Chapter 4

Detection of Motion Vector-Based Video Steganography by Adding or Subtracting One Motion Vector Value

Srinivas Bachu and Aravind Kumar Madam

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.78230

Abstract

In last decades the Steganography is an tremendous progress, at the same time there exist issues to detect the steganalysis in motion based video where the substance is reliably in motion conduct that makes that to detect it. Analyzing the difference between the rated motion value plays a crucial role that enables us to focus on difference between the locally optimal SAD and actual SAD after adding-or-subtracting-one operation on the motion value. Based on the motion vectors to play out the classification and extraction process at last, two features sets are been used based on the fact that most motion vectors are locally optimal for most video codec's to complete this process. The conventional approaches announced the technique for proposed prevails to meet the requirement applications and detecting the steganalysis in videos compare in the literature.

Keywords: adaptive filters, SNR, MSE, LMS, NLMS

1. Introduction

To detect the presence of secretly hidden data in an object is the main objective of steganalysis. Video, audio and images are digital media file that are ideal cover object for steganography to install a secret message. By using measurable descriptor, some empirical spreads are somewhat difficult to show precisely besides which considerably confuses recognition of embedding changes. From cover and stego objects the location can't be founded on assessments of the basic probability distributions of statistics removed except for a couple of pathological cases. Rather, detection is normally given a role as a classification administered issue executed by utilizing machine learning [1].

Although there exists an extensive variety of different machine learning tools, support vector machines (SVMs) appear to be by a wide margin the most popular choice. This is because of the way that SVMs are upheld by a strong mathematical cost inside the statistical learning hypothesis and based on the fact that they are impervious to overtraining and per-outlines rather well despite when the element dimensionality is identical or greater than the traverse of the training set. Moreover, executions of productive open source are available for download and utilize easy.

The SVM training complexity, however, development cycle slows down even for the issue of moderate size, as the complexity of calculating the Gram Matrix representing the kernel is proportional to the square of the product of feature dimensionality and the size of training set. Moreover, in the number of samples training at least quadratics is itself in training. To the analysis the ensemble classifier give more freedom, without constrain on feature dimensionality who can now design the feature virtually and the size of training set through a much faster development cycle to build detectors.

Based on the steganalysis algorithm early features used just a few dozen features, e.g., discrete cosine transform (DCT) features, changing an image utilizing higher request snapshots of wavelet coefficient, quadratic mirror filter and binary similarity metric of 72 higher request snapshots of coefficients got. With the desire the increased sophistication of steganography algorithm, to use the feature vector of increasingly higher vector dimensionality to detect steganography more accurately prompted steganalyst. The set of feature designed for the images JPEG portrayed in utilized features and twice its size by Cartesian calibration was later stretched out, while feature vector dimensionality of 324-and 486 were proposed in and individually. The pixel difference in the second-order Markov model spam set has a dimensionality of 686. Additionally, it builds beneficial computed from different domain to merge features to increase further diversity. In a key dependent domain the dimensionality of 1234 cross-domain features (CDF) set demonstrated particularly successful against YA that make embedding changes.

Various number of Eigen vectors are selected by utilizing different systems. The Eigen vectors are supplanted to enhance the accuracy and also the data compression is done based on the largest K Eigen value. The FERET (Facial Recognition Technology) database was created by Moon and Phillips (1998) to estimate and compare the single step of the face recognition approach. The experimental results of present work presenting the comparisons distance measure over the real time results of the trained set of images, videos [2].

1.1. Cryptography

The process of the methods such cryptography and the steganography both are almost same. In existing, those methods have the wider area but now, the recently developed method is the sub domain of the existing one. Here, the original sensitive information's are encrypted by utilizing the cryptography method. This encrypted information's are hard to recognize by others. These methods are also known as the interrelated process, here, initially, the sensitive information's are encrypted then the stego-tool is utilized to hide the encrypted data. Compared with other methods, the stego-tool is worked efficiently to hide the sensitive data [2, 3]. In the cryptography process, the information's are shared in a secret manner or chippers between the users. **Figure 1** shows the process of the cryptography method.

http://dx.doi.org/10.5772/intechopen.78230

Plain text is the data or original message as input that is fed into the algorithm. By using any cryptographic algorithm the process of Encryption that modifies the plain text as cipher text. The encrypted message of the cipher text is the mix of the secret key and the original message. Using a secret key to get the original plain text decryption is the reverse process of encryption is used. Without using key for gathering original information of the cipher text cryptanalysis is the way to study the methods. To produce original plaintext the algorithm of decryption takes the secret key and cipher text.

From unauthorized persons to conceal the information the first raw message, alluded to as plaintext, is changed over into a random cipher text. To be changed the original message is said as text plain, from the change the message coming about is the text cipher. A plain content into a cipher text the procedure of is called encryption. The Decryption is the reverse process. The process of encryption contains a key and algorithm. The algorithm is controlled by key.

To design an encryption technique is the objective that would be impossible or very difficult for an unauthorized party. By using the secret key, a user can recover the original message only by decrypting the cipher text. The algorithm will create different output depending upon the secret key. The output of the algorithm changes if the secret key changes.

The conventional encryption security depends on several factors. The algorithm of encryption must be intense. The message of the decryption ought to be troublesome. The algorithm is dependent on the secrecy of the key. To keep it secret in this way, it is mandatory.

The message is denoted as A and the k is denoted as encryption key, the process of encryption will be write as,

$$B = En\ (K, A). \tag{1}$$

$$A = De\ (K, B). \tag{2}$$

Here the cipher text is meant as B. With key K to encrypt the message An En is a capacity. The opposite procedure of description DE is the En encryption.

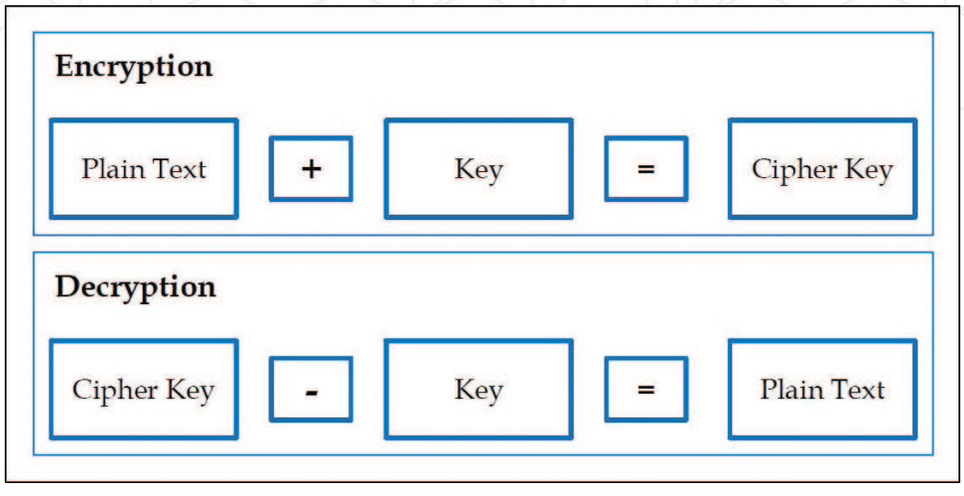

Figure 1. Process of cryptography.

$$\begin{aligned} \text{Example}: \quad & \text{Plain text } (X) = \text{This is a sample text, } K = \text{strrev}(X) \\ & \text{Cipher text } (Y) = \text{txet elpmas a si siht.} \end{aligned} \tag{3}$$

To K or X watching, Y yet not approaching an opponent, will attempt to recuperate K and X. It is accepted that the Opponent has learning of the decryption (De) and encryption (En) algorithms.

1.2. Steganography

The process of the Steganography is, the sensitive information about the audio of the video file is hiding and the hided information is not hacked and seen by other unknown persons. If the unknown persons try to hack the crypted data, they are confused, because both the cryptography and the steganography methods have the same process to hide the sensitive information. Nevertheless, the steganography is efficient method because the data are encrypted without knowing others.

The term Steganography is taken from Greek word. The words Steganos and graptos are combined to form the term Steganography. The meaning of 'Steganos' is the covered and the meaning of 'graptos' is the writing. By using this method, the digital information is converted into audio or video files. The inverse process of the Steganography is known as the Steganalysis. The concealed data are detected by using this Steganalysis (**Figure 2**).

1.3. Video steganography

Among the different kinds of steganography the video steganography is one of the variants of steganography. The info media is a video document in video steganography. The video steganography forms are appeared in **Figure 3**.

Signature is the message original that is fed into the cover media. As the cover media the video frames are taken. Key is the method for organizing divided computerized signature into the cover media. Utilizing any cryptographic algorithm the procedure of encryption is arranging

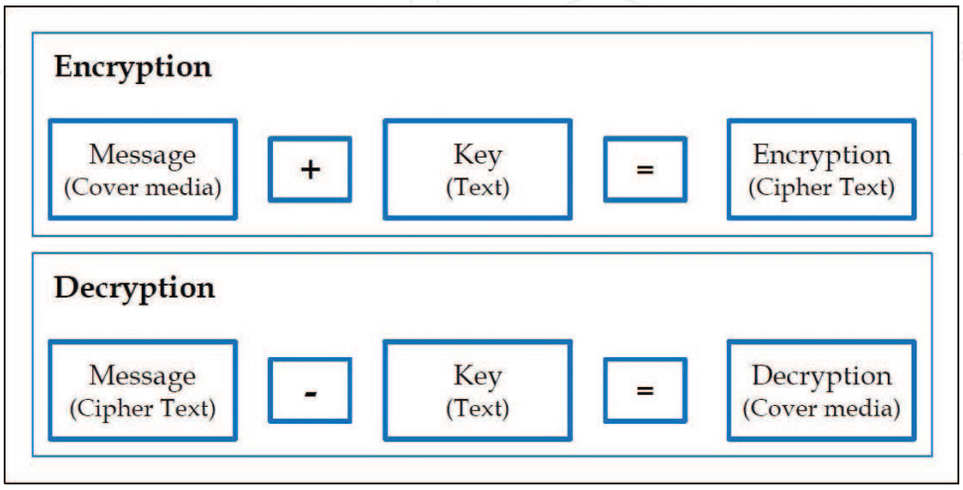

Figure 2. Process of steganography.

http://dx.doi.org/10.5772/intechopen.78230

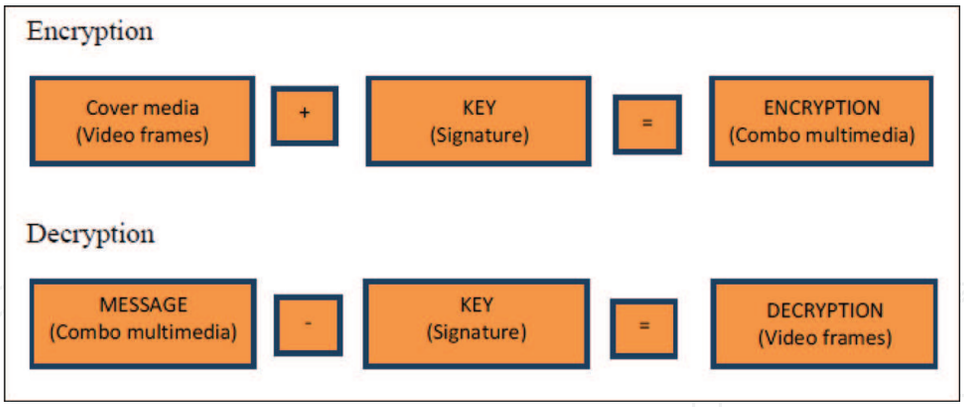

Figure 3. Process of video steganography.

partitioned digital signature into the cover media. The secret key and the first message are the mix of cipher data. Utilizing secret key to get original information the decryption is the inverse process of encryption, which is used.

2. Literature survey

In 2004 for binary images a basic data hiding technique was proposed by Liu and Chang [4]. At the edge part of host binary image the proposed strategy installs secure data. To discover the edge pixels of host binary image the distance matrix mechanism is utilized. For picking the most appropriate one to consider the network of the neighborhood around alterable pixels then the weight mechanism is utilized. To appropriate the embedding data into the general image an irregular number generator is utilized for the security and quality thought. These technique not just implants a lot of data into host binary image yet additionally can keep up quality of image.

In 2005 in view of pixel value differencing (PVD) and least significant bit (LSB) Replacement strategies a novel stenographic strategy was proposed by Wu et al. [5] so as to give am imperceptible stego quality of image and to enhance the capacity of the shrouded secret data. To segregate between smooth areas and edge areas of cover image the pixel value differencing (PVD) strategy is utilized. By LSB technique the secret data is covered up into the smooth areas of cover image in the edge areas while utilizing the PVD strategy. In the edge areas the proposed techniques store data as well as in smooth areas in this manner it can conceal considerably bigger data and keeps up a decent visual nature of stego picture.

A no-reference video quality metric that aimlessly assesses the quality of a video was proposed by Carli et al. [6] in 2005. To embed a fragile check into perceptually critical zones of the video frames they had utilized block based spread spectrum embedding strategy. To describe the perceptual significance of a region they utilized an arrangement of perceptual features that are color, contrast and motion. On receiver side from the perceptually essential territories of the decoded video the check is extricated. By figuring the degradation of the extracted check then

a quality measure of the video is acquired. On perceptually critical areas of the video frame by utilizing basic embedding system along these lines quality of a compressed video is assessed.

In binary image a novel strategy for hidden data was proposed by Tseng et al. [7] in 2007. For turning to choose the most appropriate pixel a weight mechanism is utilized. To counteract boundary distortion and to enhance the visual quality of stego image, the boundary check is performed. For watermarked image this strategy accomplished a decent visual quality and has embedding high capacity.

Utilizing minimum significant piece to hide data in a colorful image a novel technique was proposed and all in all the art and science of steganography was talked about by Mehboob and Faruqui [8] in 2008. After the header this technique cleaves the data in 8 bits and to hide data utilized LSB. For hiding data so they demonstrated LSB strategy is the most suggested than alternate techniques that require filtering and masking.

In 2010, LSB substitution and on four pixel differencing for gray level images a novel stenographic strategy was proposed by Ould Medeniand and El Mamoun Souidi [9]. In the most piece of the pixel where K is chosen by the quantity of one for hiding the secrete data into the every pixel they utilized K-bit LSB substitution technique. For the PSNR measure this strategy gave best values, which imply that there were no enormous distinction between the stegno and original image.

To execute a strong dynamic technique for data hiding to make stegnalysis a convoluted undertaking and additionally to enhance the capacity of the secret data assignment they tried in view of PVD and LSB substitution a data hiding strategy was proposed by Mahjabin et al. [10] in 2012. dynamic embedding and efficient algorithm was proposed with an imperceptible visual quality here that not just shrouds secret data and capacity expanded for the attackers yet in addition make mystery code breaking a decent irritation. Lower image degradation and an increased embedding capacity accomplished this strategy with enhanced security when contrasted with the substitution technique LSB and a few data hiding existing strategy.

In 2012 in RGB lossless images for hiding text messages an enhanced stenography approach was proposed by Ankit Chaudhary and JaJdeep Vasavada [11]. Inside specific image portions by randomly appropriating the instant message over the entire image as opposed to clustering the security level is expanded. For storing data by using all the color channels they expanded storage capacity and giving the compression of source text message. For hiding the message by changing just a single rent critical piece per color channel the degradation of the images can be limited, in the original image causing a next to no change. In this way, while acquiring minimal quality degradation this strategy enhanced the capacity and expanded the security level.

In 2012 for video stenography a secured has based LSB technique was proposed by Dasgupta and Mandaland Paramartha Dutta [12]. To disguise the nearness of sensitive data paying little heed to its arrangement in spatial domain this system uses cover video files. With LSB technique in the wake of looking at the proposed technique it is discovered that the execution examination of proposed technique is quite reassuring. In multiple frames as the message can be embedded in video stenography the upside of this technique is that the span of the message does not make a difference.

To recover the hidden information and in computer video file to hide data containing content a strategy was proposed by Bodhak and Gunjal [13] in 2012. Utilizing DCT and LSB Modification strategy in a video file such that the video does not lose its functionality by embedding the text file this can be outlined. The imperceptible modification is connected by this strategy. To identify hidden information to an eavesdropper's failure this proposed strategy strives for high security.

In 2012 in light of Huffman encoding for image stenography a novel method was proposed by RigDas and Themrichon Tuithung [14]. By adjusting the least significant bit (LSB) of each of the pixel's powers of cover image over the secret image/message before implanting and each piece of Huffman code of mystery Image/message is inserted inside the cover image the Huffman encoding is performed. The measure of the Huffman table and Huffman encoded bit stream are installed inside the image cover, to the beneficiary so that the stego-image moves toward becoming independent data.

In a spectrum (change) area of a digital medium (video, audio and image) the issue of separating indiscriminately data embedded over a wide band was considered by Li et al. [15] in 2013. In HOSTS by means of multicarrier spread-spectrum embedding to look for obscure data hidden we build up a novel multicarrier/signature iterative generalized least squares (M-IGLS) center strategy. Nor the embedding transporters neither the original host is accepted accessible.

3. Proposed methodology

3.1. Assumptions based steganography for motion vector

i. In the event that the stego noise is encrypted or encoded before embedding to be independent of $V_{k,l}$ the stego noise $\eta_{k,l}$ is expected and of each other, which is a sensible supposition.

ii. From the compressed video MV values directly acquired are locally optimal, which implies hiding information on MVs will move the local optimal MVs to non-optimal.

3.2. Based steganalysis MV value add-or-subtract-one

By steganography to break down the impact created on MVs the add-or-subtract-one (AOSO) operation is then exhibited, trailed by the extraction of new feature AoSo. The universal applicability of AoSo feature is broke down contrasted with existing highlights at long last.

Inter-MB coding generic structure is appeared in **Figure 4**. Inter-MB coding was presented by distortion that is spoken to by the contrast between recreated MB and current MB, and is principally because of truncation and quantization. With the Laplacian probability density function (PDF) since the dispersion of the 2D-DCT coefficients of PE can be roughly demonstrated as

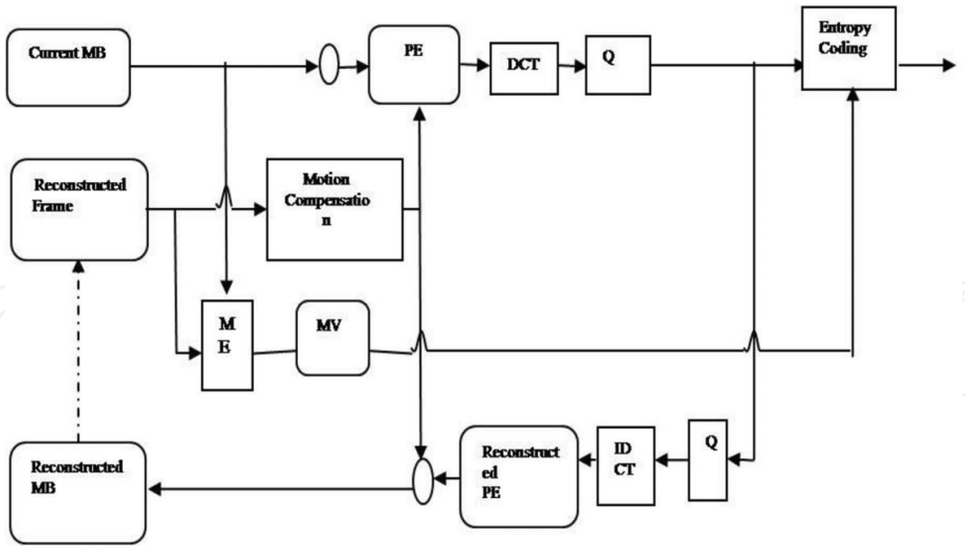

Figure 4. Inter-MB coding generic structure.

$$f_y(y) = \frac{\alpha \exp(-\alpha|y|)}{2} \tag{4}$$

Where distribution of parameter is represented as α, with the accuracy of the motion estimation and it is mainly correlated. To get the coefficients y are then quantized

$$\tilde{y} = iQ, \quad if\ \mathrm{y} \in \left[\left(\mathrm{i}\text{-}\frac{1}{2}\right)\mathrm{Q}, \left(\mathrm{i}+\frac{1}{2}\right)\mathrm{Q}\right] \tag{5}$$

Where Q is the quantization step and i is an integer. The probability of the quantized coefficients can be calculated by

$$\mathrm{P_i} = \int_{\left(\mathrm{i}-\frac{1}{2}\right)}^{\left(\mathrm{i}+\frac{1}{2}\right)} f_y(y)dy \tag{6}$$

Thus the PDF of the residual signal introduced by quantization is

$$f_z(Z) = f_{|y-\tilde{y}|(|y-\tilde{y}|)} \tag{7}$$

and

$$E[Z] = \frac{\tanh\left(\frac{\alpha Q}{4}\right)}{\alpha} \tag{8}$$

E [ε] ∈ (0, Q/4] is positively associated with Q, and is negatively correlated. To α and Q since the distortion of the coefficients DCT is connected, to α and Q likewise related the distortion of the SAD. The more genuine the distortion of the SAD might be is the bigger Q is and the littler α. At the point when motion estimation is much mistaken the worst case happen (e.g., the ME strategy is outlandish, the video content is FAST-moving and of complex texture) and with a

large quantization step the DCT coefficients are compressed (e.g., the video bit rate of is set too little, or a huge incentive to a region around the quantization step is restricted).

4. Results and discussions

For lossy compressed images as quality estimation the PSNR is most usually utilized. The original image maximal power is the ratio of PSNR and twisted image noise power. In a wide unique range on the grounds that the powers of signals are for the most part, so it is spoken to in the logarithmic domain (**Figures 5–8**).

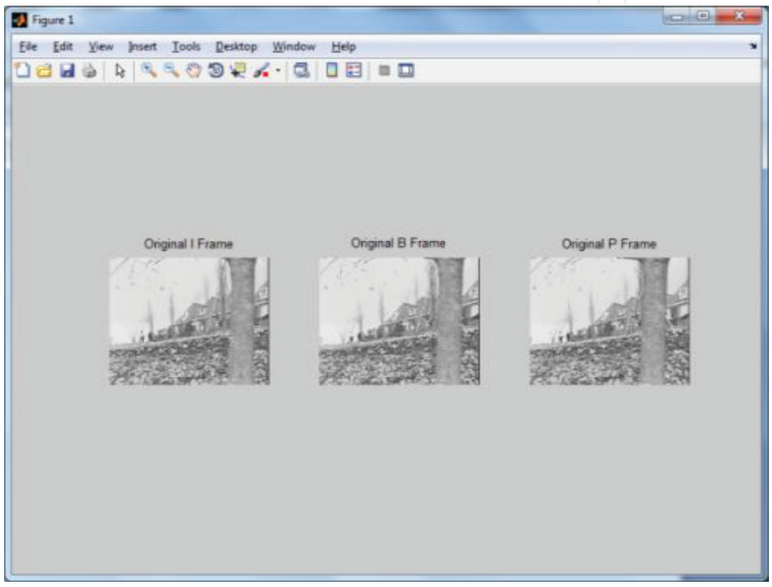

Figure 5. IBP frames chosen for embedding.

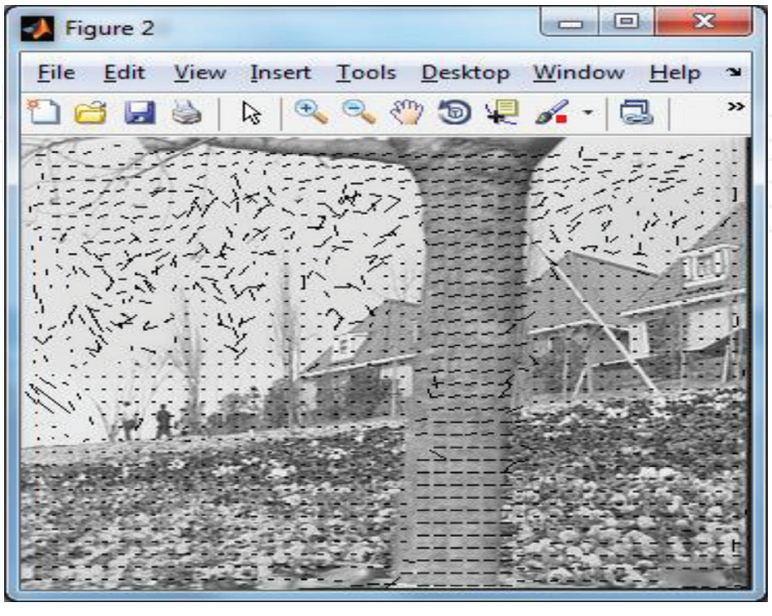

Figure 6. Motion vectors estimated.

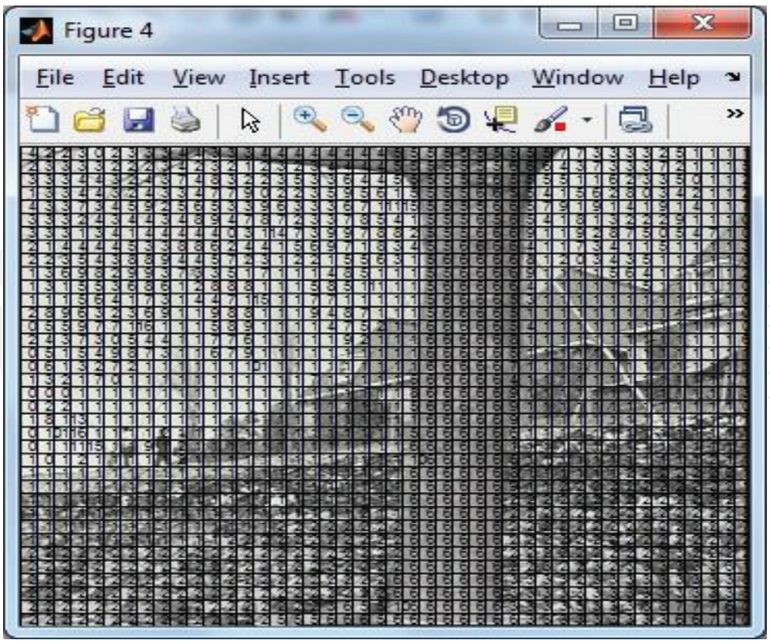

Figure 7. Macro block based processing.

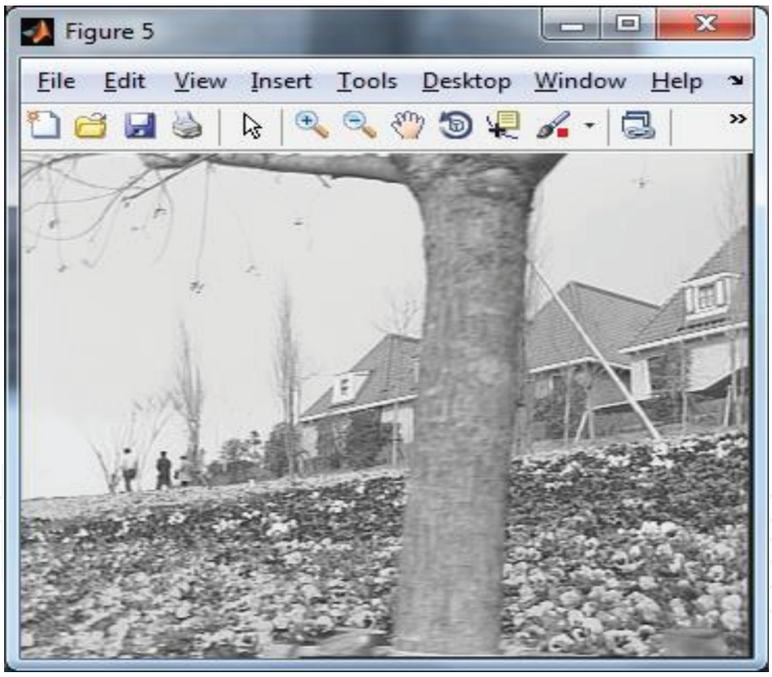

Figure 8. Frame after embedding data.

The most significant difference between the error SSIM metrics and sensibility is the extraction of structural information. The luminance we see in a scene is the result of the illumination and the reflectance; however the structure of a protest is autonomous of the illumination. As the objective is to extricate the structural information from objects in an image, we wish to isolate the impact of the illumination. In other words, the structural information we consider should be independent of the luminance and the contrast.

In diagram X and Y are input signals to be measure. First, their luminance is compared. Second, the mean intensities are removed from each signal such that $\sum_{i=1}^{N} x_i = 0$ and $\sum_{i=1}^{N} y_i = 0$, and the signal contrast are estimated by the standard deviations. Third, each signal is normalized by dividing its standard deviation, so that the two signals being compared have both unit

Figure 9. Data embedding process in frame by frame.

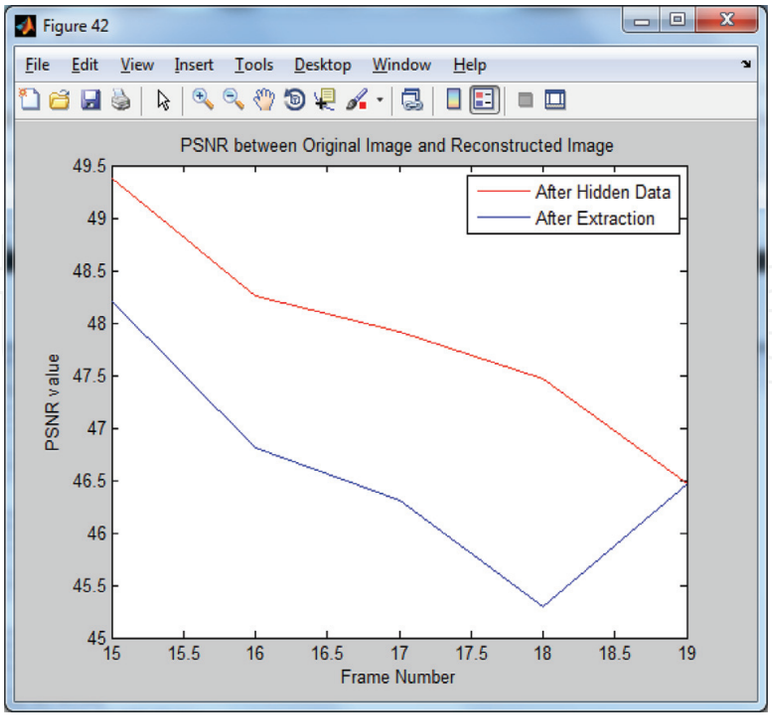

Figure 10. PSNR between original image and reconstructed image.

standard deviations. Next, the structure comparison is conducted on the two normalized signals. Finally, the three components: luminance, contrast, and structure comparison, are combined together to yield an overall similarity measure $S(X, Y)$. Here, the comparison functions should be defined such that $S(X, Y)$ can satisfy the three following conditions that should come to an image structure (**Figures 9** and **10**).

A. Luminance Comparison

B. Contrast Comparison

C. Structure Comparison

5. Conclusion and future scope

This paper exhibited the ME method for searching the locally optimal MV value, and additionally the proof that MV construct steganography has slight impact based on SAD. To observe whether the actual MV is locally optimal, the operation of AoSo on MVs is employed and how deviates the actual SAD from the locally optimal one. For steganalysis the features based on AoSo activity are removed.

Analyzing the difference between the rated the motion value plays a crucial role that enables us to focus on difference between the locally optimal SAD and actual SAD after adding-or-subtracting-one operation on the motion value. Finally based on the motion vectors to perform the classification and extraction process two features sets are been used based on the fact that most motion vectors are locally optimal for most video codec's to complete this process. In the literature to conventional approaches announced the technique for proposed prevails to meet the requirement applications and detecting the steganalysis in videos compare.

Author details

Srinivas Bachu[1]* and Aravind Kumar Madam[2]

*Address all correspondence to: bachusrinivas@gmail.com

1 Department of Electronics and Communication Engineering, KL Deemed to be University, Hyderabad, Telangana, India

2 Department of Electronics and Communication Engineering, GVVIT, Bhimavaram, Andhra Pradesh, India

References

[1] Wang K, Zhao H, Wang H. Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Transactions on Information Forensics and Security. May 2014;**9**(5):741-751

[2] Srinivas B, Priyanka O. A novel approach for detection of motion vector-based video steganography by AOSO motion vector value. Proceedings of International Conference on Innovations in Computer Science & Engineering. Springer-AISC Series. **413**:225-233

[3] Kumar S, Biswas M. New method of noise removal in images using curvelet transform. In: International Conference on Computing, Communication & Automation (ICCCA), 15–16 May 2015, Noida, India

[4] Liu T-H, Chang L-W. An adaptive data hiding technique for binary images. In: 17th Proceedings of the International Conference on Pattern Recognition (ICPR) 2004. Cambridge, UK; 20 September 2004

[5] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings–Vision Image and Signal Processing. 2005;**152**(5):611-615

[6] Carli M, Fariasy MCQ, Drelie Gelascaz E, Tedesco R, Neri A. Quality Assessment using Data Hiding on Perceptually Important. IEEE AREAS0-7803-9134-/05/$20.00©;2005

[7] Tseng H-W, Feng-Rong W, Hsieh C-P. Data hiding for binary images using weight mechanism. In: Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007); Kaohsiung, Taiwan; Nov. 2007. pp. 26-28

[8] Mehboob B, Faruqui RA. A steganography implementation. In: International Symposium on Biometrics and Security Technologies. IEEE; 2008. pp. 1-5

[9] Medeni Mb O, El Mamoun S. A generalization of the PVD steganographic method. International Journal of Computer Science and Information Security. 2010;**8**(8):156-159

[10] Mahjabin T, Hossain SM, Haque MS. A block based data hiding method in images using pixel value differencing and LSB substitution method. IEEE; 2012

[11] Chaudhary A, Vasavada J, Raheja JL, Kumar S, Sharma M. A hash based approach for secure keyless steganography in lossless RGB images. In: 22nd International Conference on Computer Graphics and Vision; 2012

[12] Dasgupta K, Mandal JK, Dutta P. Hash based least significant bit technique for video steganography(Hlsb). International Journal of Security, Privacy and Trust Management (IJSPTM). April 2012;**1**(2)

[13] Chaudhary A, Vasavada JJ. A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGB Images. IEEE; 2012

[14] Das R, Tuithung T. A Novel Steganography Method for Image Based on Huffman Encoding. IEEE; 2012

[15] Li M, Kulhandjian MK, Pados DA, Batalama SN, Medley MJ. Extracting spread-spectrum hidden data from digital media. IEEE Transactions on Information Forensics and Security. July 2013;**8**(7)

IntechOpen