# A Systematic Study of 2D and 3D Image Steganography Techniques for Real Time Applications

Gunja Venkat Chandra [1], D.Subhashini [2]
[1] *Pondicherry Engineering College, Pondicherry*
[2] *Assistant Professor, Mahatma Gandhi institute of technology, Hyderabad*

**Abstract:** This study presents an overview of various two dimensional (2D) and three-dimensional (3D) image steganography techniques from survey point of view. The authors present taxonomy of 2D and 3D image steganography techniques and identify the recent advances in this field. Steganalysis and attacks on 2D and 3D image steganography algorithms have also been studied. 2D and 3D image steganography techniques in all the three domains: geometrical, topological and representation domains have been studied and compared among each other on various parameters such as embedding capacity, reversibility and response towards attacks. Some challenges which inhibit the development of 2D and 3D steganography algorithms have been identified. This study concludes with some useful findings in the end. A comprehensive survey on 2D and 3D image steganography techniques, to the best of the authors' knowledge, is not available and thus it suffices the need of this study.

**Keywords:** steganography**,** two dimensional and three-dimensional.

## I. INTRODUCTION

### 1.1 Motivation

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. 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. The audience for this paper includes researchers in image analysis, information hiding and security communities.

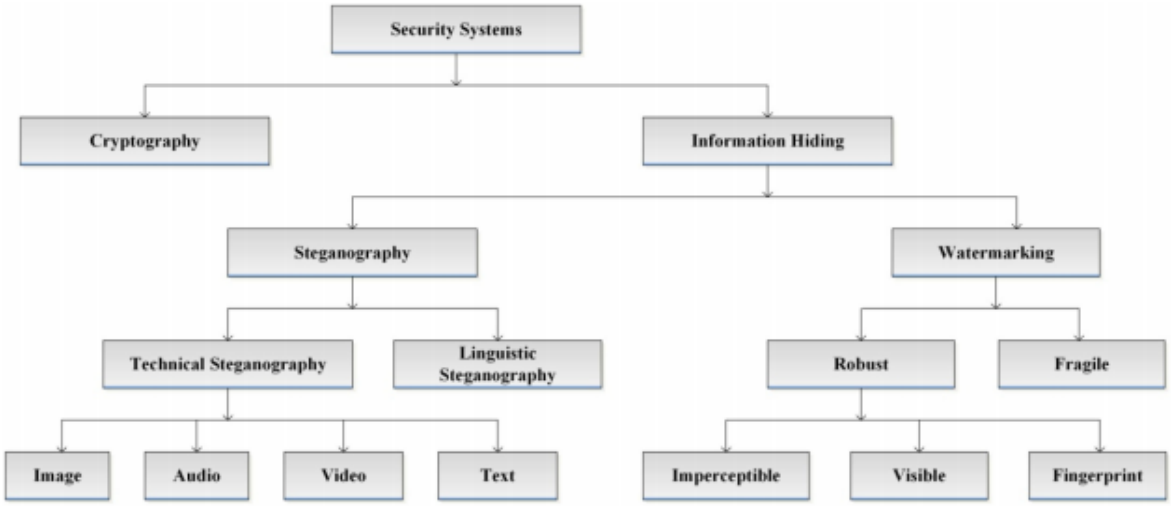


Fig. 1 Information hiding types [2]

**1.2 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 centred on utilising the optimal embedding capacity of the 3D image model.

**1.3 History**

The technique of concealing a secret message inside an innocuous message (called cover) in such a way that its presence goes undetectable, ages back to the ancient times [4]. Many examples of hiding secret data under a naïve medium have been laid out in [4]. In old times, secret message was written on the shaved head of a slave and after hair grew back he was sent to the destination [2]. Some incidents mentioned in [4] dates to the World War II times. It was reported in some news articles that prior to the 9/11 attack on the US, Al-Qaeda was using steganography for communicating secretly [5–7]. Survey of 2D image steganography techniques was reported in 2010 [2], 2014 [3] and 2016 [8]. Many books on steganography have explored 2D image steganography system and techniques [9–12]. Similarly, survey on 3D image watermarking techniques is available in the form of research papers [13, 14] as well as book chapter [15]. The comprehensive surveys of 2D image steganography and 3D image watermarking techniques were reported in literature. However, survey on 3D image steganography has not been reported. Thus, the need for a detailed survey of 3D image steganography techniques arises.

**1.4 Outline**

This paper is structured as follows. Section 2 presents the definitions and mathematical representation of terms used in steganography techniques. Section 3 summarises the 3D image models used in steganography. Section 4 lays out the literature review of the 3D image steganography techniques with their strengths and weaknesses. Attacks on 3D stego-model have been discussed in Section 5. 3D image steganalysis techniques proposed till now have been brought up in Section 6. Section 7 discusses some applications of 3D steganography. Some challenges which inhibit the progress of development of 3D image steganography algorithms have been identified in Section 8. Section 9 lists the findings of the literature review and future scope of 3D image steganography. Finally, Section 10 presents concluding remarks.

## II. BACKGROUND

The technique of covertly hiding the secret message is steganography. Steganography techniques comprise of two main phases: embedding and extraction. In embedding phase, the secret message which may be considered as a bit stream is placed inside the cover file. This is done in such a way that the human eye is not able to differentiate between the cover image and the stego-image perceptually. In extraction phase, secret message is taken away from the stego media (secret bits imbibed inside cover file) at the destination. In this phase, the secret message bits are extracted from the stego-file with or without keys.


Fig. 3 Mesh representation of a 3D object (or polygon mesh representation) (a) Vertices, (b) Edges, (c) Faces (d) Polygons, (e) Surfaces [67]

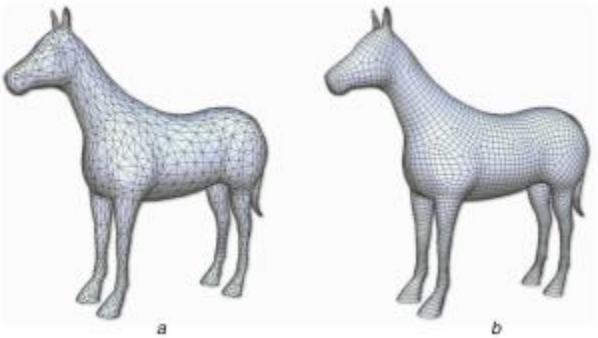


Fig. 4 Triangle mesh and quad mesh of 3D horse (a) Triangle mesh, (b) Quad mesh

### 2.1 Mathematical representation

If the host or cover file is denoted by 'C' and embedding secret message 'M' in it using key 'K'; produces stego-file denoted by 'C'. Embedding and extraction processes are denoted by Em and Ex , respectively. Em and Ex use same key and are inverse of each other. These processes can be described using the following equations:

$$\text{Embedding: } C' = Em(C, K, M),$$
$$\text{Extraction: } M = Ex(C', K) \quad (1)$$

The cover file can be an audio, video, text or an image file. The steganography technique in the above four types of cover file would be termed as audio steganography, video steganography, text steganography and image steganography, respectively. Image steganography techniques outnumber the other three. A video file can be considered as moving frames of images, so if a secret data is concealed inside an image, then it can be embedded inside the video file also. Thus, image steganography paves the way for video steganography. Audio and text steganography techniques have not received much attention compared with image steganography because of the larger carrier required in the former two when the same amount of payload is being carried in all three [16]. A preferable way of extracting secret message bits from the stego-media is without using the original cover file for extraction. However, not all steganography techniques are blind [17]. The reversible steganography algorithms are used when the cover image is carrying important information which cannot be lost when secret data is being embedded.

## 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. Fig. 4 shows a triangle mesh and a quad mesh of the 3D image model of a horse.

Table 1 Comparison between 2D and 3D image steganography algorithms

| 2D steganography algorithm | Payload size, bits | 3D steganography algorithm | Payload size, bits |
|---|---|---|---|
| Fridrich *et al.* [18] | 1024 | Wang and Cheng [19] | 201107 |
| Xuan *et al.* [20] | 5000–49,000 | Cheng and Wang [21] | 1,049,417 |
| Celik *et al.* [22] | 15,000–143,000 | Cheng and Wang [23] | 522 834 |
| Li and Wang [24] | 73,728 | Chao *et al.* [25] | 4,433,319 |
| Sun [26] | 108,074 | Huang and Tsai [27] | 4,101,995 |

## IV. 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. This is because of the extra efforts required to move the image in and out of the frequency domain. Since a 3D mesh model consists of huge data points, so the time taken for these operations is huge. Also, the embedding capacity in the spatial domain is higher than that in the frequency domain [29]. Further, the technique of hiding secret data inside the 3D image has been accomplished in the following three ways in spatial domain as shown in Fig. 5.

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

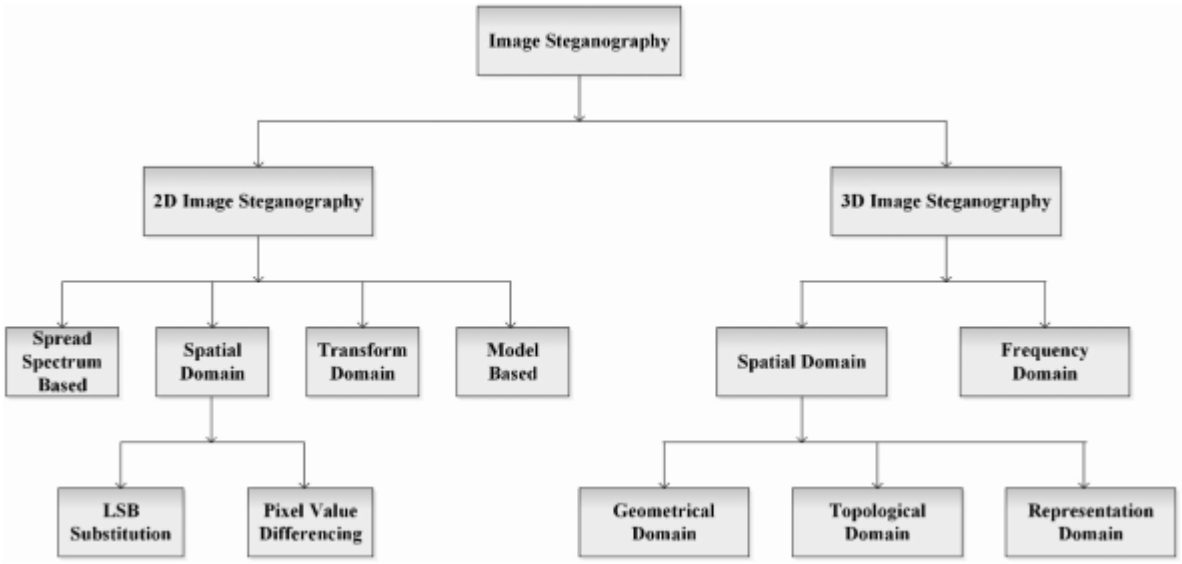


Fig. 5 Types of image steganography

### 4.1 Geometrical domain based steganography

In geometry based steganography, the approach is to change the geometry (e.g. vertices, edges, strips of triangles etc.) of the 3D cover object in order to hide the secret message [30]. The embedding is done in such a way that the change is unnoticeable. Embedding to geometrical aspects of the 3D model is extremely vulnerable to affine transformations (e.g. uniform scaling, rotation, translation). These transformations

are capable of harming the hidden secret data; hence the steganography algorithm in this domain must be able to withstand them. However, more embedding capacity is achieved by algorithms based in this domain as compared to those in other two domains. Thus, most of the 3D image steganography algorithms are based on the geometrical domain. Ohbuchi et al. [31] listed some of the geometrical aspects where the embedding can withstand geometrical transformation attacks. Although the work was concentrated on watermarking 3D models, yet two novel algorithms, i.e. triangle similarity quadruple embedding and tetrahedral volume ratio embedding show how data hiding is done in 3D models. Triangle similarity quadruple embedding algorithm was designed for macro-embeddingprocedure (MEP) and similar triangles in the polygonal mesh. It was able to resist uniform scaling, rotation and translation transformations and the extraction was blind. The other proposed algorithm, tetrahedral volume ratio embedding is also blind. It uses the volume ratio of the tetrahedrons created using the spanning tree of the mesh. Embedding of the data bits is done in the volume ratio. The algorithm could withstand the affine transformations, but was not able to resist, the more general transformations. The embedding capacity of the vertices was 2 bits per vertex. Taking the basic idea of triangle strip peeling symbol sequence (TSPS) from Ohbuchi et al. [32] for moving over the mesh, Cayre and Macq [33] proposed a macro-embedding procedure (MEP). MEP sees a triangle having one entry edge and two exit edges. One of the two exit edges is chosen depending on the data bit to be embedded. Hence, the algorithm was able to resist affine transformation as the movement is invariant to the affine transformations. Change in the states while moving was noted and used as erasing key. Thus, the algorithm is blind and reversible. Maret and Ebrahimi [34] proposed a new approach for resisting rotation, scaling and translation transformations. As a pre-requisite step of embedding, construction of a space which is invariant to above mentioned similarity transformations is done. 3D cover model was taken in this similarity invariant space and some modifications were carried out in the geometry of the cover model so that embedding can be done. The distortion of the stego-model was measured using mean symmetrical Hausdorff distance using software MESH [35]. The stego-model suffered from few distortions, although the embedding capacity reduced and the time taken for extraction was also brought down in comparison to [33]. Cheng et al. proposed three different methods of embedding secret information in 3D image models: [19] in 2005, [21] in 2006 and [23] in 2007. In [19] algorithms were written only for triangular meshes. Using MEP from Cayre and Macq [33] with some modifications along with embedding method from Cayre et al. [36], secret data was hidden inside the cover image model. The distortion to stego-model was less and embedding time was reduced. Small cover models introduce machine precision errors and hence for such cases the distortion was more than that using large cover models. The main difference in the second and third works lies in the treatment of smooth and noisy surfaces of the cover mesh. In [21] (second one) both these surfaces are treated equally while embedding. As a result, some distortion in the stego-model is inevitable. However, in [23] adaptive embedding was done, i.e. embedding less data in smooth surfaces and more data in noisy surface. This led to less distorted stego-model. Adaptive embedding was done for the first time in 3D image steganography [23].

Table 2: Comparison of various approaches proposed for 3D image models in geometrical domain

| Year | Authors | Algorithm/technique | Reversible | Blind | Withstands geometrical transformations |
|---|---|---|---|---|---|
| 1998 | Ohbuchi *et al.* [31] | triangle similarity quadruple embedding | no | yes | yes |
| 1998 | Ohbuchi *et al.* [31] | tetrahedral volume ratio embedding | no | yes | yes |
| 2003 | Cayre and Macq [33] | macro embedding procedure | yes | yes | yes |
| 2004 | Maret and Ebrahimi [34] | embedding in similarity invariant space | no | yes | yes |
| 2005 | Cheng *et al.* [19] | multi-level embedding procedure | yes | yes | yes |
| 2007 | Cheng and Wang [23] | adaptive minimum-distortion estimation | no | yes | yes |
| 2009 | Chao *et al.* [25] | multilayered embedding scheme | no | yes | no |
| 2009 | Wu and Dugelay [37] | adjacent bin mapping method | no | yes | no |
| 2010 | Chuang *et al.* [29] | embedding using histogram shifting | yes | yes | yes |
| 2013 | Thiyagarajan *et al.* [40] | embedding after triangle mesh formation | no | yes | yes |
| 2015 | Huang and Tsai [27] | embedding based on histogram shifting | yes | yes | yes |
| 2017 | Anish *et al.* [41] | embedding in *x*-coordinate of vertex | no | yes | no |

Chao et al. [25] proposed a new scheme for embedding secret data by embedding inside the cover model in multiple layers. Principal components analysis (PCA) was used for determining the initial vertices for embedding. After embedding in single layer, similar procedure was carried out for multiple layer embedding. The blind algorithm proposed however was not able to resist more general mesh transformations such as simplifying mesh, nonuniform scaling and so on. Wu and Dugelay [37] applied LSB+ algorithm for 2D image steganography [38] on 3D image steganography. The histogram was made for the coordinate values in each axis, i.e. value of all points in the three axes. Using histogram,

the embedding is done using the LSB+ (least significant bits) algorithm for data hiding in 2D images. The non-blind algorithm was shown to have much lower signal-to-noise ratio value of 3D images. Chuang et al. [29] proposed reversible image steganography for 3D cover models using histogram. The algorithm was based on Ni et al.'s idea of histogram shifting [39]. Distances of all points from the centre point were taken and normalised by the largest distance and then multiplied by some magnification factor. Afterwards, histogram was drawn for these values. Then histogram shifting method was followed. Points were displaced according to the new distances. Blind extraction of secret data from the stego model required a small amount of information to be sent along with the stego-model. The algorithm used PCA and registration technique to resist rotation, scaling and translation transformations. Thiyagarajan et al. [40] proposed embedding of secret data bits in LSBs of vertices of 3D cover model. The algorithm first obtained a secret key based on the secret message. An initial triangle was constructed by joining the maximum values on each of the three coordinate axes. The triangle mesh for embedding data was formed by decomposing this initial triangle into several smaller triangles using the secret key. Vertices of the newly formed mesh were labelled using stego key (i.e. giving each vertex a '0' or '1') and embedding was done based on label. The blind steganography algorithm required the stego key for extraction of secret data. The algorithm was shown to be robust against the rotation, cropping and scaling attack. Huang and Tsai [27] proposed a reversible steganography algorithm based on Ni et al.'s idea of histogram shifting [39]. However, the histogram was made for normalised distance differences of a vertex with its neighbours and not from centre. This made it different from Chuang et al.'s reversible data hiding method [29]. Distortion in stego model in Tsai et al.'s method was less as compared to Chuang et al.'s approach.

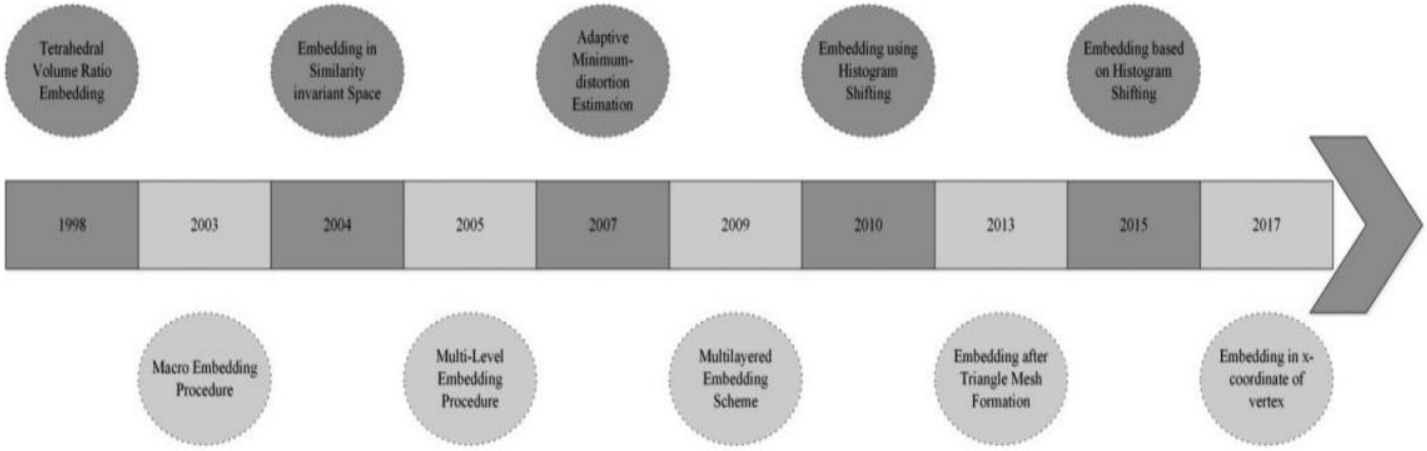


Fig. 6 Timeline showing progress of geometrical domain based approaches over the years

Anish et al. [41] proposed a simple steganography technique for data hiding in pcd type of 3D images which hides the data by manipulating the x-coordinate of the cover 3D image. This technique considers the secret text as a stream of ASCII characters and hides their decimal representation inside the x-coordinate value, as its fractional part. Performance of the proposed approach is not measured in terms of embedding capacity. Also, the security of the approach when geometrical transformations (or attacks) are carried out on the stego model is also not checked. The progress of various geometrical domains based 3D steganography approaches is shown in Fig. 6. Table 2 lists all the proposed steganography algorithms/ techniques based in geometrical domain tested using Stanford images [42] as the sample images.

**4.2 Topological domain based steganography**

In topological based steganography, the connectivity of vertices or topology of 3D cover model is modified slightly for hiding secret data bits [30]. Connectivity information in 3D model is less as compared to the geometrical primitives amounting to less embedding capacity in topological based steganography than geometrical based steganography. As the secret data is hidden in the connectivity of 3D model, geometrical transformations to it will not be able to destroy the secret data, but are vulnerable to mesh simplification, vertex reordering and other such topological modification transformations. Ohbuchi et al. [31] proposed two algorithms which are based on modifying the topological information for hiding secret data.

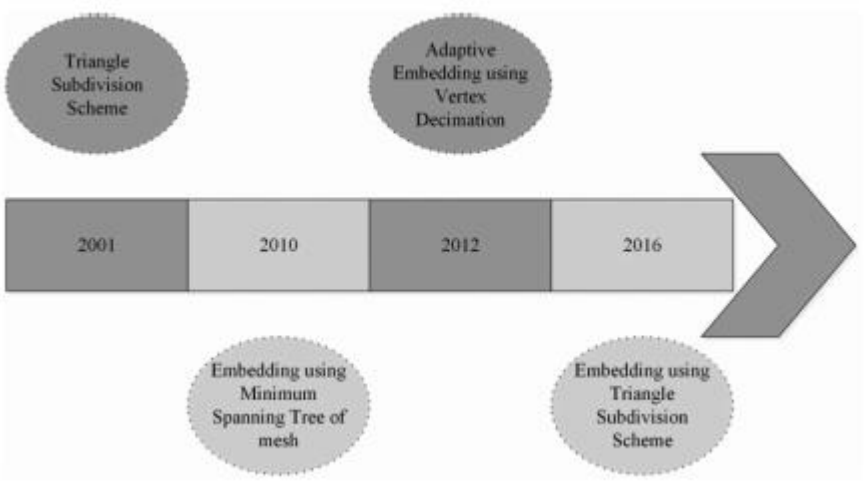


Fig. 7 Timeline showing progress of the topological domain based approaches over the years

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

| Year | Authors | Algorithm/technique | Reversible | Blind | Withstands geometrical transformations |
|---|---|---|---|---|---|
| 2001 | Mao *et al.*[43] | triangle subdivision scheme | no | yes | yes |
| 2010 | Amat *et al.* [44] | embedding using MST of mesh | no | yes | yes |
| 2012 | Tsai [45] | adaptive embedding using vertex decimation | no | yes | yes |
| 2016 | Tsai [47] | embedding using triangle subdivision scheme | yes | yes | yes |

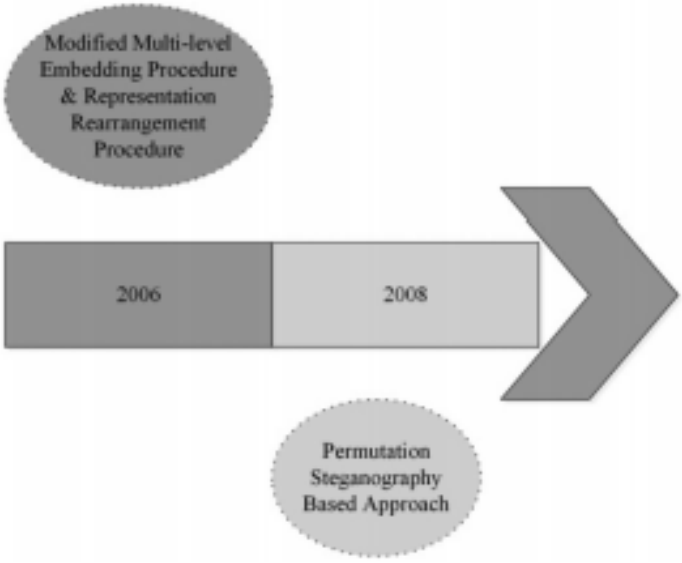


Fig. 8 Timeline showing progress of representation domain based approaches over the years

TSPS embedding takes up a triangle strip from triangle mesh for encoding secret data. The order in which adjacent triangles are stripped is used for embedding secret data bits. Due to its simplicity, TSPS is used for traversing over the polygon mesh [33]. Polygon stencil pattern embedding, the second algorithm, embeds a pattern inside a mesh by cutting out the strip in the desired pattern. This algorithm is able to resist mesh simplification transformation. Mao et al. [43] argued that the ratio of two line segments on a line remains unchanged even when the line is subjected to geometrical transformations. The triangle subdivision process is carried out on the triangle mesh creating new vertices. The ratio in which an edge of a triangle is subdivided to create a new triangle is determined by the secret data to be embedded. The

blind extraction of secret data requires same seed as that used in the embedding process. The algorithm withstands the affine transformations and can even prevent mesh simplification attacks. Amat et al. [44] used minimum spanning tree (MST) in the proposed topological based steganography algorithm. The algorithm consists of three steps: construction of MST in the mesh; analysing embedding areas in MST; and finally embedding secret data bits by joining the common edge or uncommon edge in between two triangles. The proposed method is lossless as no new edges are formed while embedding is carried out. The extraction of secret data bits from stego-model does not need the cover model. Tsai [45] proposed adaptive embedding algorithm for 3D image steganography based on vertex decimation by Schroeder et al. [46]. Information from vertex decimation is used for embedding secret data bits. The embedding is done by taking 3D cover model to PCA coordinate system. This is done in order to make the stego model resistant to the rotation, scaling and translation transformations. The blind extraction algorithm has high embedding capacity and less distortion.

Tsai [47] proposed steganography scheme in 3D image mesh models by modifying the topology of the cover model, using recursive triangle subdivision process. The proposed approach has been shown to be robust against the vertex reordering attack but is not able to withstand the intentional attacks on the stego model. The blind extraction of secret message from the stego model fails when the stego model is attacked by noise. However, the proposed approach has high embedding capacity. The progress of various topological domain based 3D steganography approaches is shown in Fig. 7. Table 3 lists the proposed steganography algorithms/techniques based on topological domain tested using Stanford images [42] as the sample images.

## V. 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. Attacks on 3D image steganography, just like 3D image watermarking [51], can be divided into two main categories: distortion less attack and distorting attack, as shown in Fig. 10.

Table 4 Comparison of various approaches proposed for 3D models in representation domain

| Year | Authors | Algorithm/technique | Reversible | Blind | Withstands geometrical transformations |
|---|---|---|---|---|---|
| 2006 | Cheng and and Wang [21] | modified multi-level embedding procedure and representation rearrangement procedure | no | yes | yes |
| 2008 | Bogomjakov *et al.* [50] | permutation steganography based approach | yes | yes | yes |

Table 5 Embedding capacity of different approaches in three domains

| Year | Authors | Domain | Embedding capacity (in bits per vertex) | Embedding location |
|---|---|---|---|---|
| 2003 | Cayre and Macq [33] | geometrical | 0.8 | vertices |
| 2004 | Maret and Ebrahimi [34] | geometrical | 0.5 | vertices |
| 2005 | Cheng *et al.* [19] | geometrical | 3 | vertices |
| 2006 | Cheng and Wang [21] | representation | 9 | vertices and polygons |
| 2007 | Cheng and Wang [23] | geometrical | 6 | vertices |
| 2009 | Chao *et al.* [25] | geometrical | 3 | vertices |
| 2010 | Chuang *et al.* [29] | geometrical | 0.7 | vertices |
| 2012 | Tsai [45] | topological | 15.6 | vertices |
| 2013 | Thiyagarajan *et al.* [40] | geometrical | 3 | vertices |
| 2015 | Huang and Tsai [27] | geometrical | 0.5 | vertices |

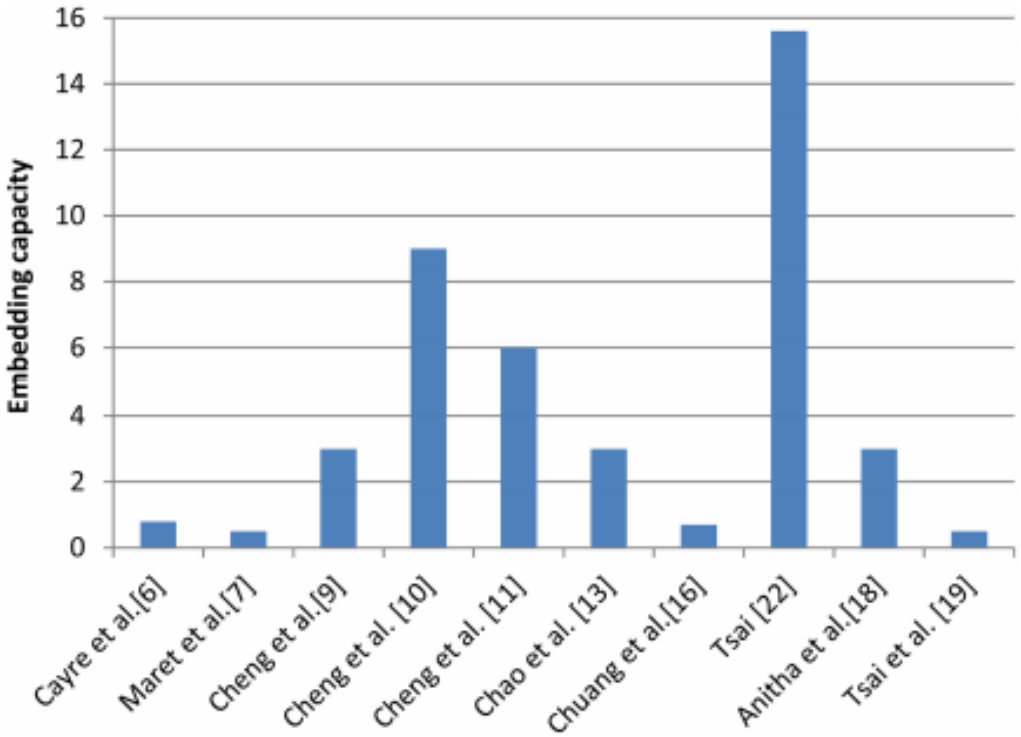


Fig. 9 Embedding capacity (in bits per vertex) of some works

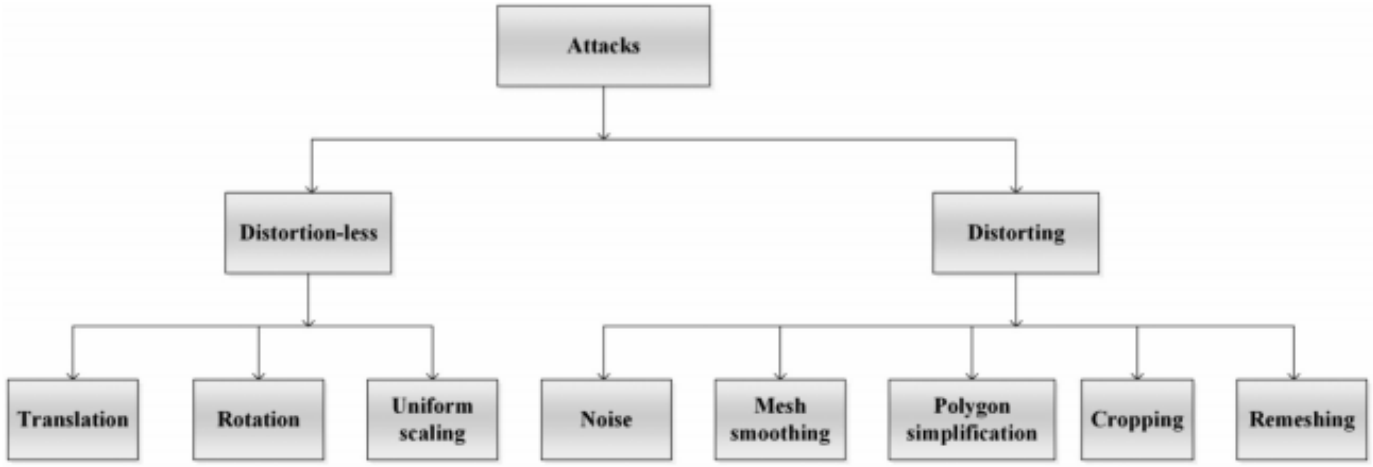


Fig. 10 Types of attacks on 3D mesh model

Distortion less attacks are those which do not cause any distortion to the geometry or topology of 3D mesh but these attacks are potent enough to harm the hidden secret message. Such attacks include rotation, uniform scaling and translation.
Other type of attack is distorting attack which changes the geometry or connectivity or both and destroy 3D mesh model along with the hidden secret message. These attacks include noise, vertex reordering, mesh smoothing, geometry or topology compression, remeshing, cropping and polygonal simplification.

Table 6 Attacks on 3D stego model

| Attack | Type | Impact on mesh model |
|---|---|---|
| translation | distortion less | no impact |
| rotation | distortion less | no impact |
| uniform scaling | distortion less | no impact |
| noise | distorting | random vertices are modified |
| mesh smoothing | distorting | mesh surface is smoothened |
| polygonal simplification | distorting | vertices are reduced |
| cropping | distorting | one or more parts of mesh are removed |
| remeshing | distorting | topology of mesh is changed |

Table 7 Some steganalytic approaches

| Year | Steganalyser | Targeted steganography Technique | Author | Accuracy |
|---|---|---|---|---|
| 2014 | Yang and Ivrissimtzis [54] | patch generation based approach [28] | Ohbuchi *et al.*[28] | 98% |
| 2014 | Yang *et al.* [57] | histogram for spherical coordinates based approach [58] | Cho *et al.* [58] | 98% |
| 2016 | Li and Bors [60] | multilayered embedding scheme [25], histogram for spherical coordinates based approach [58] | Chao *et al.* [25], Cho *et al.* [58] | — |
| 2016 | Li and Bors [61] | multilayered embedding scheme [25] | Chao *et al.* [25] | — |
| 2017 | Yang *et al.* [52] | histogram for spherical coordinates based approach [58] | Cho *et al.* [58] | 99% |

Most of the steganography algorithms proposed so far have been proved to be secure from the distortion less attacks but many algorithms fail in case of distorting attacks. Table 6 lists the various attacks on 3D stego model. These attacks can deteriorate the embedded secret data while may or may not affect the stego model.

## VI. 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 [52], 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 [52, 53]. 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 [30]. Yang and Ivrissimtzis [54] 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 [55] 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 [28] was 99% while universal steganalyser was 80% accurate against [19, 25, 36, 56]. Yang et al. [57] proposed another specific steganalyser against the steganography system proposed by Cho et al. [58] 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 cover model. The proposed steganalytic algorithm achieved 98% accuracy for detection of hidden secret data. Use of Fisher linear discriminate ensemble [59] was done in the steganalytic algorithm proposed by Li and Bors [60]. This algorithm used the simplified version of the feature set used in [54] 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. [52] proposed an improvement over their previous steganalytic algorithm [57] proposed for Cho et al. [58] 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 [61] 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 [52, 60]. Table 7 lists various 3D steganalytic algorithms proposed so far along with the accuracy of the steganalyser, where '__' stands for 'not mentioned.

## VII. 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 [5–7]. 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 [62]. 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, 62]; it might be a possibility that 3D image steganography has also been used for covert communications but the news has not broken out yet [25]. 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 [63]. 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 [64] 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.

## VIII. 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 [30, 65] 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, such as.obj,.ply,.pod,.off and many more. 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 standardised 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 [66] cannot be applied for hiding secret message in 3D mesh.

## IX. 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 [45] and with representation based approach as done in [21] has raised the overall embedding capacity of the algorithm.

(iv) Almost all geometrical domain based algorithms manage to withstand rotation, scaling and translation attacks [19, 23, 27, 29, 31, 33, 34, 40].

(v) Almost all the steganographic algorithms proposed so far have blind extraction, which is a vital feature since the transmission of both, cover model and stego model, would require a huge bandwidth (because of its size) [19, 21, 23, 25, 27, 29, 31, 33, 34, 37, 40, 41, 43–45, 47, 50].

(vi) Reversible data hiding using histogram shifting by Su et al. [39] used in 2D image steganography has inspired reversible data hiding approaches in 3D image steganography [27, 29].

(vii) Adaptive embedding (i.e. embedding secret bits more in noisy areas than smooth areas) for 3D cover models is done in very few cases [23, 45].

(viii) Proposed 3D image steganalysis techniques targets only a few steganography algorithms [19, 25, 28, 36, 56, 58].

(ix) Only one universal steganalyser for 3D image steganography techniques has been developed so far [54].

(x) A very few steganalysers have been developed so far [52, 54, 57, 60, 61].

There is a need to develop steganography algorithm which can withstand more complex mesh editing attacks such as mesh simplification, vertex reordering and so on, in addition to rotation, scaling and translation transformations (attacks). Also, the objective of achieving more embedding capacity should not be done at the cost of introducing distortion in the mesh. The algorithms proposed so far are applicable only to a particular 3D mesh format. This inhibits the use of these algorithms for the practical applications where the mesh formats used are interchangeable.

## X. 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. A survey on these two could pace up the progress of research in these fields which suffices the need of this paper.

## XI. REFERENCES

[1] Stanley, A.: 'Pairs of values and the chi-squared attack'. Master's thesis, Department of Mathematics, Owa State University, 2005

[2] Cheddad, A., Condell, J., Curran, K., et al.: 'Digital image steganography: survey and analysis of current methods', Signal Process., 2010, 90, (3), pp. 727–752

[3] Subhedar, M.S., Mankar, V.H.: 'Current status and key issues in image steganography: a survey', Comput. Sci. Rev., 2014, 13–14, pp. 95–113 [4] Johnson, N.F., Jajodia, S.: 'Exploring steganography: seeing the unseen', Computer, 1998, 31, (2), pp. 26–34

[5] Daily Telegraph: 'Terror plot horror hidden in porn film', Adelaide now, 2012. Available at http://www.adelaidenow.com.au/news/world/terror-plothorror-hidden-in-porn-film/news-story/49886a10ddeccdfb341cf72c48bbf5d5, accessed 1 August 2016

[6] Kolata, G.: 'Veiled messages of terror may lurk in cyberspace', in Science, The New York Times, 2001. Available at http://www.nytimes.com/ 2001/10/30/science/veiled-messages-of-terror-may-lurk-in-cyberspace.html, accessed 19 November 2016

[7] Wired and D. McCullagh, 'Bin Laden: Steganography master?' WIRED. Available at http://archive.wired.com/politics/law/news/2001/02/41658? currentPage=all, accessed1 June 2016 [8] Shi, Y., Li, X., Zhang, X., et al.: 'Reversible data hiding: advances in the past two decades', IEEE Access, 2016, 4, pp. 3210–3237

[9] Johnson, N., Duric, Z., Jajodia, S.: 'Information hiding: steganography and watermarking attacks and countermeasures' (Kluwer Academic Publishers, Boston, 2000)

[10] Wayner, P.: 'Disappearing cryptography' (Elsevier, Amsterdam, 2009, 1st edn)

[11] Fridrich, J.: 'Steganography in digital media' (Cambridge University Press, Cambridge, 2010, 1st edn)

[12] Cox, I.: 'Digital watermarking and steganography' (Morgan Kaufmann Publishers, Amsterdam, 2008, 1st edn)

[13] Wang, K., Lavoué, G., Denis, F., et al.: 'A comprehensive survey on threedimensional mesh watermarking', IEEE Trans. Multimed., 2008, 10, (8), pp. 1513–1527

[14] Alface, P.R., Macq, B.: 'From 3D mesh data hiding to 3D shape blind and robust watermarking: a survey', Trans. Data Hiding Multimed. Secur., 2007, 4499, pp. 91–115

[15] Nematollahi, M., Vorakulpipat, C., Rosales, H.: 'Digital watermarking techniques and trends' (Springer Topics in Signal Processing, 2017, 1st edn)

[16] Morkel, T., Eloff, J.H.P., Olivier, M.S.: 'An overview/image steganography'. Available at http://mo.co.za/open/stegoverview.pdf, accessed August 2016
[17] Xu, H., Wang, J., Kim, H.: 'Near-optimal solution to pair-wise LSB matching via an immune programming strategy', Inf. Sci., 2010, 180, (8), pp. 1201– 1217 [18] Fridrich, J., Goljan, M., Du, R.: 'Invertible authentication watermark for JPEG images'. ITCC 2001, Las Vegas, Nevada, April 2001, pp. 2–4
[19] Wang, C., Cheng, Y.: 'An efficient information hiding algorithm for polygon models', Comput. Graph. Forum, 2005, 24, (3), pp. 591–600
[20] Xuan, G., Zhu, J., Chen, J., et al.: 'Distortionless data hiding based on integer wavelet transform', Electron. Lett., 2002, 38, (25), p. 1646
[21] Cheng, Y., Wang, C.: 'A high-capacity steganographic approach for 3D polygonal meshes', Vis. Comput., 2006, 22, (9–11), pp. 845–855
[22] Celik, M.U., Sharma, G., Tekalp, A.M., et al.: 'Reversible data hiding'. Proc. Int. Conf. Image Processing, September 2002, vol. II, pp. 157–160
[23] Cheng, Y., Wang, C.: 'An adaptive steganographic algorithm for 3D polygonal meshes', Vis. Comput., 2007, 23, (9–11), pp. 721–732
[24] Li, X., Wang, J.: 'A steganographic method based upon JPEG and particle swarm optimization algorithm', Inf. Sci., 2007, 177, (15), pp. 3099–3109
[25] Chao, M.-W, Lin, C.-h, Yu, , et al.: 'A high capacity 3D steganography algorithm', IEEE Trans. Vis. Comput. Graph., 2009, 15, (2), pp. 274–284 [26] Sun, S.: 'A novel edge based image steganography with 2 k correction and Huffman encoding', Inf. Process. Lett., 2016, 116, (2), pp. 93–99
[27] Huang, Y., Tsai, Y.: 'A reversible data hiding scheme for 3D polygonal models based on histogram shifting with high embedding capacity', 3D Res., 2015, 6, (2)
[28] Ohbuchi, R., Mukaiyama, A., Takahashi, S.: 'A frequency-domain approach to watermarking 3D shapes', Comput. Graph. Forum, 2002, 21, (3), pp. 373– 382
[29] Chuang, H., Cheng, C.W., Yen, Z.Y.: 'Reversible data hiding with affine invariance for 3D models'. Proc. of IET Int. Conf. on Frontier Computing. Theory, Technologies and Applications, 2010, pp. 77–81
[30] Yang, Y.: 'Information analysis for steganography and steganalysis in 3D polygonal meshes', Durham University, 2013
[31] Ohbuchi, R., Masuda, H., Aono, M.: 'Watermarking three-dimensional polygonal models through geometric and topological modifications', IEEE J. Sel. Areas Commun., 1998, 16, (4), pp. 551–560
[32] Ohbuchi, R., Masuda, H., Aono, M.: 'Data embedding algorithms for geometrical and non-geometrical targets in three-dimensional polygonal models', Comput. Commun., 1998, 21, (15), pp. 1344–1354
[33] Cayre, F., Macq, B.: 'Data hiding on 3-D triangle meshes', IEEE Trans. Signal Process., 2003, 51, (4), pp. 939–949 [34] Maret, Y., Ebrahimi, T.: 'Data hiding on 3D polygonal meshes'. Multimedia and Security Workshop Proc., 2004, pp. 68–74
[35] Aspert, N., Santa-Cruz, D., Ebrahimi, T.: 'MESH: Measuring error between surfaces using the Hausdorff distance'. Proc. of the IEEE Int. Conf. on Multimedia and Expo (ICME), 2002, pp. 705–708
[36] Cayre, F., Devillers, O., Schmitt, F., et al.: 'Watermarking 3D triangle meshes for authentication and integrity', Research Report-5223, 2004
[37] Wu, H., Dugelay, J.: 'Steganography in 3D geometries and images by adjacent bin mapping', EURASIP J. Inf. Secur., 2009, 2009, pp. 1–10
[38] Wu, H., Dugelay, J., Cheung, Y.: 'A data mapping method for steganography and its application to images'. Proc. of the 10th Information Hiding Workshop, 2008 (LNCS, 5284), pp. 236–250
[39] Su, W., Ni, Z., Shi, Y.Q., et al.: 'Reversible data hiding', IEEE Trans. Circuits Syst. Video Technol., 2006, 16, (3), pp. 354–362
[40] Thiyagarajan, P., Natarajan, V., Aghila, G., et al.: 'Pattern based 3D image steganography', 3D Res., 2013, 4, (1), pp. 1–8
[41] Anish, K., Arpita, N., Nikhil, H., et al.: 'Intelligence system security based on 3-D image', Adv. Intell. Syst. Comput., 2017, 515, pp. 159–167
[42] 'Computer graphics at Stanford University'. Available at http:// graphics.stanford.edu/data/3Dscanrep/, accessed19 December 2016
[43] Mao, X., Shiba, M., Imamiya, A.: 'Watermarking 3-D geometric models through triangle subdivision'. Proc. SPIE, 2001, vol 4314, pp. 253–260
[44] Amat, P., Puech, W., Druon, S., et al.: 'Lossless 3D steganography based on MST and connectivity modification', Signal Process., Image Commun., 2010, 25, pp. 400–412 [45] Tsai, Y.: 'An adaptive steganographic algorithm for 3D polygonal models using vertex decimation', Multimedia Tools Appl., 2012, 69, (3), pp. 859–876
[46] Schroeder, W., Zarge, J., Lorensen, W.: 'Decimation of triangle meshes', ACM SIGGRAPH Comput. Graph., 1992, 26, (2), pp. 65–70
[47] Tsai, Y.: 'A distortion-Free data hiding scheme for triangular meshes based on recursive subdivision', Adv. Multimed., 2016, 2016, pp. 1–10
[48] Held, M, Arkin, E.M., Mitchell, J.S.B., et al.: 'Hamiltonian triangulations for fast rendering', Vis. Comput., 1996, 12, (9), pp. 429–444
[49] Chow, M.: 'Optimized geometry compression for real-time rendering'. Proc. IEEE Visualization, 1997, pp. 347–354
[50] Bogomjakov, A., Gostman, C., Isenburg, M.: 'Distortion-free steganography for polygonal meshes', Comput. Graph.

Forum, 2008, 27, (2), pp. 637–642 [51] Luo, M.: 'Robust and blind 3D watermarking'. PhD dissertation, Department of Computer Science, University of York, York, UK, 2006
[52] Yang, Y., Pintus, R., Rushmeier, H., et al.: 'A 3D steganalytic algorithm and steganalysis-resistant watermarking', IEEE Trans. Vis. Comput. Graph., 2017, 23, (2), pp. 1002–1013
[53] Fridrich, J., Goljan, M.: 'Practical steganalysis – state of the art'. Proc. SPIE Photonics Imaging 2002 Security and Watermarking of Multimedia Contents, 2002, vol 4675, pp. 1–13 [54] Yang, Y., Ivrissimtzis, I.: 'Mesh discriminative features for 3D steganalysis', ACM Trans. Multimed. Comput. Commun. Appl., 2014, 10, (3), pp. 1–13
[55] Fridrich, J., Goljan, M., Hogea, D.: 'Steganalysis of JPEG images: breaking the F5 algorithm'. Proc. Int. Workshop Information Hiding, 2002, pp. 310– 323 [56] Yang, Y., Peyerimhoff, N., Ivrissimtzis, I.: 'Linear correlations between spatial and normal noise in triangle meshes', IEEE Trans. Vis. Comput. Graph., 2013, 19, (1), pp. 45–55
[57] Yang, Y., Pintus, R., Rushmeier, H., et al.: 'A steganalytic algorithm for 3D polygonal meshes'. Proc. IEEE Int. Conf. Image Processing, October 2014, pp. 4782–4786
[58] Cho, J., Prost, R., Jung, H.: 'An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms', IEEE Trans. Signal Process., 2007, 55, (1), pp. 142–155
[59] Kodovsky, J., Fridrich, J., Holub, V.: 'Ensemble classifiers for steganalysis of digital media', IEEE Trans. Inf. Forensics Sec., 2012, 7, (2), pp. 432–444
[60] Li, Z., Bors, A.G.: '3D mesh steganalysis using local shape features'. Proc. of IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), 2016, pp. 2144–2148
[61] Li, Z., Bors, A.: 'Selection of robust features for the cover source mismatch problem in 3D steganalysis'. Int. Conf. on Pattern Recognition (ICPR), Cancun, Mexico, 2016, pp. 4256–4261
[62] 'Special Agent Ricci against alleged Russian agents', 2010. Available at https://www.justice.gov/sites/default/files/opa/legacy/2010/06/28/062810complaint2.pdf, accessed 10 July 2017
[63] '3D human lung model to shed light on respiratory diseases', www.financialexpress.com, 2017. Available at http:// www.financialexpress.com/lifestyle/science/3d-human-lung-model-to-shedlight-on-respiratory-diseases/667123/, accessed 10 July 2017
[64] '10 Types of 3D Graphics Software Worth Knowing | Animation Career Review', animationcareerreview.com, 2017. Available at http:// www.animationcareer-review.com/articles/10-types-3d-graphics-softwareworth-knowing, accessed 10 July 2017]
[65] Praun, E., Hoppe, H., Finkelstein, A.: 'Robust mesh watermarking'. SIGGRAPH '99 Proc., 1999, pp. 69–76
[66] Cox, I., Kilian, J., Leighton, F., et al.: 'Secure spread spectrum watermarking for multimedia', IEEE Trans. Image Process., 1997, 6, (12), pp. 1673–1687
[67] E. S. W. complex and Weisstein, 'Polygon mesh', in Wikipedia. Available at https://en.wikipedia.org/wiki/Polygon_mesh#/media/File:Mesh_overview.svg, accessed17 October 2016.