A Novel Hash based Encryption technique on Video steganog-raphy integrity verification against attacks

V.Annapurna, S.Nagaraja Rao, M.N.Giri Prasad

Abstract--- Steganography is an essential task to construct a secure communication among various authorized entities. Video Steganography is one of the essential source of transmitting secret data using data hiding techniques in videos. Securing the embedded data along with video data is an essential task in data hiding techniques. However, this sensitive information is vulnerable to third party attacks such as video content change, copyright change, key change etc. A large number of cryptographic algorithms have been proposed in the literature for integrating the sensitive data into the data hiding techniques. But, as the size of the sensitive data increases these models require high computational memory and time. Also, these cryptographic models are not applicable to large video data for integrity computation and encryption. In order to overcome these issues, a novel integrity verification technique is proposed to find the change bits in the video with high sensitive rate. Also, proposed model use integrity based encryption technique to hide the sensitive information securely in the video. Proposed model use motion vectors to find the integrity of the video for data hiding against the third party attacks. Motion vectors are extracted using the kalman filter in the source video for integrity computation. Proposed integrity computation model use polynomial structures to increase the complexity or sensitive of the hash during the data hiding process. Experimental results proved that the proposed integrity verification based video steganography approach is more sensitive and efficient than the traditional cryptographic approaches in terms of bit rate, runtime and memory are concerned.,

Keywords-Video Steganography,Integrity Verification, Kalman filter, Motion Vectors

1. INTRODUCTION

The process of information hiding uses the digital signals in order to embed essential information. Different digital media carriers (audio, video, images, etc.) are used for the processing of information hiding. Steganography can be defined as the process of hiding secret data within a cover media. The cover media can be text, or, audio, or, image, or video. Presently, the video steganographic approaches have become more popular in case of various video sharing and social networking applications just like livestreaming. All of these algorithms are categorized into two types, those are:- watermarking and steganography. Watermarking technique is useful to embed copyright information into the carriers. It explains the rights of the content owner. Also, it provides protection to the content to be copied or modified. Information leakage is usually traced back by using various authentication schemes. On the other hand, steganography can be defined as a special kind of information hiding in which important information are embedded within the carriers to ensure secure communication. Video information hiding is very much essential now-a-days. The above technique is beneficial for the illegal transmission and distribution of videos.

The process of video steganography is of two types, :-

1. In this kind of video steganography, information is embedded prior to the encoding process. Video is considered as a sequence of motion pictures. It can hide important information inside the video frame pixel depending upon their intensity. This approach is considered as the simplest one. The only limitation of this technique is that, the video information is usually lost after compression encoding.

2. In the second type of video steganography, information embedding occurs at the time of encoding.

Sensitive information are embedded during the coding process of image or video. By integrating various characteristics of coding constraints and detecting the exact information embedding positions, we can modify several intermediate outcomes in order to obtain information embedding. In the above kind of information hiding process, video is transmitted after successful completion of compression coding. Therefore, this kind of embedding approach can be implemented in wide range of applications.

Video data redundancy is eliminated after completion of compression coding. Hence, large amount of data can't be embedded within a particular compressed video stream. Some approaches those can be included within this category are:- DCT transform, entropy coding, kalman motion estimation, and so on. Most of the traditional models use intra prediction during the process of information hiding. All of these approaches changes the intra encoding prediction mode in order to hide information efficiently. These secret information can be embedded inside frame. Hence, the overall embedding capacity of this approach is restricted. DCT transform technique uses large non-zero coefficients in order to hide information. As there are only few numbers of such coefficients, the embedding capacities of these methods are also restricted.

On the other hand, the entropy coding approaches changes the code elements according to the CAVLC and CABAC. It may result with huge distortion and sometimes decoding terminations. Motion estimation approach is

Revised Manuscript Received on March 10,2019.

V.Annapurna, Research scholar, JNTUA, Ananthapuram, AP, India
Dr.S.Nagaraja Rao, Professor, Dept of ECE, G.Pullareddy Engineering College,Kurnool, AP, India
Dr.M.N.Giri Prasad, Professor & Director of Admissions, JNTUA Ananthapuram, AP, India

implemented to hide information through the modification of motion vector. The distortion of motion estimation is also encoded as well as transferred. The traditional motion vector technique involves hiding of sensitive information through modification of motion estimation. The basic concept behind these approaches is that, the amplitude of modified motion vector must fulfill several constraints.

Some of the traditional hiding approaches perform modification of search range of motion during the process of video encoding.Most of these approaches follow two operations on videos. At first the total numbers of search points are spilt into two sets. One set can represent the information by 0s and other set by 1s. The hidden information can be searched with 1/4 pixel accuracy. In the second case, a distortion function through exploiting the spatial-temporal correlation in order to decrease the embedding impact on motion vectors.

Motion Video Steganography:

The main objective of steganalysis is to detect whether there exist any secret message in a hidden format within digital media just like image, video and audio. Almost all steganalysis approaches gives emphasis on image steganography, but since today there is no significant amount of research works in the area of the steganalysis for digital video. With the advancement of video recording devices and video applications, digital video is considered as the most convenient information carrier.

As the volume of a video is comparatively large than that of other digital media, hence the spaces for information hiding inside a video is sufficient. Generally, digital video or compressed digital video consists of different components. These components play significant role in the development process of various steganographic algorithms. Motion vector is considered as the most important and basic component of compressed videos. Presently, numbers of steganography tools or methods is increasing rapidly. With increase of steganographic methods, the challenges of video steganalysis are also increasing day by day.

In between various steganography, the motion vector based technique in H.264/AVC is selected mostly frequently for the process of steganalysis due to two important reasons, those are:-

Improved security and better embedding capacity

Presently, H.264/AVC is considered as the most commonly used video encoding standard. Hence, in most of the real world applications, the motion vector based techniques can be implemented efficiently and effectively.

In case of motion vector based techniques, motion vectors are changed. Additionally, the relevant prediction errors are adjusted at the same time. There exist numbers of different motion vector based techniques. Several traditional approaches use certain previously defined selection rules in order to choose candidate motion vectors. These rules play significant roles during the whole process of embedding. In another type of motion vector based method, selection of motion vector is done by some threshold value. These motion vector components are changed with greater magnitude in order to carry out the process of embedding smoothly. There exists a different type of motion vector based technique in which message is hidden with the help of phase angle among two different components. Apart from this, the selection rules may lead to various risks. Hence, the process of steganography includes different adaptive techniques in order to enhance the overall security to a great extent.

The traditional adaptive method is modified and extended in order to give rise a new threshold selectionIn order to identify various motion vector based steganography techniques, different feature based steganalytic techniques are introduced presently. All of the above mentioned steganography techniques can be broadly classified into three types, those are described below.

The first type of steganalytic approaches use feature based concept case of neighbouring motion vector difference. In other words it can be stated that, each individual feature is extracted from statistical characteristics of neighbouring motion vector difference. In some other steganalytic techniques a combined distribution of neighbouring motion vector difference among a particular macroblock and other two macroblocks are considered. In case of H.264/AVC video coding standard, if two neighbouring macroblocks shows different partition, in that case it is very complicated to evaluate the neighbouring motion vector difference.

The second group of steganalytic approaches usually implements the statistics of the Sum of Absolute Difference. The Sum of Absolute Difference plays vital role throughout the designing process of features. This method considers that, the regional optimality of Sum of Absolute Difference can be modified if and only if, the appropriate motion vector is modified. Another research Idea includes the concept of subjective probability of optimal matching through the implementation of the regional optimal Sum of Absolute Difference. The basic concept of AoSO and SPOM are almost same. In case of large quantization parameter, the stability of the regional optimality of Sum of Absolute Difference gradually decreases because of quantization distortion. Therefore in the above mentioned case, the identification performance also decreases.

The third group of steganalytic approaches which implement calibration functions in order to improve the features. This traditional calibration function is again compressed. After that, the motion vector features are generated from the difference of motion vectors and sum of absolute differences. The above phenomena takes place just before the calibration process. Furthermore, the coding parameters in case of both the compression process is required to be equivalent. However, the identification performance can degrade gradually. The above proposed approach is based upon the basic concept of the correlation in between different neighbouring motion vectors. In the presented case, the locations in existence of neighbouring motion vectors are not at all considered.

All of the above mentioned approaches have certain limitations. Additionally it can be mentioned here that, motion vector based steganography is capable of modifying motion vectors and the corresponding pixels at the same time.

Video Steganography Techniques and Its Issues:

Steganography is also known as " covered writing". In other words, steganography can be defined as a special way of hiding information in order to avoid identification of hidden messages. Cover object is actually a particular file that has the responsibility to hide sensitive information. Secret message is actually the sensitive data is embedded inside the cover object. Through the integration of cover object and updated sensitive data, stego object is generated. The Secret sensitive message is encrypted prior to the process of embedding.

A specific encryption key is required during the process of encryption. That particular key is known as stego key. On the other hand, steganalysis can be defined as various attacks those try to break the steganographic methods.

Almost all steganographic approaches suffer from different types of challenges. There are four major challenges or issues which are mostly found in all of the traditional steganographic approaches. Those four issues are:-

1. Robustness,
2. Tamper proof,
3. Hiding efficient and
4. Perceptual transparency.

All of these four are inversely proportional with each other. Hence, it will cause sequential data hiding problem. Robustness can be defined as the amount of changes the stego object can manage causing any serious damage. Tamper resistance is a special type of property that increases the difficulty level for an attacker in order to modify the sensitive secret information. The above mentioned secret information is already embedded inside the cover object. Boat hiding capacity and perceptual transparency are interlinked with each other. In case of a large hiding capacity, a very small cover object is required in order to hide the secret message. Very large hiding capacity may give rise to distortions. The attacker always tries to identify the distortion, because in this way he can identify the presence of hidden message. In the above mentioned scenario, the secret communication is visible and the process of steganography is considered as inefficient. Therefore, perceptual transparency is considered as the most important characteristic of steganography.

The visible distortions can easily reveal secret communication. Several steganographic approaches implements a model which assists during the evaluation of relevance of every individual pixel along with the undetectable distortion level. All of these above mentioned approaches are also called as visual masking approaches. They include both physiological & psychological mechanisms of the human visual system in order to carry out the masking phenomena. An advanced visual masking approach for images and videos is applied in various applications. This approach generates a relevance map of the image/frame. The frame size is restricted to 8x8 pixel blocks. This approach involves three important components, those are:-

1. JND model
2. Visual attention model and
3. Weighing model.

Any kind of digital file can be used as covers. The major concerns of all steganographic approaches are to increase the hiding ability and to reduce the embedding distortion. In this case, file formats having large redundancy are considered. The redundant bits if any objects can be replaced easily without any major effect. According to the kind of cover object used, steganography can be classified into six numbers of sub-categories, those are described below:-

1. Text Steganography:- Text steganography is considered as the most common and traditional way of steganography. Some advanced methodologies are included in order to enhance the level of security, those methodologies are:- line shifting, word shifting and feature-based encoding. Now-a-days, text steganography is no more used and it has become outdated. One of the major limitations of text steganography is, the text files always contain restricted amount of redundant data. Therefore, it will decrease the hiding capacity of the secret message. Apart from these, the text files can be modified with an ease and it may cause huge loss of sensitive information.

2. Audio Steganography:- Audio steganography is second commonly used steganography. Here, hiding of secret message occurs in case of one dimensional signal. The whole concept of audio steganography is based upon the masking concept. A poorly audible audio become almost inaudible with presence of another loud audio signal. Among various different types of audio encoding approaches, low bit encoding, phase encoding and spread spectrum are three most common audio encoding approaches.

3. Image Steganography:- The process of image steganography uses images are cover object. In other words, images are considered as the most efficient way to hide secret messages. Images include large amount of redundant data. A digital image can be defined as collection of numbers which are used to represent various light intensities at different places. These numbers are used to build a special grid and that grid is also known as pixel. There are large numbers of digital image file formats. Three most commonly used digital image file formats are:- JPEG, BMP and GIF. Many stegnographic approaches are developed by considering all of these image file formats.

4. Video Steganography:- Some researchers consider video steganography as a perfect extension of image steganography. A video stream is a collection of numbers of images. These images are consecutive and located after equal time intervals. There are certain cases where these video streams are associated with audio streams. Hence, some image steganography approaches can also be implemented here. There are huge amount of research works have been performed on video steganography since decades. Some researchers extended their previously developed image steganography technique to video steganography. Video is considered as the most appropriate kind of file that can be used as cover. The reason behind this growing popularity is because a single video can transmit a large amount of secret data with it.

5. Protocol Steganography:- This is a special kind of steganography, where secret data are usually hidden inside network packets. There exist covert channels among various layers of OSI model. In all those places, steganography can be implemented.

Additionally, the storage capacity is comparatively huge as compared to all other media.

Besides the above mentioned categories, there are several other categories of video steganography, those are described below:-

1. Substitution-based Approaches:- In case of substitution-based approaches, all redundant data can be just replaced by secret data. This approach is the simplest one and it also has very high embedding ability as compared to other steganographic approaches. The most commonly used substitution based approaches are:- least significant bit method, bit plane complexity segmentation, tri-way pixel value differencing, and so on. Least significant bit method is considered as the most popular and easy to implement steganographic approach. Again, it is capable to hide huge amount of secret data.

2. Transform domain Approach:- The main problem with substitution-based approaches is the vulnerability to cover changes. Hence, the embedded secret information can be accessed and destroyed within no time. Transform domain approaches are considered as relatively complex approaches. These approaches usually improve the robustness and the perceptual transparency. Following are the phases of a traditional transform domain approach:-

Phase-1: Initially, the cover is transformed to the frequency domain.

Phase-2: After that, the secret message is embedded within certain or all transformed coefficients.

Phase-3: The altered coefficients are again converted to its original form.

Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are some most commonly implemented transform domain approaches. DFT approaches are not much efficient in case of steganography because of huge round off errors.

3. Adaptive steganographic approaches:- Various newly developed embedding methods are included under this category of steganographic approaches. These are also known as masking or statistics-aware embedding. The adaptive approach basically depends upon the statistical behaviors of the cover prior to the secret data modifications. This approach generally assists to detect the best places in order to hide data. Those places are called as regions-of-interest ROI. An adaptive capacity function is used here that decides the amounts of secret data to be embedded. The well-known least significant bits approach has an adaptive version of it.

4. Format-based approaches:- There are different video formats those can be used as cover objects. In this type of steganographic approaches, emphasis is given on video formats. H.264/AVC is considered as the most recent compression standard for video. This approach can achieve very high compression efficiency. This is more suitable for network transmission.

Cover production approaches:- Every individual conventional embedding approach depends upon a particular cover object. An advanced steganographic approach is implemented in order to hide secret data efficiently. On the other hand, cover production approaches generates an object and use it as a cover inside some secret communication. The above concept is considered beneficial for dynamic cover video production. This approach includes the application of secret key and secret message in order to produce the appropriate cover video. A function X(A,D) is used during the production process. Here, A is denoted as the total numbers of samples needed to hide the message and D is the required secret message bits which must be hidden. The above mentioned approach uses database of images in order to gather necessary images for the process of video creation. This approach is more sustainable for steganalysis, because the original images are actually hidden from the attacker. There exists a single limitation of the above approach that is, when the chosen images are not related to each other, in that case the attacker may doubt

2. RELATED WORK

K. Rajalakshmi et.al, developed a new and advanced robust secure video steganography with the use of reversible path-wise code-based embedding [1]. At the time of data hiding and transmission, there exist loop holes where the secret data can get leaked to the attacker. Again, there exist numbers of different issues in the field of video steganography. A large video is decomposed into numbers of frames and after that the processing of data gets started. Through implementation of an efficient embedding algorithm, the sensitive confidential data gets embedded inside the cover video. The secret information can be either very large or small in size. Both the encryption and decryption algorithms are implemented in order to get highest level of security in case of data hiding. During the process of data transmission, the decryption process is associated with several issues.

The restoration of compression technique includes several video frames as input and it implements the discrete cosine transform or discrete wavelet transform method. All the information related to pixels are distorted because of frame cover conversion and encoding. Therefore, the overall encryption efficiency is influenced by lossy pixel information. Therefore, a new correlation filtering technique is integrated with blind pixel algorithm in order to hide secret data. In this case, the quality of the secret information is maintained properly. The pixel grouping mechanism is carried out through the replacement of relevant and recurrent pixels. The above mentioned process has significant role throughout encryption process just to decrease lossy pixel information.

This filtering approach is considered as an efficient pre-processing approach just to eliminate noise from the cover and secret video. Fast Fourier Transform implemented in this paper. The pixel optimisation process is carried out by considering various boundary coefficients. Both of the above mentioned phases try to decrease lossy pixel information. According to the least significant bit method,

pixel value of secret message is usually inserted within the pixel value of cover. The limitation of traditional least significant bit algorithm is resolved in this case by considering a group of random pixel among cover and secret data. Additionally, the patch wise code formation technique is implemented in the video encoding process just to result improved level of security.

S. Balu, et.al, introduced a secure and effective data transmission approach with using the process of video steganography in case of medical imaging system [2]. Usually steganography method is implemented in order to enhance the security level of data transmission. In case of medical data, medical data are transmitted from one hospital to other hospitals. Therefore, video steganography in case of medical imaging system enhances the security level significantly. The process of steganography emphasizes on information confidentiality, integrity and authenticity. Steganography approach in case of medical imaging system primarily emphasize on all areas except doctor diagnosis. According to the human vision region of interest, both foreground and background object are identified within a video.

After that, an advanced face identification approach is implemented in order to identify moving object. The secret information is usually hidden within the background object. Secret information is never hidden in the face area of foreground object.

M. Fan, et.al, implemented a cross correlation feature mining for steganalysis of hash-based LSB video steganography [3]. The popularity of video steganography has increased because of its huge capacity as compared to other traditional steganographic approaches that uses image or audio for its cover. According to this technique, 8 bits of secret message are decomposed into 3, 3, 2 smaller segments. These decomposed messages are embedded into the RGB pixel values. Apart from this, the hash function has the responsibility to identify the embedding locations.

*D. Griberman and P. Rusakov*performed detailed comparative study of various video steganographic approaches in order to embed watermark [4]. In this paper, a detailed survey is carried out on different video steganography embedding techniques and summarized a group of constraints for the process of video steganography.

Apart from the above, robustness property is also analysed and verified against different attacks. The major objective of the proposed technique is to reduce the noise created by the steganographic process.

P. Kumar and K. Singh introduced an enhanced data hiding technique with the help of skin-tone identification method [5]. Providing security to the embedded data and reducing the distortions in case of videos is still very complicated task. In this paper, an advanced steganographic technique is introduced in order to reduce the probability of identification of the embedded image data in case of cover objects. Here, human skin locations are assume as regions of interest in order to embed the secret information. It enhances the adaptability of the above presented approach in case of different kinds of image data. Certain consecutive pixels are implemented in order to embed secret data inside the cover object. The third discrete wavelet transform technique is applied here. The approximation coefficient is used in order to carry out the process of embedding after the implementation of third discrete wavelet transform method.

It improves the robustness of every individual video frame and also improves the quality of the video. The frame matrix is again considered for skin map retrieval in order to generate color based pixel selection. In the above presented technique, 8 pixel retrieval is considered for the red and blue channels.

S. Manisha et.al, proposed an advanced two-level data hiding technique in case of video steganography [6]. Sensitive data are interchanged most often in case of both wired and wireless modes of communication. Hence, these secret data are very much vulnerable to unauthorized access. Cryptography is considered as the most appropriate way to resolve the above mentioned problem. After decryption of the secret message, it gets revealed to everyone. In this work, an efficient and effective data hiding ad retrieval methodology is introduced. Here, audio video interleave videos are considered and secret messages are embedded inside a bitmap image file. Initially, the secret message was decomposed into smaller bytes and these smaller bytes are hidden inside certain frames of a video. Inserting these secret data inside a video frame increases the overall level of security. The presented research work enforces two highly secure levels of encryption techniques. Both quality and size of the secret message is not at all changed before and after the encryption process. Every individual secret image is capable of embedding certain multimedia data and these data can be again retrieved and recognized. This approach is considered as more secure because it involves two step encryption process and it only includes two bit positions in case of a single video frame. The secret image is located in four separated quadrants. Therefore, both the size and quality of image remains unaffected. The original video size must be compatible with the size of the carried video. Hence, the overall quality of secret data is improved.

J. Mansouri et.al, developed an adaptive technique for compressed video steganography [7]. This model uses both temporal and spatial characteristics of video signals. An effective approach for video steganography is implemented in case of covert communication. All secret data are inserted inside a compressed video stream adaptively with the help of temporal and spatial characteristics of the video signal. The process of embedding is carried out by considering human visual system behaviours.

R. J. Mstafa et.al, performed a detail survey on both compressed and original video steganography approaches [8]. This paper includes both study and analysis of various video steganographic approaches. The performance evaluation of each and every method is also analysed. In this survey paper, both compressed and original video steganography are considered. In case of compressed video steganography approaches, the video steganography approaches are classified depending upon the video compression phases just like appropriate locations for data embedding. Apart from this, intra frame prediction, inter frame prediction, motion vectors, transformed and quantized

coefficients, and entropy coding are several other categories of video steganography. On the contrary, original video steganographic approaches are decomposed into two broad categories, those are:- spatial domains and transform domains.

H. Noda et.al, developed a new video steganography scheme that depends upon the bit plane decomposition of wavelet transform video [9]. This paper introduces a new steganography approach that can efficiently handle lossy compressed video. It is the most convenient and traditional way to transmit huge quantities of secret data. The above presented approach completely depends uponwavelet compression for video data and bit-plane complexity segmentation (BPCS) steganography.Motion-JPEG2000, wavelet coefficients are usually quantized into a bit-plane structure. Hence, this kind of steganography is most efficient for wavelet domain.

Z. Qu, et.al, proposed a quantum video steganography protocol in case of large payload based MCQI videos [10]. Quantum video is considered as an important multimedia which is usually found in case of quantum networks. A secure and effective quantum video steganography protocol having huge payload usually depends on the videos strip encoding strategy. This encoding strategy is known as multichannel quantum images encoding strategy.

This new protocol is responsible for embedding secret data randomly. Both the original quantum video and the quantum career video show distinct characteristics of video frames. At the time of covert communication, secret information is embedded inside the quantum video. Again, the receiver can retrieve secret information from the video without retaining the carrier video. On the other hand, the original quantum video is restored perfectly.

Y. Ren, et.al, proposed a new method of video steganalysis that depends upon subtractive probability of optimal matching feature [11]. In this piece of research work, they have proposed a motion vector-based steganalytic technique. The above presented technique depends upon the optimal matching characteristic in case of a compressed video. By analysing the outcomes we can mention here that, every individual feature is stable and sensitive in nature. Hence, the cover and motion vector based video can be distinguished easily. There are total three numbers of advantages of the above-mentioned feature.

1. According to the standard constraints of motion vector production, feature can be implemented in case of large numbers of video compression standards. The optimal matching motion vector is chosen in order to decrease the overall temporal redundancy.

2. Every individual feature is independent in nature. It is not at all related to the correlation of consecutive motion vectors. In case of relatively large temporal activities, the feature shows better classification capability than that of other traditional approaches.

M. M. Sadek, et.al, performed a comparative survey on various video steganographic approaches [13]. Steganography can be defined as a security mechanism usually used for the process of data hiding. There are numerous numbers of covers which are used during the process of steganography.

[13-16] proposed a novel encryption models on compressive image datasets and high dimensional image databases using the chaotic function. These models are efficient on standard image databases with fast encryption time. These models require high decryption time on high dimensional images. Also these models require high computational memory on video frames.

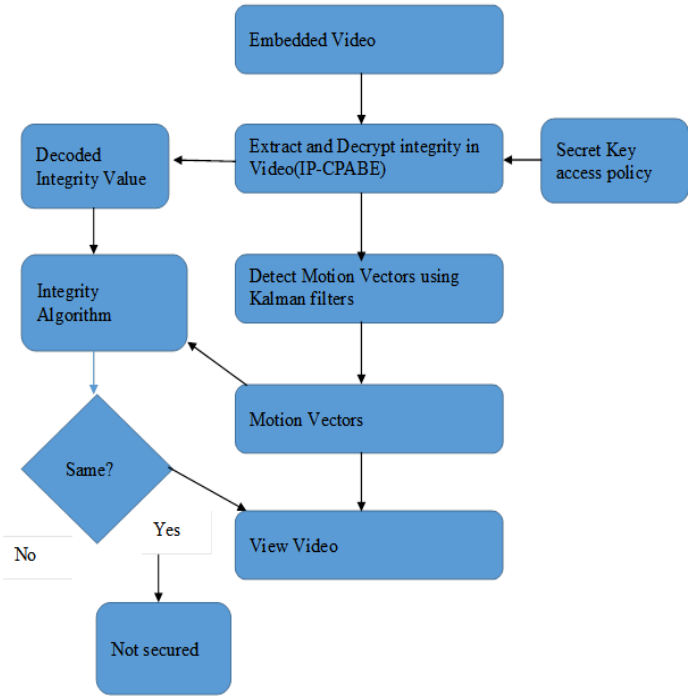
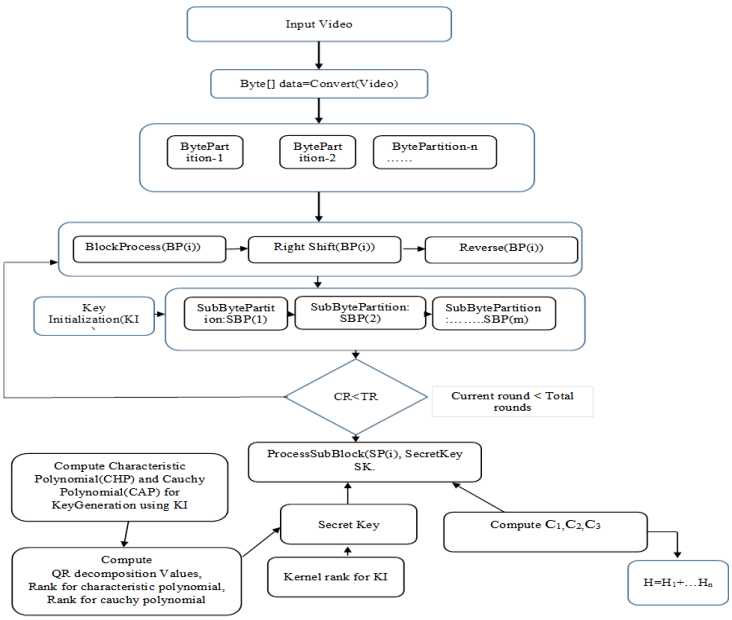
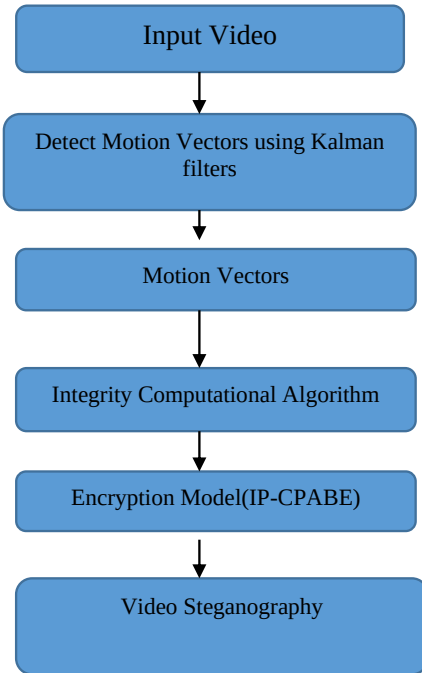


Figure 2:Video Steganography Integrity Verification process



3.Proposed Model: Secured Integrity Verification based Video Steganography Verification Model



In the proposed model, a novel polynomial based integrity verification algorithm is proposed to improve the security issues in the traditional video steganography. The overall approach is described in the fig 1. As shown in the fig 1, initially the video input is used to track the motion vectors in each frame. Here, traditional kalman filter algorithm is used to track the motion vectors in each frame of the video. All the motion vectors in the each frame are integrated to find the hash integrity computation. In the proposed model, a novel polynomial based integrity computation technique is proposed to find the unique signature of the input video motion vectors. In the proposed model, integrity based ciphertext policy attribute based encryption technique is used to embed the encrypted integrity data into the video.

In the figure 2, integrity embedded video steganography file is taken as input for video integrity verification process. Encryption algorithm is used to decrypt the encoded hash integrity value for video integrity checking. Decrypted integrity value is tested against the computed integrity value of the steganography video. If the integrity values of the decrypted one and the computed one are same then there is no modification in the source video.

Computing characteristic and Cauchy polynomials using the initial key matrix.

Compute Cauchy Polynomical to initial key as CAP

KI=[k_1,k_2..kn]=V

$m_1=k_1$; $n_1=\frac{m_1}{\|m_1\|}$

$m_2=k_2-(k_2.n_1)n_1$; $n_2=\frac{m_2}{\|m_2\|}$

$m_2=k_{r+1}-(k_{r+1}.n_1)n_1-\ldots\ldots-(k_{r+1}.v_r)n_r$; $n_r=\frac{m_r}{\|m_r\|}$

Using QR decomposition formula we have

Where Q=[n_1,n_2…..n_r] and $R=\begin{pmatrix} k_1.n_1 & \cdots & k_1.n_r \\ \vdots & \ddots & \vdots \\ 0 & \cdots & k_r.n_r \end{pmatrix}$

Rank r1=Rank(QR);

Compute Characteristic Polynomical to initial key as CHP

Find eigen vector EV[]=Eigen(CHP);

Rand r2=Rank(CHP);

Kernel Rank r3= Rank(Q*Q);

secret key SK[]={EV[0],EV[1],Max{r1,r2},r3};

Algorithm Steps:Computing the Hash Function

Step 1: Input Video motions vectors and Hash size.

Step 2: Message M=Motionvectors;

Step 3: Initializing the key as KI.

Step 4: Divide the message M into S/8 blocks.

if(M>S/8)

Partition the block into S/32 subblocks of 4 bytes each(P)

Right shift P, Reverse P

For each byte in P[i]

Compute C1,C2,C3

T1=IK%(∑ V).PolyTransform(T1)

T1=m.T1(m=1,2, ……)

T2= PolyTransform(T1) % (3√ ∑ IK)

C1=(T1%256)

C2=T2

C3=M

$H1=1+C_1+C_2+C_3$

Step 5: H=H1+H2---------Hn

Encryption Algorithm:

Cipher text based attribute based encryption is the traditional encryption model which is used to encrypt the data with the attributes list and policies. In the proposed model, attributes and policies are initialized with the computed integrity value of the motion vectors. Proposed encryption algorithm is executed in four phasesi.e setup phase, encryption phase, key generation phase for secret key and finally decryption phase. Here, group elements are taken from cyclic group elements with bilinear property.

Input : Integrity Value as input message.

Phase 1: Setup(): In this phase, public key and master key are generated using the bilinear pairing and cyclic group elements.

$$\textbf{PublicKey} = \{g_p, g \in G \wedge H; e(g, g^{\alpha})\}$$

$$\text{Masterkey} = \{g_{\alpha}, \beta \in G \wedge H\}$$

Phase 2:Encryption(): In this phase, integrity value of the video and public key are used to encrypt the message

$$\mathbf{C} = \{m \in G_T, s \in Z_r, \text{PolynomialAccessTree(Policy } \mathbf{P}, s, K),$$

Ciphertext $\mathbf{C=\{P,m.g_{\alpha}^{s}, h^{s}\}}$

Phase 3:KeyGeneration(): In this phase, secret key is generated using the public key and master key.

s

$$SK = \{r \in Z_p, g_r\ PK.g_p^r, MK(g_{\alpha}).MK(g_r), D^{MK(\bar{\beta})},$$

$$\forall A_i (D_j \in g_r.r_j, D_j^{'} \in PK.g_p.r_j)\}$$

Phase 4: Decryption(): In this phase, data is decrypted using the cipher text , secret key and public key.

$$D = \{\mathbf{C=\{P,m.g_{\alpha}^{s}, h^{s}\}}, e(C, Sk.D)\}$$

In the improved approach, the motion vector prediction error is considered as the basic concept behind the selection of motion vector carriers. Secret information are inserted through replacement of least significant bit of motion vector. According to another research idea, the insertion of secret information is carried out through the adjustment of parity of the horizontal component and the vertical component. In case of some other types of motion vector based techniques, embedding process is carried out through replacement of least significant bits of the horizontal and vertical components of each and every motion vectors. Secret bits should be added in place of those replaced bits.

3. PERFORMANCE ANALYSIS & RESULTS

Statistical Integrity Randomness:

Shannon proposed two measures namely confusion and diffusion as essential features for strong integrity verification process. For an efficient diffusion property, there should be 50 percent bit change in the hash value. Let the initial message and its bit values are taken as original data. The changed bits of the computed hash value are

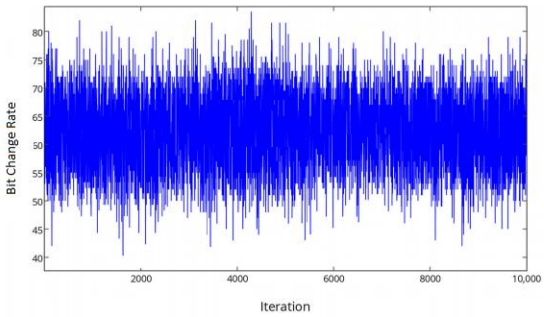


Figure 4: Bitchange rate of the integrity verification algorithm

marked as B(i). The computational measures used to compute the confusion and diffusion are given below.

Changed Minimum bit rate : B(min)=min({B(1),B(2),….B(k)});

Changed Maximum bit rate : B(max)= min({B(1),B(2),….B(k)});

$$\text{Mean changed in bit rate } \bar{B} = \sum_{i=1}^{n} B(i) / N$$

$$\textbf{Standard variance in bit rate} = \{\sum_{i=1}^{n} (B(i) - \overline{B(i)})^2 / N\}^{1/2}$$

Table 1. Comparison of integration based Cipher text policy attribute based Encryption and Decryption models with the existing approaches.(Hash bit size=2048)

Algorithm	Avg EncryptionTime(secs)	Avg DecryptionTime(secs)
Proposed	10.53	12.19
Ref.[13]	12.53	14.64
Ref.[14]	12.94	17.35
Ref.[15]	13.83	19.45
Ref.[16]	13.92	19.93

Table 1 describes the comparison of proposed model to the existing models in terms of encryption time and decryption time.

Table 1, describes the encryption and decryption time of the proposed model to the existing models on video steganography video files. As the size of the video increases, proposed model require less computational encryption and decryption time compared to the existing models.

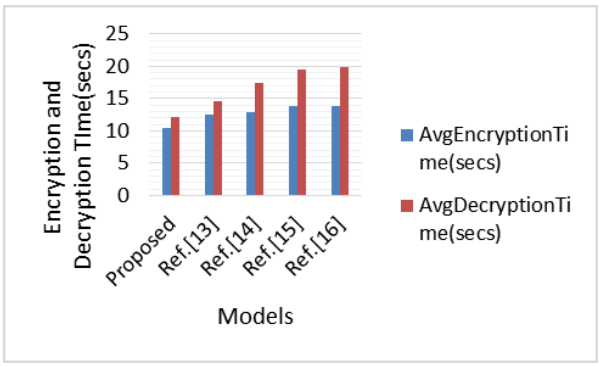


Figure 5: Comparison of the proposed model to the existing models in terms of encryption and decryption time.

Figure 5, describes the encryption and decryption time of the proposed model to the existing models on video steganography video files. As the size of the video increases, proposed model require less computational encryption and decryption time compared to the existing models.

Table 2: Mean changed bit rate of the proposed integrity algorithm to the existing algorithms

Algorithm	AvgHashBitrate
MD5	118
SHA512	124
Mixed Chaotic[17]	127
Proposed Hash	135

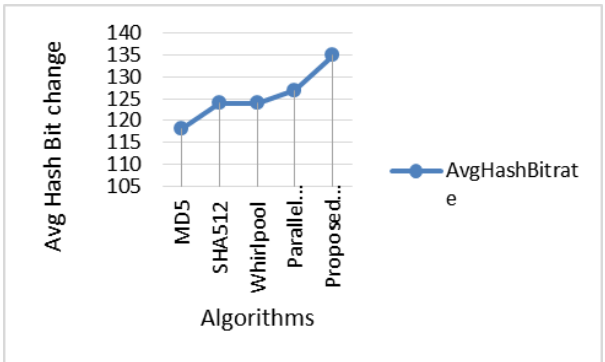


Figure 6:Avg bit change rate of the proposed integrity value to the existing algorithms

Table 2 and figure 6 describe the comparison of proposed hash algorithm to the traditional algorithms on the average bit rate change for sensitive analysis on the motion vectors of the video steganography files. From the results, it is

observed that the proposed model hash high sensitivity compared to the existing algorithms on video files.

4. CONCLUSION

Steganography can be integrated with cryptography or error correction scheme in order to enhance the efficiency and security. Before embedding of secret message, that message will get encrypted. A large number of cryptographic algorithms have been proposed in the literature for integrating the sensitive data into the data hiding techniques. But, as the size of the sensitive data increases these models require high computational memory and time. Also, these cryptographic models are not applicable to large video data for integrity computation and encryption. In order to overcome these issues, a novel integrity verification technique is proposed to find the change bits in the video with high sensitive rate. Also, proposed model use integrity based encryption technique to hide the sensitive information securely in the video. Proposed model use motion vectors to find the integrity of the video for data hiding against the third party attacks. Motion vectors are extracted using the kalman filter in the source video for integrity computation. The results of the evaluation phase demonstrate that, with increase in embedding capability rate, the detectable distortionon label reduces gradually. This technique is very much efficient in order to detect the exact frame containing secret message. The process of embedding must be carried out separately in order to minimize possibilities of identification with the help of statistical approaches. Proposed integrity computation model use polynomial structures to increase the complexity or sensitive of the hash during the data hiding process. Experimental results proved that the proposed integrity verification based video steganography approach is more sensitive and efficient than the traditional cryptographic approaches in terms of bit rate , runtime and memory are concerned.

REFERENCES

1. K. Rajalakshmi and K. Mahesh, “Robust secure video steganography using reversible patch-wise code-based embedding” Springer Science Multimed Tools Appl,2018.
2. S. Balu, C. Nelson Kennedy Babu and K. Amudha, “Secure and efficient data transmission by video steganography in medical imaging system” Springer Cluster Computing,pp 2639-2643.2018.
3. M. Fan, P. Liu, H. Wang and X. Sun, “Cross correlation feature mining for steganalysis of hash based least significant bit substitution video steganography”, “SPRINGER Telecommunication systems”, 2016.
4. D. Griberman and P. Rusakov, “Comparison of Video Steganography Methods for Watermark Embedding”,”Applied Computer Systems”,pp. 53-61.
5. P. Kumar and K. Singh, “An improved data-hiding approach using skin-tone detection for video steganography s”, “Elsevier Multimedia tools application”, 2018.
6. S. Manisha and T. Sree Sharmila, “A two-level secure data hiding algorithm for video Steganography” Springer Multidim Syst Sign Process,2018.
7. J. Mansouri and M. Khadem”, An Adaptive Scheme for Compressed Video Steganography Using Temporal and Spatial Features of the Video Signal”
8. R. J. Mstafa and K. M. Elleithy, “Compressed and raw video steganography techniques: a comprehensive survey and analysis”, “Elsevier multimedia tools and applications”, 2016.
9. H. Noda T. Furuta, M. Niimi and E. Kawaguchi, “Video steganography based on bit-plane decomposition of wavelet transformed video.SPIE-Multimedia contents Vol-5306,pp. 345-353.
10. Z. Qu, S. Chen and S. Ji, “A Novel Quantum Video Steganography Protocol with Large Payload Based on MCQI Quantum Video”,” International Journal of theory physics.
11. Y. Ren, L. Zhai, T. Zhu and L. Wang, “Video Steganalysis Based on Subtractive Probability of Optimal Matching Feature”, pp. 83-90.
12. M. M. Sadek, A. S. Khalifa and G. M. Mostafa, “Video steganography: a comprehensive review”,”Elsevier Multimedia tools applications”.
13. Ahmad J, Hwang S O. A secure image encryption scheme based on chaotic maps and affine transformation [J]. Elsevier Multimedia Tools and Applications, 2015, 75(21):13951-13976
14. Xie Eric Y, Li C Q, Yu S M, Lu J H. On the cryptanalysis of Fridrich’s chaotic image encryption scheme [J]. Elsevier Signal Processing, 2017, 132: 150-154
15. Yi S, Zhou Y C. Binary-block embedding for reversible data hiding in encrypted images . ElsevierSignal Processing, 2017, 133:40-51.
16. Xiuli Cha, An image encryption algorithm based on chaotic system and compressive sensing, Elsevier Signal Processing, Vol-143:1-50,2018.
17. Wang, X., Zhu, X., Wu, X. and Zhang, Y. (2018). Image encryption algorithm based on multiple mixed hash functions and cyclic shift. ELSEVIER Optics and Lasers in Engineering, Vol-107, pp.370-379.2017.