International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 9, Issue 11, November 2020)

Image Steganography Techniques for Security in IOT Applications

Shital Soni[1], Monika Dixit[2]

[1,2]*Assistant professor, Department of Electronics and Communication Engineering, LNCTE, Bhopal, India*

***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.**

***Index Terms*-- Image Processing, Image, 2D, 3D, Steganography.**

I. INTRODUCTION

The 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.

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.

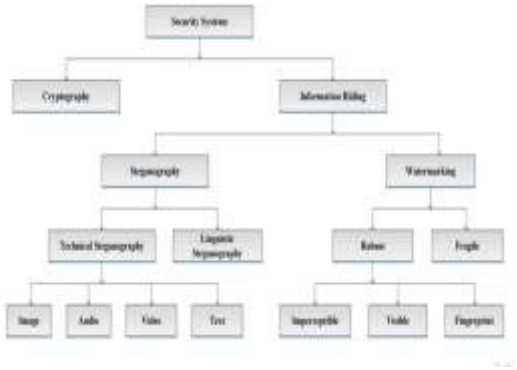

Figure 1: Methods for securing confidential information

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].

Many 2D image steganography algorithms have been developed [2]. 3D image steganography algorithms due to some inherent challenges are quite less in number.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 9, Issue 11, November 2020)

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.

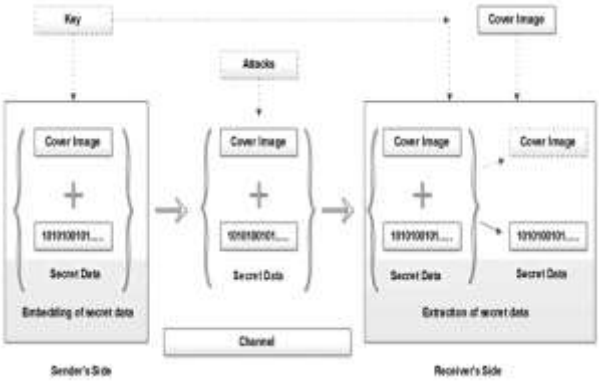

Figure 2: Generalized view of steganography system

II. Main Components Of Image Steganography

The 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.

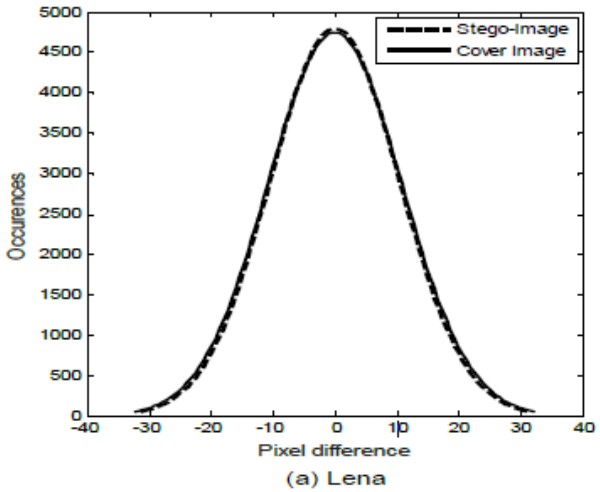

Figure 3: Pixel difference Lena image [1]

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. Attacks On 3D Image Steganography

The 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.

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.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 9, Issue 11, November 2020)

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.

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.

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%.

S. Kamil [11] a data hiding approach is designed based on the flipping approach that reduces variability and provides lesser time complexity. In the proposed method, initially, data hiding is performed using the k-bit LSB method in the cover image, and stego image is obtained. After that, the absolute difference between the cover and stego image is determined and compared with the threshold value. If the absolute difference is higher than the threshold value, then the adjacent bit of the k-bit LSB method is flipped. This process reduces the variability because flipping the adjacent bit will make the pixel value of the stego image closer to the cover image.

The simulation results show that the proposed method provides lesser variability, good visual quality, lesser time complexity than Genetic and Bayesian Optimization algorithms and the existing flip method.

X. Duan [10] Aiming at the problem that the traditional steganography based on carrier modification has the low steganographic capacity, a steganographic scheme based on Fully Convolutional Dense Connection Network (FC-DenseNet) is proposed. Since FC-DenseNet can effectively overcome the problems of gradient dissipation and gradient explosion, and a large number of features are multiplexed, the cascaded secret image and carrier image can reconstruct good image quality after entering the network. Effectively improve steganographic capacity.

Figure 4: stego-image [10]

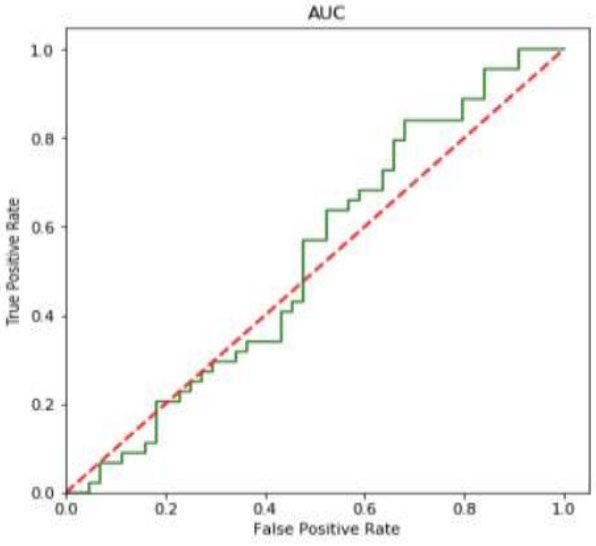

Figure 5: ROC [10]

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 9, Issue 11, November 2020)

A. G. Benedict [12] Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination. Image steganography is one of the most common and secure forms of steganography available today. Traditional steganography techniques use a single cover image to embed the secret data which has few security shortcomings.

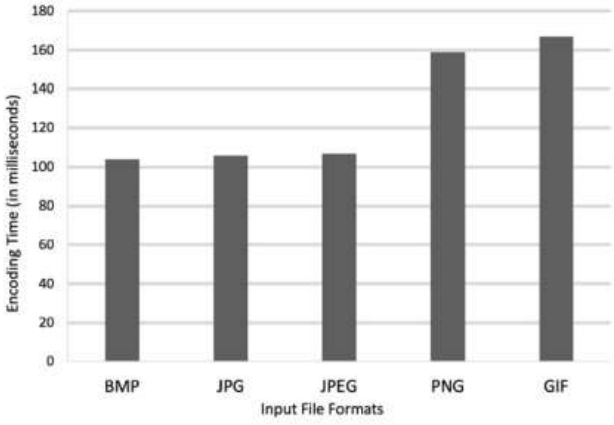

Figure 6: Encoding Speed [12]

Therefore, batch steganography has been adopted which stores data on multiple images. In this paper, a novel approach is proposed for slicing the secret data and storing it on multiple cover images. In addition, retrieval of this secret data from the cover images on the destination side has also been discussed. The data slicing ensures secure transmission of the vital data making it merely impossible for the intruder to decrypt the data without the encrypting details.

Table 1:
Result Comparison

Sr No	Method	PSNR
1	HHO-IWT [1]	25.4974
2	FC-DenseNet [10]	37.09
3	Flipping Technique [11]	5.5

IV. 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.

REFERENCES

[1] M. Hassaballah, M. A. Hameed, A. I. Awad and K. Muhammad, "A Novel Image Steganography Method for Industrial Internet of Things Security," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7743-7751, Nov. 2021, doi: 10.1109/TII.2021.3053595.

[2] T. S. Deepak and V. Enireddy, "High Payload Capacity using Steganography Combined with Cryptography," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1448-1453, doi: 10.1109/I-SMAC52330.2021.9640859.

[3] A. Sharma, A. Batta and V. K. Sharma, "A Review on Image Steganography and its Applications," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1466-1473, doi: 10.1109/I-SMAC52330.2021.9640838.

[4] J. Barker, A. Hamada and M. Azab, "Lightweight Proactive Moving-target Defense for Secure Data Exchange in IoT Networks," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2021, pp. 0317-0322, doi: 10.1109/IEMCON53756.2021.9623218.

[5] G. G, C. Ashwin, B. V. P, A. A and A. Hiremath, "Enhanced Data Encryption in IOT using ECC Cryptography and LSB Steganography," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 173-177, doi: 10.1109/ICDI3C53598.2021.00043.

[6] S. Chen, C. -C. Chang and I. Echizen, "Steganographic Secret Sharing With GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT," in IEEE Access, vol. 9, pp. 116427-116439, 2021, doi: 10.1109/ACCESS.2021.3105590.

[7] M. Z. Masoud, Y. Jaradat, A. Manasrah, I. Jannoud and A. Zerek, "HidSave: An Image Steganography Technique based on SudoKu Method for Smartphones," 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 2021, pp. 887-890, doi: 10.1109/MI-STA52233.2021.9464512.

[8] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana and S. K. Pani, "SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT," in IEEE Access, vol. 9, pp. 87563-87578, 2021, doi: 10.1109/ACCESS.2021.3089357.

[9] N. Mohamed, T. Rabie, I. Kamel and K. Alnajjar, "Detecting Secret Messages in Images Using Neural Networks," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422500.

[10] X. Duan et al., "High-Capacity Image Steganography Based on Improved FC-DenseNet," in IEEE Access, vol. 8, pp. 170174-170182, 2020, doi: 10.1109/ACCESS.2020.3024193.

[11] S. Kamil, S. N. H. S. Abdullah, M. K. Hasan and F. A. Bohani, "Enhanced Flipping Technique to Reduce Variability in Image Steganography," in IEEE Access, vol. 9, pp. 168981-168998, 2021, doi: 10.1109/ACCESS.2021.3133672.

[12] A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," 2019 International Conference on Data Science and Communication (IconDSC), 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8816946.