3D mesh. Since both geometry and topology information of 3D object are irregular, methods like cannot be applied for hiding secret message in 3D mesh.

A. FINDINGS AND FUTURE SCOPE

From the literature survey, some observations can be drawn which are put up as below:
(i) 3D image steganography techniques offer more payload carrying capacity than 2D image steganography techniques as can be seen in Table 1.
(ii) Majority of the approaches are based on geometrical domain because of better embedding capacity than both topological and representation domains based algorithms.
(iii) Combination of geometrical based approach with topological based approach as done in [4] and with representation based approach as done in [2] has raised the overall embedding capacity of the algorithm.

V. CONCLUSION

A comparison of various 2D and 3D image steganographic approaches regarding their resistance towards different geometrical attacks has been presented. Other challenges that post difficulties in developing steganography algorithm for 3D mesh have also been discussed in this paper. Additionally, 3D steganalytic approaches have also been investigated in the present work. It can be concluded that both 32D and D steganography and steganalysis are underdeveloped areas and are largely unexplored fields.

REFERENCES

[1]. A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," *2019 International Conference on Data Science and Communication (IconDSC)*, Bangalore, India, 2019, pp. 1-5.

[2]. M. C. Kasapbaşi, "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption With Post-Quantum Security," in *IEEE Access*, vol. 7, pp. 148495-148510, 2019

[3]. X. Xie, C. Chang and C. Lin, "Reversibility-oriented secret image sharing mechanism with steganography and authentication based on code division multiplexing," in *IET Image Processing*, vol. 13, no. 9, pp. 1411-1420, 18 7 2019.

[4]. D. Hu, H. Xu, Z. Ma, S. Zheng and B. Li, "A Spatial Image Steganography Method Based on Nonnegative Matrix Factorization," in *IEEE Signal Processing Letters*, vol. 25, no. 9, pp. 1364-1368, Sept. 2018.

[5]. E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639-649, June 2018.

[6]. X. Zhang, F. Peng and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," in *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, Dec. 2018.

[7]. W. Zhou, W. Zhang and N. Yu, "A New Rule for Cost Reassignment in Adaptive Steganography," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2654-2667, Nov. 2017.

[8]. B. Debnath, J. C. Das and D. De, "Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication," in *IET Circuits, Devices & Systems*, vol. 11, no. 1, pp. 58-67, 1 2017.

[9]. F. Wang, W. Lyu and J. Pan, "Robust image authentication scheme with self-repair capability for greyscale source document images via PNG format," in *IET Image Processing*, vol. 10, no. 12, pp. 971-978, 12 2016.

[10]. W. Zhang, H. Wang, D. Hou and N. Yu, "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," in *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469-1479, Aug. 2016.

[11]. R. Jain and M. Jain, "A REVIEW OF DIFFERENT ALGORITHMS USING IN COLOR IMAGE COMPRESSION", IJOSCIENCE, vol. 2, no. 4, Jul. 2016. https://doi.org/10.24113/ijoscience.v2i4.88

[12]. J. H. J. Yin, G. M. Fen, F. Mughal and V. Iranmanesh, "Internet of Things: Securing Data Using Image Steganography," *2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)*, Kota Kinabalu, 2015, pp. 310-314.