An Analysis on Video Steganography Techniques

Ms. J. Mary Jenifer[1]
[1] Assistant Professor
Department of CSE, Aalim Muhammed Salegh College of Engineering

Ms. A.Mahalakshmi[2]
[2] Assistant Professor
Department of IT, Karpagam Insitute of Technology

***Abstract*— Steganography is the approach of hiding the name of the game message inside the information supply. It now not handiest maintains the statistics as mystery however also the existence of the statistics is kept as secret. It is used in various fields which include protection, scientific and online transactions. It is mainly utilized in stable communique. In steganography, the message can be hidden in vendors consisting of textual content documents, snap shots, audios, and movies. The goal of this paper is to provide a trendy evaluate of numerous video steganography strategies. It covers associated works, the electricity of steganography, kinds of steganography and special video steganography techniques. The comparative evaluation of various video steganography techniques is also highlighted**.

Keywords—Hiding, secret, steganography, video.

I. INTRODUCTION

DATA transmission in digital multimedia consisting of textual content, picture, audio and video plays an crucial function within the cutting-edge trend of steady communication. Secure communique is beneficial in many instances which it wishes to develop new communication strategies [1].

Steganography is one of the maximum beneficial strategies for stable conversation [2]. It is the method of covering the information within the information. In a primary steganographic approach, the cover object act because the provider of the name of the game information and the name of the game records is embedded into the quilt object. The stego object is the medium containing the embedded statistics [3].

Depending on the duvet item, information hiding can be classified into textual content steganography, picture steganography, audio steganography and video steganography respectively [4]. Present day net improvements demonstrate that films are the most useful media for sharing facts, army intelligence, medical information and banking statistics.

This paper makes a speciality of video steganography. The paper proceeds as follows. Section II explains the kinds of steganography and Section III describes the comparative analysis of video steganography strategies. Finally Section IV concludes the paper.

II. STRENGTH OF STEGANOGRAPHY

1.Undetectability

The primary strength of steganography is undetectability, which deals with how strongly the secret message is hidden. Undetectability is one of the strengths of the steganographic algorithm. The cowl item need to no longer be distorted. If the set of rules is stronger, then the secret message isn't detected via the intruders.

2.Capacity

The second strength of steganography is capability, which explains how a lot statistics may be hidden. If the steganographic method can conceal a massive quantity of facts then the steganographic approach is the most effective. Hiding extra statistics should now not affect the satisfactory of the quilt item.

3.Robustness

The third strength of steganography is robustness, which assists to avoid from intrusions. During transmission, the secret message is transmitted in the compressed shape and on the receiver aspect, the message is decompressed. During those processes, the message must now not be various and additionally the scaling and rotation troubles need to not affect the name of the game message. The steganographic algorithm ought to be such that it prevents most of these troubles and the name of the game message is transmitted to the receiver aspect secure

4.Security

Security is another difficulty of the steganographic rules

Even if an interloper finds the existence of the secret message on the quilt, it can't open due to safety. The set of rules and the important thing ought to be recognized handiest via the sender and receiver. The mystery message is protected from the unauthorized access so the message is transmitted securely in the conversation channel. A right steganographic algorithm have to satisfy these types of four homes [6].

III.Comparative Analysis of Video Steganography Techniques

Videos are the maximum crucial media for stead communique of the secret message. The existing video steganography techniques are spatial domain technique, rework area method and layout based approach.

Spatial Domain Technique

In spatial domain technique, facts hiding is without delay primarily based on pixel values. The various spatial area techniques are, Least Significant Bit [7]-[9], Bit-Plane Complexity Segmentation [10]-[12] and Pixel Mapping [13], [14].

1.Least Significant Bit (LSB)

LSB is one of the primary techniques for statistics hiding. It is likewise an simpler approach for secret communication of facts inside the spatial Domain. LSB performs an important role in the steady transmission. In this technique, picture's least enormous bit is exchanged through the records bit [7]. Different LSB strategies are indexed in Table I.

1. Bit-Plane Complexity Segmentation (BPCS)

BPCS technique is used to cover the personal information. Some of the BPCS strategies used to hiding statistics are three-D set partitioning in hierarchical timber set of rules, Frame Selected Approach, and Modified BPCS. Different BPCS techniques are listed in Table II.Pixel Mapping

3.*Pixel Mapping*

Pixel mapping approach is achieved in the spatial area. Some mathematical capabilities are used to choose the embedding pixels. Before embedding, checking is performed to find whether the selected pixel lies in the barriers of the photograph or now not. Integer Wavelet Transform and Embedding Plane Selection are a number of the pixel mapping strategies used for hiding records. Different pixel mapping strategies are listed in Table III.

TABLE I
Least Significant Bit

Technique	Description	Advantages	Disadvantages
LSB Replacement [7]	The mysterious message bit is utilized to change the LSB of casing. The speed of the video is 30 casings each second. The pixel data of the picture is concealed in the video outlines.	The classified data is sent safely and difficult for an aggressor to identify that data.	This technique requires high time complexity.
Non-Uniform Rectangular Partition [8]	It conceals an uncompressed secret video transfer in a host video transfer without bends. The segment codes are utilized to around recover the first picture.	The quality of video does not change.	The error rate is higher.
Genetic Algorithm [9]	The enhancer improves the qualities utilizing 3-3-2 LSB technique. The expense capacities with two variables are utilized by the enhancer.	The PSNR value is high.	Nonexclusive calculation works just in uncompressed area.

TABLE II
Bit-Plane Complexity Segmentation

Technique	Description	Advantages	Disadvantages
3-D Set Partitioning In Hierarchical Trees (SPIHT) algorithm [10]	This calculation plays out the pressure activity in recordings. Requested piece plane coding is utilized	Provides good video quality.	Poor embedding capacity.

Frame Selected Approach [11]	The interaction is completed utilizing advanced recordings and casing determination rationale is utilized. The data is concealed in the chose outline.	Provides high security.	Used to embed only small amount of data.
Modified BPCS [12]	The privileged intel is encoded by crossover cryptography and afterward pressure technique is applied. The mysterious key contains the data about the specific planning of privileged information.	Gives two degrees of safety.Accomplishes high inserting limit.	Less video quality.

TABLE III
PIXEL MAPPING

Technique	Description	Advantages	Disadvantages
Integer Wavelet Transform [13]	Information installing is done on uncompressed video area. The video is isolated into two sections, the sound and the picture succession.	The tremendous measure of information is inserted into the casing. The restricted information are not apparent to the natural eye.	Does not support all video formats.
Embedding Plane Selection [14]	The implanting bit planes are chose utilizing some numerical capacities and afterward pixel planning is applied.	The operations are performed in less time.	The quality of frame is affected.

B. Transform Domain Techniques

In remodel area techniques, data hiding is carried out through embedding the statistics within the converted photo acquired by making use of transformation strategies. The various transform domain strategies are, Discrete Cosine Transform (DCT) primarily based technique [15], [16], and Discrete Wavelet Transform (DWT) based approach [17], [18], [19].

1.DCT Based Techniques

In DCT based totally technique, the picture is segmented into low, middle and excessive frequency bands. The blessings of this method are high compression ratio and very low mistakes fee. Some of the DCT primarily based techniques are Bose-Chaudhuri- Hocquenghem (BCH) mistakes-correcting codes, Intra-body errors propagation-loose data hiding algorithm, DCT based totally perturbation scheme, Secret message formula and Trailing coefficients. These DCT based totally techniques are listed in Table IV.

1. DWT Based Techniques

Wavelet is a small wave and the wave oscillation is based at the time area. DWT is the latest and efficient method for hiding facts. The benefit of DWT method is that it plays each neighborhood and multi-decision analysis. The inverse wavelet remodel is used to offer the original format of the object. Some of the DWT based totally techniques used for hiding the data are Inverse two-dimensional DWT, Kanade Lucas Tomasi Tracking set of rules, Integer wavelet Transform, Arnold Transform and Channel hiding. Different DWT based totally techniques, as listed in Table V.

TABLE IV
DCT BASED TECHNIQUES

Technique	Description	Advantages	Disadvantages
The BCH Error Correcting Codes [15]	The encryption and the encoding are finished by BCH codes. The mysterious message is implanted into the DCT coefficient of the edge.	Provides high robustness and good hiding capacity.	Hides only small amount of data.
Intra-frame error propagation-free data hiding algorithm [16]	High-productivity video coding blocks are grouped. The grouping is done dependent on bury forecast mode blend.	Achieves good video quality.	The embedding capacity is low

TABLE V
DWT BASED TECHNIQUES

Technique	Description	Advantages	Disadvantages
Inverse two-dimensional DWT [17]	The mysterious message encoding is finished by the BCH codes. The private information are embedded into the DWT coefficient which has the high recurrence. The security keys are utilized.	It is secure and robust.	Poor video quality.
Kanade Lucas Tomasi (KLT) Tracking algorithm [18]	In the twofold stream, encryption and BCH codes are applied successively. The encoded message is implanted into the high and center recurrence of DWT coefficient.	Provides high embedding efficiency.	Less robustness
Channel hiding [19]	The cover video is deteriorated. The mysterious video outlines supplant the less critical wavelet band.	Offers high security.	Low PSNR value.

C. Format Based Techniques

Different video codecs can be used as a cover object. This technique is used to perform the operations of particular video formats. H.264/AVC, MPEG, and FLV are the different formats [20]-[22]. Readable records hiding set of rules, Inter prediction scheme, Scene trade detection set of rules, Multivariate regression-bendy macro block ordering, Video steganography scheme and Context adaptive variable period coding are a number of the layout based totally techniques used for hiding records. Different layout based totally strategies are indexed in TableVI.

TABLE VI
FORMAT BASED TECHNIQUES

Technique	Description	Advantages	Disadvantages
Readable data hiding algorithm[20]	The data are embedded into DCT coefficient of the frame.	High embedding capacity. Very low visual distortions.	Poor Robustness.
Inter prediction scheme [21]	Encoded sequence is used to hide the scene change information.	Simplest method. Does not affect the video quality.	Used only in uncompressed domain.
Scene change detection Algorithm [22]	MPEG motion estimation scheme is used. The operations are done in the compressed domain.	Computation cost is low. Provides high processing speed.	Poor video quality.

IV. CONCLUSION

In the technology of speedy message interchange using the net, steganography is one of the essential gear for stable communique and also protects the facts from unauthorized get admission to, so that the message is transmitted securely inside the communique channel. The paper provides a evaluation of the energy of steganography and numerous varieties of steganography. Different video steganography strategies are surveyed and its methodology, benefits, and downsides are also as compared.

ACKNOWLEDGEMENT

This work was supported in part by Anna University recognized research center lab at Aalim Muhammed Salegh College of Engineering,Avadi,Chennai.

REFERENCES

[1] M. Chen, R. Zhang, N. Xinxin and Y. Yang, “Analysis of current steganography tools: classifications & features”, *IEEE international conference on intelligent information hiding and Multimedia signal processing*, pp. 384-387, Dec. 2006.

[2] C. Gayathri and V. Kalpana, "Study on Image Steganography Techniques", *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 2, pp. 572-577, April 2013.

[3] H. K. Mohanta and J. Hyma, "A Hybrid Method with Lorenz attractor based Cryptography and LSB Steganography", *International Journal of Current Engineering and Technology*, vol.5, no. 3 , pp. 1533-1538, June 2015.

[4] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", *IEEE International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 870-875, Mar. 2014.

[5] P. Joseph and S. A. Vishnukumar, "Study on Steganographic Techniques", *IEEE Global Conference on Communication Technologies (GCCT)*, pp. 206-210, Jan. 2015.

[6] T. F. Idbeaa, S. A. Samad and H. Husain, "Comparative Analysis of Steganographic Algorithms within Compressed Video Domain", *IEEE International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1-7, Dec. 2014.

[7] S. Singh and G. Agarwal, "Hiding image to video: A new approach of LSB replacement", *International Journal of Engineering Science and Technology*, vol. 2, no.12, pp. 6999-7003, 2010.

[8] S. D. Hu and U. K. Tak, "A Novel Video Steganography based on Non-uniform Rectangular Partition", *IEEE international conference on computational science and engineering*, pp. 57-61, Aug. 2011.

[9] K. Dasgupta, J. K. Mondal and P. Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", *International Conference on Computational Intelligence: Modeling, Techniques and Applications-Elsevier*, vol. 10, pp. 131-137, Dec. 2013.

[10] H. Noda, T. Furuta, M. Niimi and E. Kawaguchi, "Application of BPCS steganography to wavelet compressed video", *IEEE International Conference on Image Processing*, vol.4, pp.2147 - 2150, Oct. 2004.

[11] H. A. Jalab, A. A. Zaidan and B.B. Zaidan, "Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation", *Journal of computing*, vol.1, no. 1, pp. 108-113, Dec. 2009.

[12] S. P. Bansod, V. M. Mane and R. Ragha, "Modified BPCS Steganography using Hybrid Cryptography for Improving Data embedding Capacity", *IEEE International Conference on Communication, Information & Computing Technology (ICCICT)*, pp. 1-6, Oct. 2012.

[13] S. Bhattacharyya and G. Sanyal, "A Novel Approach of Video Steganography Using PMM", *International Conference on Information Processing -Springer*, pp. 644–653, Aug. 2012.

[14] S. Bhattacharyya, A. Khan, A. Nandi, A. Dasmalakar, S. Roy and G. Sanyal, "Pixel Mapping Method (PMM) Based Bit Plane Complexity Segmentation (BPCS) Steganography", *IEEE World Congress on Information and Communication Technologies (WICT)*, pp. 36 – 41, 2011.

[15] R. J. Mstafa and K. M. Elleithy, "A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes", *IEEE Conference on Long Island Systems, Applications and Technology*, pp. 1 -6, April 2016.

[16] P. C. Chang, K. L. Chung, J. J. Chen and C. H. Lin, "A DCT/DST-Based error propagation-free data hiding algorithm for HEV intra-coded Frames", *Journal of Visual Communication and Image Representation-Elsevier*, vol. 25, no. 2, pp. 239–253, Feb. 2014.

[17] R. J. Mstafa and K. M. Elleithy , "A High Payload Video Steganography Algorithm in DWT Domain Based on BCH codes (15, 11)", *IEEE Wireless Telecommunications Symposium (WTS)*, pp 1-8, April 2015.

[18] R. J. Mstafa and K. M. Elleithy, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes", *IEEE Conference on Systems, Applications and Technology*, pp. 1-7, May. 2015.

[19] A. Kolakalur, I. Kagalidis and B. Vuksanovic, "Wavelet Based Color Video Steganography", *IACSIT International Journal of Engineering and Technology*, vol. 8, no. 3, pp. 165-169, June 2016.

[20] X. Ma, Z. Li, H. Tu, and B. Zhang, "A Data Hiding Algorithm for H.264/AVC Video Streams without Intra-Frame Distortion Drift", *IEEE Transactions On Circuits And Systems For Video Technology*, vol. 20, no. 10, pp. 1320 – 1330, Oct. 2010.

[21] S. K. Kapotas and A. N. Skodras, "A new data hiding scheme for scene change detection in h.264 encoded video Sequences", *IEEE International Conference on Multimedia and Expo*, pp. 277-280, June 2008.

[22] Z. Li, J. Jiang, G. Xiao, and H. Fang, "An Effective and Fast Scene Change Detection Algorithm for MPEG Compressed Videos", *International Conference on Image Analysis and Recognition-Springer*, pp. 206-214, Sep. 2006.