Analysis of Different Mechanism of Steganography based on Video: A Comprehensive Survey

[1]Abhilash Pathrod, [2]Dr. Sandeep Dubey
[1]M-Tech Scholar, [2]Associate Professor
[12]Department of Computer Science Engineering, AGNOS College of Technology
[12]RKDF University, Bhopal, India
[1]abhilashkumar8844@gmail.com, [2]sandeepdubey1981@gmail.com

Abstract- In this modern era, huge amount of information such as multimedia, text, audio, images etc. transferred every day. It is possible because of the speed of internet but there is huge possibilities of violation of rule and regulation of cyber. Due to avalanche growth of technology may also lead the violation of private data and their security. So, that we require the system which provide us a better security against these sorts of violation of private information data and their security. Digital steganography is one which gives us a better security against internet breaches. There are numerous mechanisms of steganography such as LSB, Transform based, various corner edge detection methods, and numerous sorts of steganography in term of cover data such as image, text, audio and others. In this paper, discusses the various literature of methods for steganography process.

Keywords: Steganography, Cryptography, Video, Image, Text, Multimedia.

I. INTRODUCTION

The security of information is a major concern for everybody, people wants more security over internet when they transferred data. For last decades, huge amount of security level increased over internet. The people's have worried about being trace on web at various instances, protection of privacy, identification, and most important authentication at digital work. For these reason new methods of steganography and cryptography have emerged in the past few decades [1]-[3].

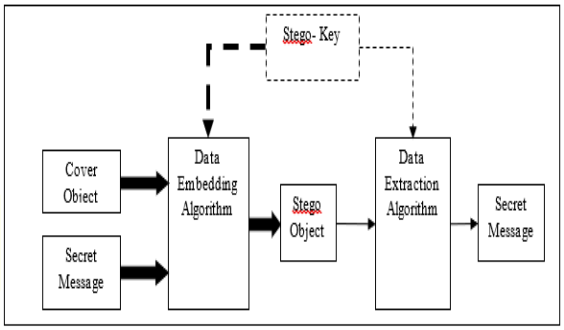

Figure 1: Generalized System Architectural Process of Steganography

As depicted figure 1 shows that the system architectural process of steganography. This is the process where medium like video, image and other digital multimedia can hide the important information with the help of numerous methods or algorithm to provide the security for particulars. On other hand, cryptography is the process where important information or data has to converted into an unappropriated sequence of data so that the

trespassers can not be crack them or exact the important information [4]-[7]. It is clear from the above discussion both systems such as steganography and cryptography are trying to provide better secure environment for the user. But it cannot be saying that the single system either steganography or cryptography offer unbreakable cyber environment. Sometimes it has recommended by the many researchers and developers to use of both mechanisms simultaneously in the single system. This system is generally known as an integrated system mechanism. The benefits of this mechanism based system is that, if the trespassers breaks the first process but still second process can save the important data and information for example if the trespassers extract the process of steganography but the do not get any information because second process still providing security to the system therefor trespassers have to require to decrypt the second process which has not an easy task [8]-[11].

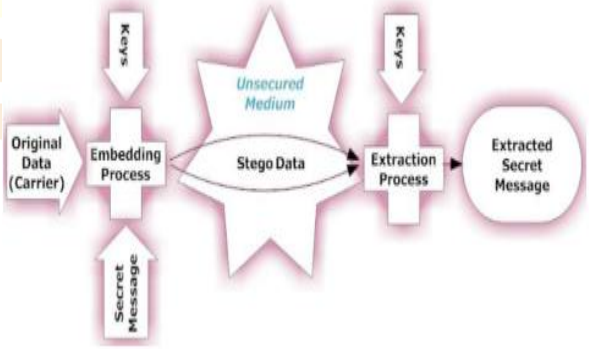

Figure 2: Generic Steps of Steganography Mechanism

The steps involved in the steganography algorithm for embedding and extraction process depicted in the above figure 2. The successful concealment of information depends upon the numerous factors such as capacity of embedding, security, imperceptibility, and robustness. The development of new steganography mechanism has to considered these factors for improving the existing mechanism.

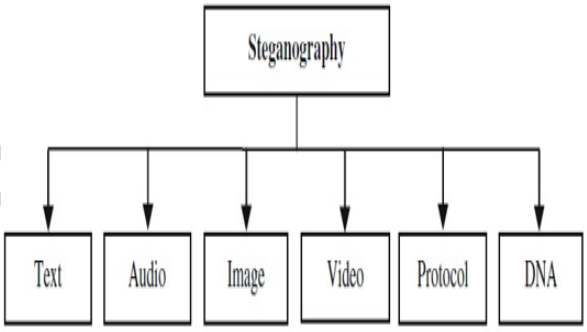

Figure 3: Steganography Types as per Cover Medium

Above depicted figure shows that the sorts of steganography as per medium of cover information.

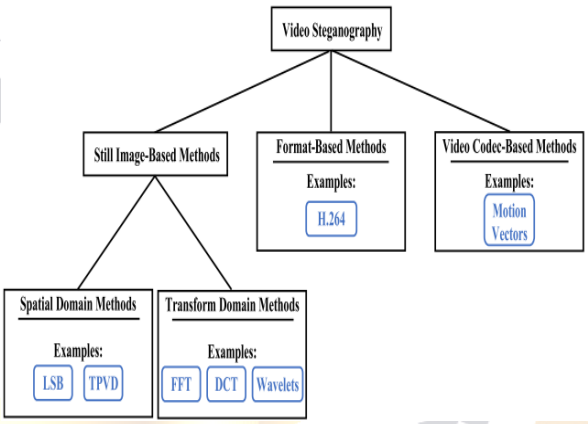

Figure 4: Steganography Factors based on Video (Categories Classification)

As above depicted figure 4 shows that the factor-based category classification of steganography algorithm based on video. The factor robustness defines the degree of resistance that provide by the secure system like steganography to the user against processing of signal and attacks. The capacity of embedding may define as the quantity of information that could be conceal into the medium of cover. The term security is the process of establishing inability towards trespassers so that they can not able to extract the information or data. An imperceptibility of the system defines as the degree of distortion in

the original cover during steganography process [12]-[15].

This section discusses the introductory part of the topic such definition, types and their classification and generalized structure of steganography system. The rest of paper summarized as follows; second section of the paper discusses the review of literature in which discusses the previous work and reported work. The problem statement discusses in the section III and last conclusion discusses in the section IV.

II. REVIEW OF LITERATURE

This section of paper discusses the literature about the steganography mechanism and draw some point as benefits, advantages, differences and problems facet by the researchers which were works in this field of steganography.

Zhang Z. et al. (2021): Reportable a bit of writing as High efficiency Video committal to writing (HEVC) can be a global trendy video coding trendy, the steganography of HEVC films has received extra and greater attention. Experimental outcomes display that the embedding functionality are frequently extensively enlarged, and as compared with the revolutionary work, the deliberate approach has ample large ability while preserving excessive visible quality. Prediction unit (PU) is one a number of the major important modern modules of HEVC; thus, PU partition mode-primarily based totally steganography is becoming a totally specific department of HEVC steganography [16].

Ding H. et al. (2021): Reported a sturdy watermarking set of rules for space compressed films towards recompression assaults with one in every of a sort QPs is proposed. The predominant contribution of this article is that we tend to use the texture and movement facts of the video content to get the superior perform of the embedded watermark adaptively, the candidate blocks on the superior function have higher hardiness to set about to the recompression assault than others Areas [17].

Mstafa J. R. et al. (2020): This paper proposes a video steganography technique altogether totally at the nook factors areas and Arnold' cat map set of rules. The projected technique encrypts the name of the sport knowledge the employment of Arnold' cat map set of rules previous to the embedding technique to boost the security of the name of the game data. For concealing the encrypted mystery data, the proposed technique 1st detects the ROI in frames of the cover video the use of SHI-TOMASI nook detector set of rules with a predefined threshold [18].

Kanwal N. et al. (2020): The projected approach offers an entire associate through storing such proof steganographic-best friend embedded on the video content, with usual encryption. although particularly simple, the approach isn't perpetually simplest a GDPR protection-through-layout aimed toward police work video but is likewise ready to being applied on resource-restricted gadgets consisting of the Raspberry-Pi processor. In fact, making a recording tool bodily tamper-evidence is past the scope of this paper, alevin though we have a tendency to pinpoint this as a downside for destiny research. Future paintings will even take into consideration the high-quality mechanism to get each rectangle's place from the video seize tool's explicit identifier [19].

Nlu K. et al. (2019): The set of rules has massive embedding capability and excellent invisibility. When completely embedded, the capability reaches one point nine% or more, the visible impact does

now no longer alternate significantly, and the PSNR price decreases inside 2db. After the name of the game message embedded information, the video bit price is accelerated inside nine%. The steganographic version primarily based totally on sport concept is improved. A hybrid steganography version that satisfies the Kerckhoffs Principle via way of means of combining the method version of the sport concept version and the content material version withinside the cowl version is proposed. The embedded framework proposed has excellent applicability. As lengthy as its miles mixed with the content material adaptive set of rules of the corresponding cowl, the steganography set of rules with distinct sorts of cowl may be designed. In addition to being relevant to video, it's also efficaciously carried out to photographs and audio [20].

Wang J. et al. (2019): In this paper, a singular IPM-primarily primarily based wholly video steganography in HEVC has been proposed. Since the preceding literature on steganography in HEVC specifically makes a specialty of the employment of the capabilities of HEVC to assemble a mapping rule or distortion feature for STC, this paper 1st indicates that the capabilities of HEVC can also be used for cover selection. The experimental effects show its practicableness and effectiveness [21].

Zhai L et al. (2019): In this paper, we tend to advise a preferred characteristic set for steg-evaluation of video steganography in every partition mode (PM) space and movement vector (MV) area. The characteristic set is constructed wholly} totally at the not unusual-place applied math traits shared through embedding domains, specifically the movement vector consistency (MVC), therefore on be changed through each PM modifications or MV modifications [22].

III. PROBLEM STATEMENT

From the study a lot of literature draw some conclusion in terms of problem statement such as robustness, imperceptibility, inability, security, and capacity of embedding.

1. The system should provide better solution as security system means have to provide very much secure system which is also a huge task for any researchers. The making of robustness of the system is also a complex task.

2. The system should be more inability against trespassers.

3. Security should be a complex process which should be follow by the system.

4. The system should good in embedding capacity with higher imperceptibility.

IV. CONCLUSION

This paper has presented a review of various mechanism of steganography based on different cover medium such as video, image, text, audio and other multimedia digital elements. As per the important factors that affect the process of steganography such as imperceptibility, inability, security, capacity of embedding and robustness are the major concern in today's scenario. This paper suggested that the integrated approach gives us a better result in all factors and parameter. So, the region of interest in this field of steganography is to present or propose a new dimension of steganography algorithms.

REFERENCES

[1] Yang, Y. and, Zhang, Z., et al.: , "High-capacity and multilevel infor^{n} hiding algorithm based on PU partition-modes for HEVC-videos.," Multi.-

media. Tools. Appl., volume 78, number. 7, pp. 8423-8446, April-2019 DOI:-10.1007/s11042-018-6859-7.

[2] Muhammad, K. and Baik, W. S.: , "A novel (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multi-media. Tools. Appl., volume. 75, number. 22, pp. 14867-14893, November 2016, DOI:-10.1007/s11042-015-2671-9.

[3] Sahu, A., and, Lakshmaiah, K., et al.: , "Dual stego- imaging based reversible data hiding using improved LSB matching," Inter. Jour. Intelligen. Engin. Syste., volume. 12, number. 5, pp. 63-73, October. 2019.

[4] Bhole, T., A., et al.: , "Steganography over video le using ran- dom byte hiding and LSB technique," in Proced. IEEE Inter. Confer. Computer Intelli. Computing. Re. (ICCIC), December-2012, pagep. 5-10, DOI:-10.1109/ICCIC. 2012.6510230.

[5] Mstafa, J., R., and, Elleithy, K., M. et al.: , "A novel vid steganography algo in the wavelet-domain based on the KLT tracking algo and BCH-codes," in Proced. Long-Island Syste., Appli. Technolo., May-2015, pagep. 1-7, DOI:-10.1109/LISAT.2015.7160192.

[6] Sahu, A., K., and, Swain, G. et al.: , "High fidelity based reversible data hiding using modified LSB matching and pixel difference," Jour. King Saud Univer. of Computer. Info. Scien., to be, DOI:-10.1016/J.JKSUCI.2019.07.004.

[7] Ma, M., and, Chen, J. et al.: , "Certificateless searchable public key encryption scheme for mobile healthcare system," Compute. Electro. Engi., volume. 65, pagep. 413-424, January-2018.

[8] Sadek, M., M., and, Mostafa, M., G., M., et al. ``Video steganography: A comprehensive review," Multi-media. Tools. Applic., volume. 74, number. 17, pagep. 7063-7094, Sepember-2015, DOI:-10.1007/S11042-014-1952-Z.

[9] Das, R., and, Tuithung, T.: , "A novel steganography method for image based on Huffman encoding," in Proced. third Nation. Confer. Emerging. Trends. Appli. Computing. Scien. (NCETACS), Marrch-2012, pagep. (14-18), DOI:-10.1109/NCETACS. 2012.6203290.

[10] Mstafa, R., J., and, Elleithy, K., M.: , "A new video steganography algorithm based on the multiple object tracking and Hamming codes," in Proced. IEEE 14th Inter. Confer. Machi. Learni. Appli. (ICMLA), December-2015, pagep. 335-340, DOI:-10.1109/ICMLA.2015.117.

[11] Shehab, A., and Hou, G., et al.: , "Secure and robust fragile watermarking scheme for medical images," IEEE. Access., volume. 6, pagep. 10269-10278, 2018, DOI:-10.1109/ACCESS.2018.2799240.

[12] Mstafa, R., J., and, Elleithy, K., M.: , "A video steganography algo. based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," Multi-media. Tools. Appli., volume. 75, number. 17, pagep. 10311-10333, September.-2016, DOI:-10.1007/S11042-015-3060-0.

[13] Douglas, M., and, Curran, K., et al.: , "An overview of steganography techniques applied to the protection of biometric data," Multi-media. Tools. Appli., volume. 77, number. 13,

pagep. 17333-17373, July. 2018, *DOI:-10.1007/S11042-017-5308-3.*

[14] Mstafa, R., J., and, Elleithy, K., M., et al.: , "A high payload video steganog- raphy algorithm in DWT domain based on BCH codes (15, 11)," in Proced. Wirel. Telecommuni. Sympo. (WTS.), April.-2015, pagep. 1-8, *DOI:-10.1109/WTS.2015.7117257.*

[15] Mstafa, R., J., and, Elleithy, K., M., "A highly secure video steganogra- phy using Hamming code (7, 4)," in Proced. IEEE. Long-Island Syste., Appli. Technolo. (LISAT) Confe., May-2014, pagep. 1-6, *DOI:-10.1109/LISAT.2014.6845191*.

[16] Zhang., Z., and, Yu., L., et al.: , "Stegano-graphy algo based on modified EMD-coded PU partition modes for HEVC-videos.", Zhang et al. EURASIP Journ. on Imag. and Vid. Process. - (2021) 2021 : 7.

[17] Ding, H., and, Li., J., et al.: , "A Compressed-Domain Robust Video Watermarking Against Recompression Attack.", IEEE. Access. 2021, *Digital Object Identifier 10.1109/ACCESS.2021.3062468.*

[18] Mstafa., R., J., and Atto., M., et al.: , "A New Video Steganography Scheme Based on Shi-Tomasi-Corner-Detector.", IEEE Access. 2020, *Digital Object Identifier 10.1109/ACCESS.2020.3021356.*

[19] Kanwal., N., and, Qiao., Y., et al.: , "Preserving Chain-of-Evidence in Surveillance Videos for Authentication and Trust-Enabled Sharing.", IEEE. Access. 2020, *Digital Object Identifier 10.1109/ACCESS.2020.DOI.*

[20] Nlu., K., and, Wang., B., et al.: , "Hybrid Adaptive Video Steganography Scheme under Game Model.", IEEE. Access-2017, *Digital Object Identifier 10.1109/ACCESS.2017.Doi Number.*

[21] Wang., J., and, Shi., Y-Q., et al.: , "A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode.", SPECIAL SECTION ON RECENT ADVANCES IN VIDEO CODING AND SECURITY 2019. *Digital Object Identifier 10.1109/ACCESS.2019.2936614* .

[22] Zhai., L., and, Ren., Y., et al.: , "Universal Detection of Video Steganography in Multiple Domains Based on the Consistency of Motion Vectors.", IEEE. Trans. on Infor. Forensi. and Secu. 2019.
DOI 10.1109/TIFS.2019.2949428,