International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 8 47 - 51

A Review of 2D &3D Image Steganography Techniques

Anjum Ara
M.Tech Scholar
Department of Electronics and Communication
SISTec, Bhopal (M.P.)

Prof. Deepa Gianchandani
Assistant Professor
Department of Electronics and Communication,
SISTec, Bhopal (M.P.)

***Abstract*—** 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.

Keywords- *Image Processing, Image, 2D, 3D, Steganography*

*****

I. INTRODUCTION

Picture 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.

Fig. 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.

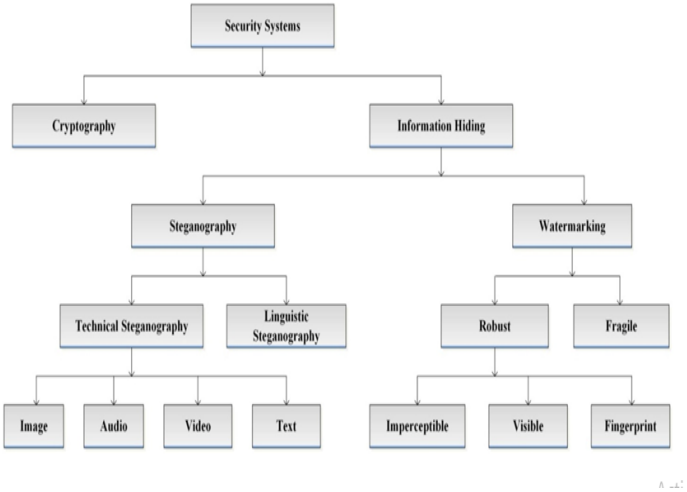

Fig. 1 Methods for securing confidential information

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.

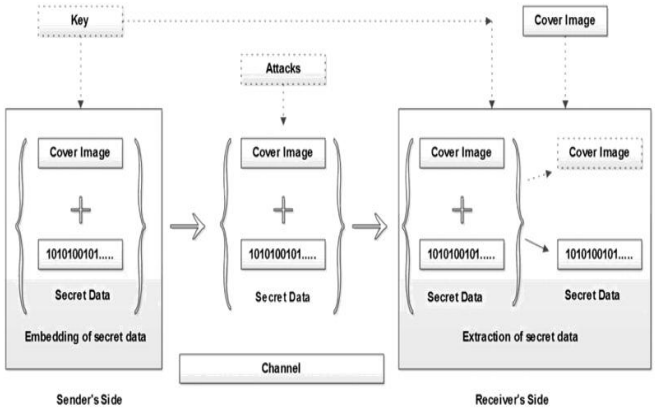

Fig. 2 Generalized view of steganographic system

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. 3D IMAGE MODELS

3D images (which have depth also, along with length and breadth) are represented in the form of mesh models in order to capture the shading effect of 3D object correctly. Polygon mesh model has advantage of being transferred at a higher rate than the other forms of representations of a 3D object such as non-uniform rational basis spline (NURBS) surface, point cloud and so on. Hence polygon mesh model is preferred over the other representations for data hiding.

Mesh representation of a 3D object (or polygon mesh representation) is made of faces, edges and vertices as shown in Fig. 3. A point in the mesh is termed as a vertex. Two vertices join to form an edge. The closed set of edges is termed as face or polygon. A mesh containing only triangle faces is a triangle mesh and likewise a mesh with only quadrilateral faces is a quadrilateral mesh.

A. Taxonomy of image steganography approaches

Image steganography can be divided into two categories such as 2D image steganography and 3D image steganography. 2D image steganography uses a 2D image as cover in which secret information is hidden inside the pixel intensities. 3D image steganography on the other hand, uses a 3D image as cover image which has points or vertices in the 3D geometry which are manipulated for hiding a secret message. Embedding capacity of 2D image steganography is measured in terms of number of bits embedded per pixel of cover image. In case of 3D image steganography, it is measured in terms of number of bits embedded per vertex of cover image. In Table 1, comparison has been done on the basis of size of secret message (payload size) that algorithms in 2D and 3D image steganography techniques can carry. Since 3D image steganography algorithms use a bigger cover file (i.e. 3D image model) than 2D image steganography, the former ones are able to carry a bigger payload (secret message).

Image steganography using 3D image can be done in both spatial and frequency domains. Some work has been done in the frequency domain [28] while the most of work in 3D image steganography is done in spatial domain Further, the technique of hiding secret data inside the 3D image has been accomplished in the following three ways in spatial domain.

(i) Geometrical domain based steganography.
(ii) Topological domain based steganography.

Table 1 Comparison of various approaches proposed for 3D image models in geometrical domain

Year	Authors	Algorithm/technique
1998	Ohbuchi *et al.*	triangle similarity quadruple embedding
1998	Ohbuchi *et al.*	tetrahedral volume ratio embedding
2003	Cayre and Macq	macro embedding procedure
2004	Maret and Ebrahimi	embedding in similarity invariant space
2005	Cheng *et al.*	multi-level embedding procedure
2007	Cheng and Wang	adaptive minimum-distortion estimation
2009	Chao *et al.*	multilayered embedding scheme
2009	Wu and Dugelay	adjacent bin mapping method
2010	Chuang *et al.*	embedding using histogram shifting
2013	Thiyagarajan *et al.*	embedding after triangle mesh formation
2015	Huang and Tsai	embedding based on histogram shifting
2017	Anish *et al.*	embedding in *x*-coordinate of vertex

IV. ATTACKS ON 3D IMAGE STEGANOGRAPHY

Ability of resisting the attacks defines the robustness of the stego model. On the other hand, security of stego model is decided by its ability to withstand steganalysis. Steganalysis requires expertise on the knowledge of 3D mesh models and working of steganography system. However, the attacker of 3D stego model may or may not be having any knowledge of it. Hence, attacks and steganalysis on 3D stego model differ from one another.

A. STEGANALYSIS

Steganalysis is the science of developing algorithms which could detect the existence of secret data inside an otherwise undetectable stego model. What cryptanalysis is to cryptography; steganalysis is to steganography [2]. As pointed out in [5], 3D steganalysis techniques are underdeveloped when compared with 2D image steganalysis and thus need to be explored. Some of the 3D steganalysis approaches proposed so far have been overviewed in this paper.

There are two kinds of steganalytic approaches to break the steganography algorithms; namely specific and universal Specific steganalyser aims at detecting the hidden message embedded inside the cover model by using a specific steganography algorithm. On the contrary, universal steganalyser is used for detecting the hidden message embedded inside the cover model embedded using any steganography algorithm.

3D image steganalysers are designed taking into account the statistical changes that might have crept in cover mesh model because of embedding of secret message inside it. Secret message inside the cover model may be imperceptible to the human eye but disturbs the natural statistics of the cover model .

Yang and Ivrissimtzis [4] proposed a 3D steganalytic algorithm for the first time which extracts feature vectors (which includes Cartesian and Laplacian coordinates, dihedral angles and normal of the mesh) from the mesh and its 'reference' copy (obtained by Laplacian smoothing) of both cover and stego meshes. Calibration [5] is done on the difference between the features of mesh and its reference copy and for the stego-model the values are distinctively larger than that of cover model. Afterwards, a supervised learning classifier based on quadratic discriminate analysis was used to distinguish between given cover models and stego models. The accuracy of the specific steganalyser against was 99% while universal steganalyser was 80% accurate against .

Yang et al. [7] proposed another specific steganalyser against the steganography system proposed by Cho et al. [8] designed for the spherical coordinate system. The steganalytic algorithm was based on the fact that stego model had two clusters of the mean values of histogram bins in place of a single cluster in case of covermodel. The proposed steganalytic algorithm achieved 98% accuracy for detection of hidden secret data.

Use of Fisher linear discriminate ensemble [9] was done in the steganalytic algorithm proposed by Li and Bors [6]. This algorithm used the simplified version of the feature set used in [6] along with vertex normal and local curvature of the meshes as features. It was observed in the proposed approach that the simplified variation of feature set exhibited better results than using the complete feature set.

Yang et al. [2] proposed an improvement over their previous steganalytic algorithm [7] proposed for Cho et al. [8] steganography algorithm with an accuracy of 99%. Based on the loopholes in the steganography approach identified from the steganalysis, Yang et al. proposed a modified data hiding algorithm which was successful in bringing down the accuracy of steganalyser to 50–60%.

Recently, Li and Bors [6] proposed robustness and relevance based feature selection algorithm in order to deal with the cover source mismatch (CSM) problem. CSM problem arises when the cover source used for generating training sets is different cover source than the one for originating testing sets. The proposed approach was proven to give better results than other steganalytic approaches.

V. APPLICATIONS

Steganography has applications wherever secret communication is desired. Some of these areas where steganography plays a vital role have been discussed below.

(i) Military and defence organisations: Steganography has been used by terrorist organisations for communicating secret information among their various units. A few years ago, a US Special agent from FBI filed complaint against some alleged Russian agents that they have been using steganography for hiding encrypted messages [2]. 3D cover image models can be used as bigger carrying vessels than 2D cover images. News of using 2D cover images for steganography by defence and criminal organisations has been seeing daylight time to time [5–7, 2]; it might be a possibility that 3D image steganography has also been used for covert communications but the news has not broken out yet [6] Thus, development of steganography algorithms using 3D image models is crucial for the efficient working of defence organisations.

(ii) Medical area: Another application of steganography is in medical area. Steganography algorithms can be used for hiding the patient history and other such useful information inside the reports prepared on 3D model of human organs [3]. It should be noted that the embedding done in this case should be reversible in nature so that it does not alter the patient's report.

(iii) Monitoring copyrighted material on internet: Availability of various 3D computer graphics software such as Blender, Maya, Mudbox and so on [4] has made the task of designing of 3D models easy and simplified. As a result, need to protect these 3D models against their copyrighted use arises. Steganography plays an important role in this case as it secretly carries the owner's name and other related information inside the 3D model and inhibits its illegitimate use. It should be noted that the steganography algorithm used for hiding this information is robust against attacks. In other words, attackers or duplicate copy makers are not able to remove the information from the original work however hard they may try.

A. 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.

B. 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.

VI. CONCLUSION

A comparison of various 3D image steganographic approaches regarding their resistance towards different geometrical attacks has been presented. Other challenges that pose 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 3D steganography and steganalysis are underdeveloped areas and are largely unexplored fields.

REFERENCE

[1]. Nannan Li , Jiangbei Hu1, Riming Sun, Shengfa, Zhongxuan **"A High-Capacity 3d Steganography Algorithm Adjustable Distortion"** Ieee Journal Of Image Processing 2017

[2]. H. Huang, B. Liao, and J. Pan, ``Special issue on information hiding and multimedia signal processing," Int. J. Innov. Comput., Inf. Control, vol. 6,. 3, pp. 12071208, 2010.

[3]. M. Luo and A. G. Bors, ``Surface-preserving robust watermarking of 3-D shapes," IEEE Trans. Image Process., vol. 20, no. 10, pp. 28132826,. 2011.

[4]. M.-T. Li, N.-C. Huang, and C.-M. Wang, ``A novel high capacity 3D steganographic algorithm," Int. J. Innov. Comput., Inf. Control, vol. 7,no. 3, pp. 10551074, 2011.

[5]. C.-H. Lin, M.-W. Chao, J.-Y. Chen, C.-W. Yu, and W.-Y. Hsu, ``A highcapacity distortion-free information hiding algorithm for 3D polygon models," Int. J. Innov. Comput., Inf. Control, vol. 9, no. 3, pp. 13211335, Mar. 2013.

[6]. Y. Yang, N. Peyerimhoff, and I. Ivrissimtzis, ``Linear correlations between spatial and normal noise in triangle meshes," IEEE Trans. Vis. Comput. , vol. 19, no. 1, pp. 4555, Jan. 2013.

[7]. Y.-Y. Tsai, ``An adaptive steganographic algorithm for 3D polygonal models using vertex decimation," Multimedia Tools Appl., vol. 69, no. 3, pp. 859876, Apr. 2014.

[8]. Y. Yang and I. Ivrissimtzis, ``Mesh discriminative features for 3D steganalysis," ACM Trans. Multimedia Comput., Commun. Appl., vol. 10, no. 3, pp. 27:127:13, Apr. 2014.

[9]. H. Kaveh and M.-S. Moin, ``A high-capacity and low-distortion 3D polygonal mesh steganography using surfacelet transform," Secur. Commun. Netw., vol. 8, no. 2, pp. 159167, Jan. 2015.

[10]. Y.-Y. Tsai, ``An efcient 3D information hiding algorithm based on sampling concepts," Multimedia Tools Appl., vol. 75, no. 13, pp. 78917907, Jul. 2016

[11]. Y. Yang, R. Pintus, H. Rushmeier, and I. Ivrissimtzis, ``A 3D steganalytic algorithm and steganalysis-resistant watermarking," IEEE Trans. Vis. Comput. Graphics, vol. 23, no. 2, pp. 10021013, Feb. 2017.

[12]. R.. Ohbuchi, H. Masuda, and M. Aono, ``Watermarking three-dimensional polygonal models through geometric and topological modications," IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 551560, May 2010