An Advanced Motion Vectors Using Sensitive Video Steganography

Dr.S. Senthilkumar, Dr.V. Amirthalingam, Dr.R. Bharanidharan
and M. Vimal Gautham

Abstract--- *Video steganography is considered as a technique for concealing data and mystery correspondence of the most noteworthy issues happened on the protected the information transmission in the electronic time. The video steganography plot dependent on motion vectors and straight square codes has been proposed in this paper. Our technique implants mystery messages in the motion vectors of spread media during the procedure of H.264 packing. Linear block codes have been accustomed to lessening the alteration pace of the motion vectors. In this paper, an advanced motion vector based video steganography technique is proposed. For embedding the mystery bit stream, the embedding motion vectors are chosen for the homogeneous districts of the reference outline. Since homogeneous or smooth locales contain full scale obstructs with comparative expectation blunder squares, it assists with lessening the opportunity of discovery by concealing the embedding clamor with comparative forecast mistake among neighboring large scale squares. The proficient inquiry window and polar direction based embedding strategy are utilized to improve the intangibility against standard steganalysis plans. A lot of examinations is been completed to legitimize the viability of the proposed conspire over the related existing steganographic strategies.*

Keywords--- *Video, Steganography, Advanced Motion Vector, Steganalysis, Embedding Domain.*

I. INTRODUCTION

As the fast development of rapid PC systems, for example, the Internet, information getting sneaked around during transmission turns out to be increasingly genuine. The security issues of different information correspondence by means of Internet can be tended to by Cryptography and Steganography. Steganography strategies become progressively significant in maintaining a strategic distance from information being sneaked around in light of its huge compelling to keeping others from endeavoring to decode the data covered up in the host object while the Cryptography strategy continually making the others do the unscrambling for its encoded mystery information. In this way, Steganography is a craft of concealing mystery data and make them by and large undetectable [4]. The point of video steganography is to accomplish the objective of mystery correspondence and send the mystery data to the objective side securely. Video is essentially a blend of various casings and all the edges establishing a video has a fixed edge rate. These casings are fundamental structure obstruct for the video just as for video encryption process [3]. Video Steganography might be a procedure to cover any sensibly records into a conveying video document [5].

Dr.S. Senthilkumar, Assistant Professor, Department of Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed To Be University) Salem. E-mail: senthilkumars@vmkvec.edu.in

Dr.V. Amirthalingam, Associate Professor, Department of Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed To Be University) Salem. E-mail: amirvbm14@gmail.com

Dr.R. Bharanidharan, Assistant Professor, Department of Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed To Be University) Salem. E-mail: bharanidharanr@vmkvec.edu.in

M. Vimal Gautham, M.E. CSE, Department of Computer Science & Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed To Be University) Salem. E-mail: gautham2394@gmail.com

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

With the expansion in the measure of data transmitted as of late, it has gotten imperative to choose spread records to such an extent that they can hold a huge volume of data [6]. Motion vectors are normally determined by those measures so as to evacuate the transient redundancies between outlines [7]. Contrasted and advanced picture, video has more preferences, similar to huge limit, more repetition, high correspondence quality, and heartiness [8].

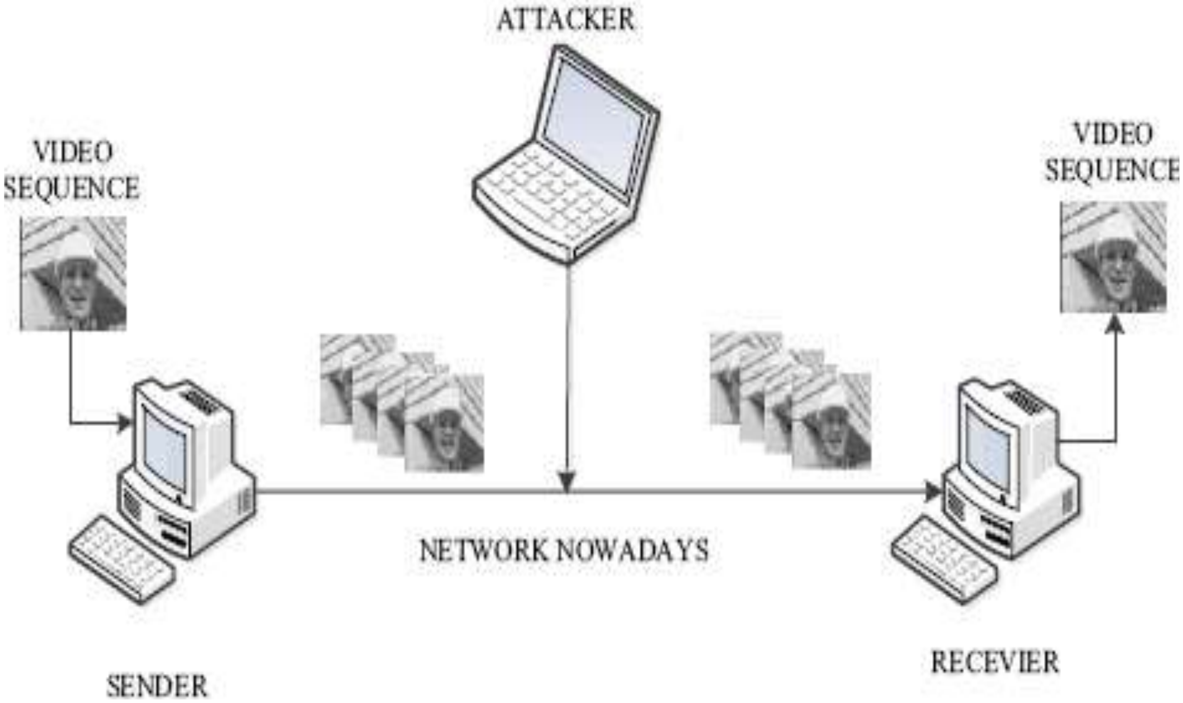


Figure 1: Video Information Sharing into Sender and Recipient through System

With the end goal of viable application, it is particularly important to structure steganalytic techniques that can all around distinguish video steganography in various areas (multi-space steganalysis for short). Be that as it may, multi-space steganalysis for computerized videos is a significant testing issue. Since the steganalytic highlights ought to at the same time consider a few embedding areas, whose factual properties may vary altogether from one another.

Different sorts of embedding areas enhance the video steganography and subsequently muddle their discovery. When distinguishing the video steganography, the current video steganalytic strategies [2] all expect that the embedding area is pre-known. Since various embedding spaces have various properties, the steganalytic highlights are in every case firmly connected with the accepted area where the embedding is completed. Despite the fact that the current steganalytic highlights can accomplish high all inclusiveness in the focused on embedding space, they are not really adjusted to recognize the video steganography in other embedding areas.

The association of the paper is as per the following. Section II represents the writing audit utilized for video steganography. Section III explains the proposed work Section IV depicts the means associated with the proposed method results. Section V concludes the paper.

II. Background Study

Eltahir, M.E., et al. [1] presents another methodology for video steganography was given. The premise of this technique considers the computerized video document as isolated edges and changing the yield picture showed on every video outline by shrouded information that doesn't outwardly change the picture. With this method, one can apply shrouded data with more space superior to other steganography media. The creators are applied the 3-3-2 methodology. The outcomes were effective on the extricated set of the video outlines.

Patel, R., et al. [2] Steganography is an incredible methods for talking clandestinely if there are ensures on the honesty of the channel of correspondence. It isn't vital for the two gatherings to consent to a particular concealing arrangement. On the off chance that the video is seen by typical individual, it is discovered that there is only the ordinary video, however just the realized people can discover the decoded message from the video. The Different encryption techniques can be concurs by the two people, so that nobody can discover the data from the video.

Every method can be executed effectively, yet on the off chance that somebody attempts to discover the stunts in the wake of realizing that somebody utilizing the stego-video record, at that point there are acceptable odds of discovering the concealed data. So as to dodge this, the some cross breed framework is utilized, so that despite the fact that somebody discovers the one procedure, it is utilized distinctly on scarcely any casings and different edges contains diverse sort of steganography and consequently complete discharge message isn't conveyed.

Rajalakshmi, K., et al. [3] Video embedding dependent on pressure strategies study the current techniques don't proficiently reestablish the pressure outlines; the pixel data is likewise lost during the changes. Further, these current philosophies increment the time and computational multifaceted nature and furthermore don't give a security of the video. Hence, to address every one of these issues on this paper, in view of our proposed work has presented a novel procedure utilizing Patch wise Code Formation (PCF) is anticipated for secure video change.

The recommended structure misuses a fix insightful pixel gathering procedure for playing out the pressure. During the pressure procedure, the videos are part into numerous patches. The intermittent area of the pixels is distinguished for each fix. The evaluated pixel areas are bound preceding the pixel esteem for the whole video. In the wake of packing the edges, the LSB calculation plays out the embedding procedure. By utilizing the video pressure basically for decreasing the quantity of bits and furthermore embedding process for keep up the security procedure.

Hu, S.D., et al. [4] Image can be apportioned adaptively by following the non-uniform rectangular parcel calculation. The segment codes acquired can be utilized to reproduce the first picture roughly. An epic picture steganography calculation is structured dependent on the non-uniform rectangular parcel calculation. Diverse introductory parcels, bivariate polynomials and control mistakes lead distinctive segment codes along these lines the client can utilize distinctive mix of them as the security key to improve the security of the steganography calculation. This paper proposes a novel secure enormous limit uncompressed video steganography calculation dependent on that picture steganography calculation.

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

Selvigrija, P., et al. [5] the Linked List strategy and Feistel Network has been presented for concealing Information inside Video. The two fundamental calculations utilized for information encryption and information embedding are Feistel Network and Linked List technique individually. The work starts with removing outlines from spread video.

At that point the encryption of information happen utilizing Feistel Network. After encryption of information, the scrambled information is implanted inside every video outlines utilizing Linked List strategy and Stego outlines are delivered. Afterward, the Stego Frames are joined to get a Stego Video. This method gives an elevated level security to the data and the nature of stego video will be equivalent to the spread video. Since Feistel Network is utilized for scrambling information, it will be hard for the gatecrashers to unscramble the data.

Zhang, Y., et al. [8] proposed a video steganography calculation dependent on trailing coefficients in rapid system, and the creators are adjust the benefit of trailing coefficients to ensure when the mystery data bit is 0, the total worth is negative, and when the mystery data bit is 1, the entirety esteem is sure, so as to guarantee the DCT coefficients of the spread video in the wake of embedding changes close to nothing, the calculation utilizing the strategy that altering the odd-numbered squares to cover up and changing the even-numbered squares to address.

III. SYSTEM MODEL

The lossless steganography requires putting away shrouded data in determination area and will requires some an opportunity to run the calculation so as to locate the particular area where concealed data can be get put away. Consequently, progressively application, the lossless calculation is getting harder to execute, and that relies upon the framework determinations.

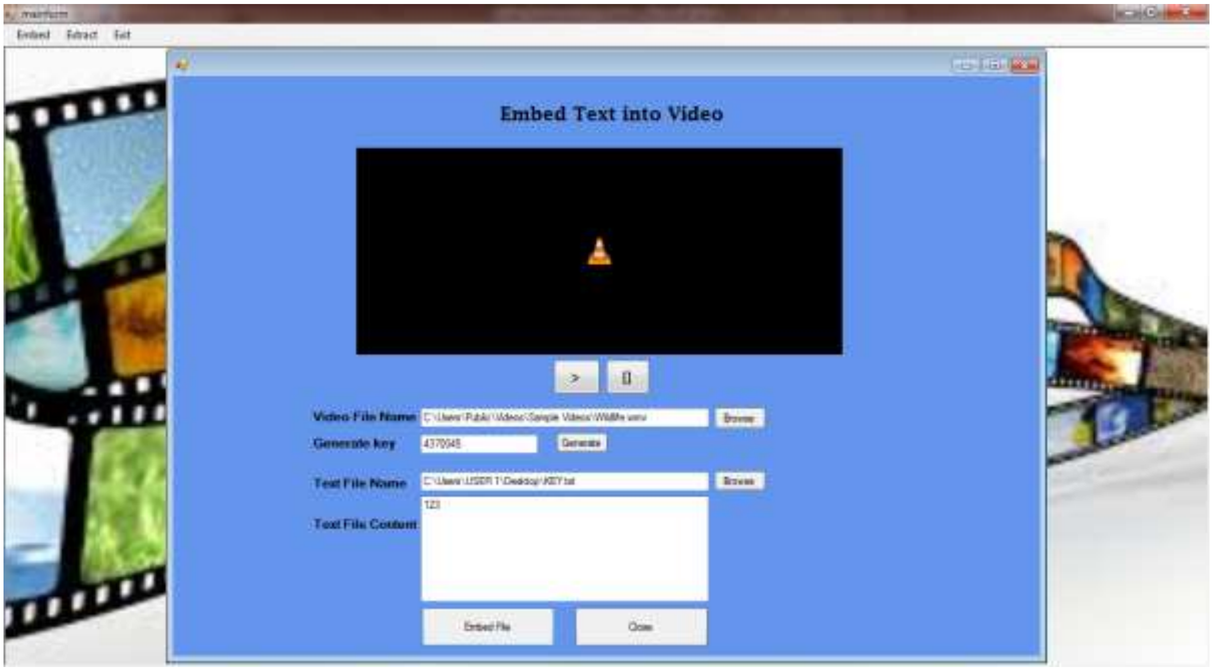
a) Linear Block Codes

Linear Block codes have the property of linearity, i.e the whole of any two codeword's is additionally a codeword, and they are applied to the source bits in squares, consequently the name straight square codes. Standard exhibit for a code C is a look-into table for all cossets of C and the primary segment contains a base weight vector for each coset. These base weight vectors are called coset pioneers of C for a given standard exhibit. Coset pioneers can be treated as the correctable mistake designs when one utilize the particular standard exhibit to decipher the got vectors.

b) Advanced Motion-vector Embedding

In this steganographic strategy, a mystery bit stream (W) is embedded with the video successions by adjusting the advanced motion vectors. In this situation, they chose even and odd motion vectors (MV_e, MV_o) are utilized for embedding. In the event that the embedding bit is 'Zero' at that point MV_e is utilized in the spot of the first motion vector and for 'One', the MV_o is utilized instead of the first ones. After modification of the bit, quantization and bit pressure is done to produce the encoded video bit-stream.

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020



Video File Name: C:\Users\Public\Videos\Sample Videos\Wildlife.wmv

Generate key: 4370048

Text File Name: C:\Users\USER 1\Desktop\KEY.txt

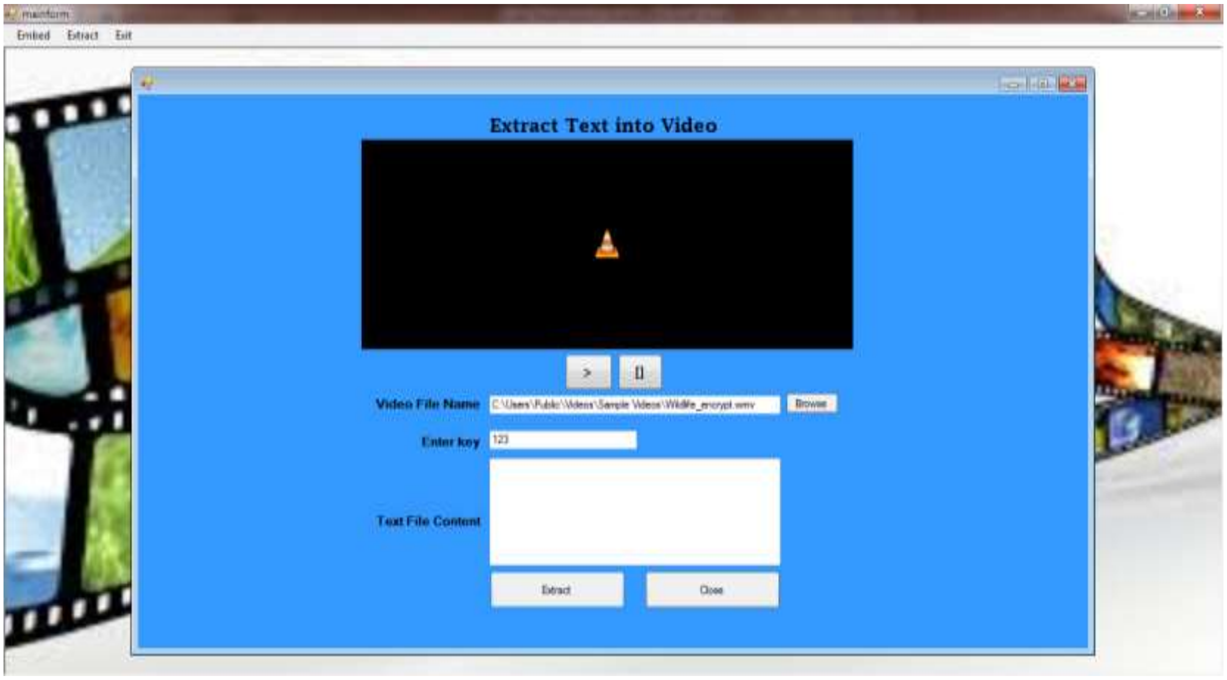
Text File Content: 123

Figure 2: Embedding Process

c) *Extraction*

The extraction method is converse of the embedding procedure. The extraction procedure is completed during video translating. The motion vectors direction point is utilized to distinguish the full scale square is even or odd.

d) *Distortion Analysis*



Video File Name: C:\Users\Public\Videos\Sample Videos\Wildlife_encrypt.wmv

Enter key: 123

Text File Content

Figure 3: Extraction Process

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

In this proposed plot, embedding is finished by modification of the motion vectors in time of video pressure. Motion vector of the comparable districts are utilized to supplant the first ones. Therefore, the new PE will be comparable with the first ones. Additionally, in time embedding, new MV is chosen by examining the MV of the neighboring MBs to such an extent that in time of re-encoding, comparable squares are chosen and the forecast mistake doesn't changed. Also, the ideal motion estimation keeps up the visual quality in the wake of embedding.

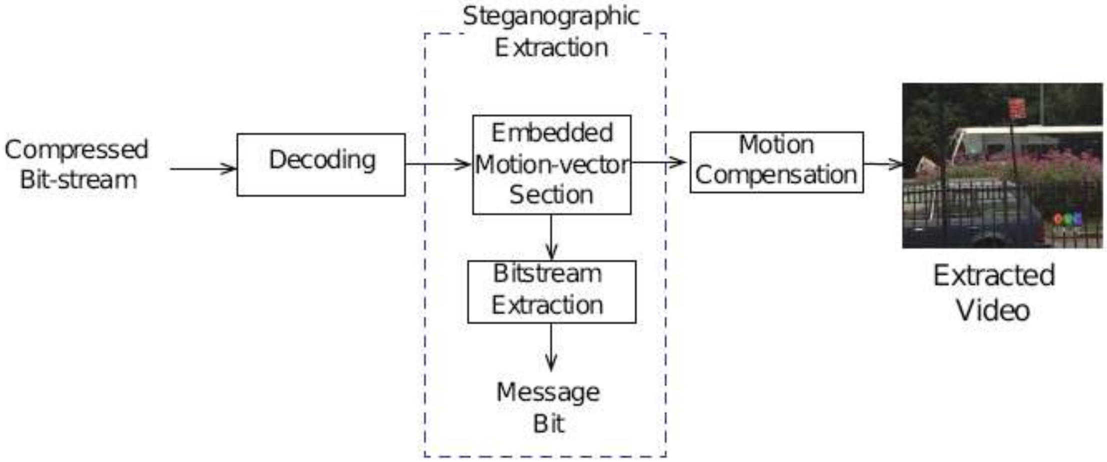


Figure 4: Motion-vector based Steganography Extraction

Algorithm 1.1 for Frame Selection

The frame with the highest amount of color information was selected as the Key frame. The following steps were followed:

Step 1:

Read the image file

Step2:

Read the R, G, B values of every pixel for every frame.

Step 3:

Calculate the sum total of R, G, B values of every pixel for each frame.

Step 4:

Select the frame with the largest RGB sum as the key frame.

Algorithm 1.2 for Frame Selection

The video information was calculated and using the duration we implemented an algorithm where the middle frame was selected as one of the key frames. Further we applied the previous approach to select another key frame and then merged the two selected key frames to get one resultant key frame. The following steps were followed:

Step 1:

Calculate the total duration of the video.

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

Step 2:

Set the start time and seconds between frames.

Step 3:

Read the input video using IMediaReader and create BufferedImages in BGR 24bit color space.

Step 4:

Read out the contents of the media file and dispatch events to the attached listener. Calculate end time

In attached listener if the selected video stream id is not yet set, select a video stream.

Step 6:

Set seconds between frames as equal to the half of the duration of the video.

Step 7:

Receive the resultant frame i.e the middle frame and the first frame in BufferedImages.

Step 8:

Merge both frames obtained in Step 7 to give a single frame i.e the key frame.

IV. Results and Discussion

In this work, the steganography embedding is completed by modifying the motion vectors in the encoded video succession. In the hour of adjustment, utilizing of the homogeneous macroblocks makes comparative expectation blunder like the first bitstream. In conventional steganalysis plans, forecast blunder of the low motion vectors is investigated in light of the fact that the higher motion vectors have higher expectation mistake and don't follow any example.

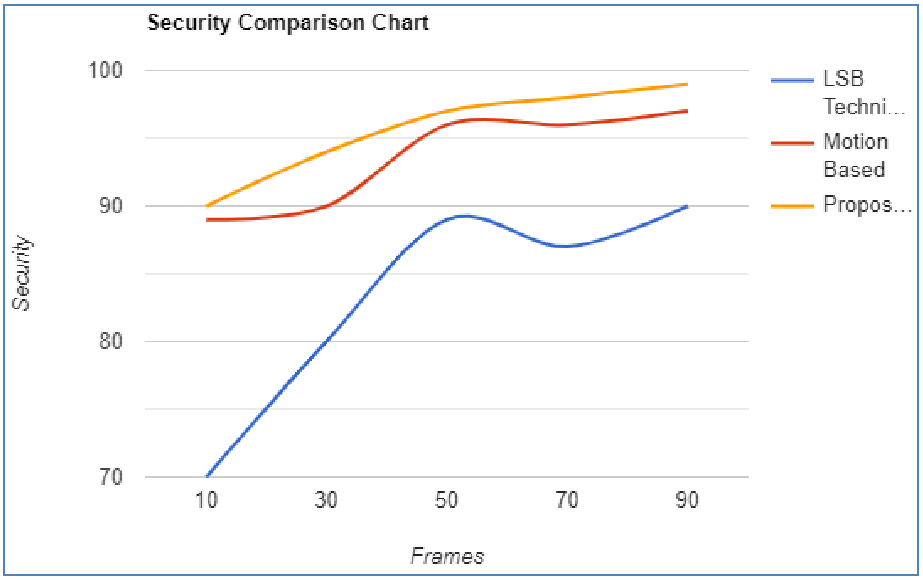


Figure 5: Security comparison Chart

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

In Figure 5 shows the compared with Lsb and advanced motion based and proposed system has been compared.

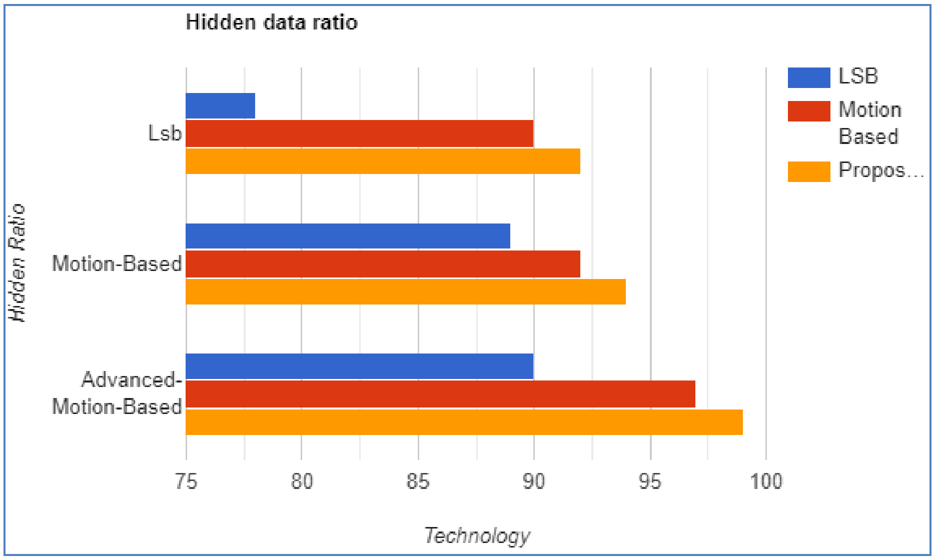


Figure 6: Hidden Ratio

In figure 6 shows the data hidden ratio has been compared with other techniques with proposed system. The new steganographic technique utilizing motion vectors and direct square codes was proposed. We embedding (*n*-*k*) bits in per n motion vectors and just the heaviness of *eb* motion vectors are altered all things considered. Along these lines, our calculation isn't just improved the embedding proficiency yet additionally diminished the MV change rate. Exploratory outcomes show that our proposed plan can implant a lot of data and can keep up great video quality too. The enormous embedding limit and visual subtle in the wake of embedding process caused our plan to can fulfill the solicitation of clandestine correspondences.

V. Conclusion

In this paper, a novel advanced motion-vector based steganography plot has been proposed for MPEG-2 video pressure procedure. Here, the mystery bit has been inserted by modifying the motion vectors in the homogeneous districts. To improve the factual imperceptibility, higher motion vectors have been utilized for embedding reason. An advanced inquiry window has been proposed used to discover the applicant large scale obstructs in the homogeneous locales for embedding. An epic embedding plan has been acquainted with modify the motion vectors with the applicant full scale square motion vectors for productive embedding with a higher possibility of imperceptibility at re-encoding based steganalysis strategies. The general list of capabilities is steganalytic of video steganography in both partition mode (PM) space and motion vector (MV) area. The list of capabilities is built dependent on the basic factual attributes common by two embedding spaces, specifically the motion vector consistency (MVC), which will be changed by either PM adjustments or MV alterations. The MVC highlight set is removed from the MV space, and accomplishes the best in class recognition exactness for a scope of steganographic techniques in PM and MV areas. In future, the plan can be reached out for 3D video steganography with profundity and perspectives independently.

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020

REFERENCES

[1] Eltahir, M.E., Kiah, L.M., Zaidan, B.B., & Zaidan, A.A. (2009). High Rate Video Streaming Steganography. 2009 *International Conference on Information Management and Engineering.*

[2] Patel, R., & Patel, M. (2014). Steganography over video file by hiding video in another video file, random byte hiding and LSB technique. 2014 *IEEE International Conference on Computational Intelligence and Computing Research.*

[3] Rajalakshmi, K., & Mahesh, K. (2017). Video steganography based on embedding the video using PCF technique. 2017 *International Conference on Information Communication and Embedded Systems (ICICES).*

[4] Hu, S.D., & U, K.T. (2011). A Novel Video Steganography Based on Non-uniform Rectangular Partition. 2011 14th *IEEE International Conference on Computational Science and Engineering.*

[5] Selvigrija, P., & Ramya, E. (2015). Dual steganography for hiding text in video by linked list method. 2015 *IEEE International Conference on Engineering and Technology (ICETECH).*

[6] Paul, R., Acharya, A.K., Batham, S., & Yadav, V.K. (2013). Hiding large amount of data using a new approach of video steganography. *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference)*.

[7] Pan, F., Xiang, L., Yang, X.Y., & Guo, Y. (2010). Video steganography using motion vector and linear block codes. *2010 IEEE International Conference on Software Engineering and Service Sciences*.

[8] Zhang, Y., Zhang, M., Niu, K., & Liu, J. (2015). Video Steganography Algorithm Based on Trailing Coefficients. 2015 *International Conference on Intelligent Networking and Collaborative Systems.*

DOI: 10.37200/IJPR/V24I5/PR2020760
Received: 20 Apr 2020 | Revised: 27 Apr 2020 | Accepted: 18 May 2020