Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P. 15912-15924 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

An Efficient And Secure Data Hiding Technique : Video Steganography

[1]K.Sailaja, [2]N.Madhavi, [3]Dr K.Sreeramamurthy, [4]Dhanaraju Murala, [5]K Ashwini, [6]Swapna Vanguru

[1]Assistant Professor, Dept.of CSE, Guru Nanak Institutional Technical Campus,Hyderabad.
[2]Assistant Professor , Dept.of CSE, Geethanjali College of Engineering and Technology, Hyderabad.
[3]Professor , Dept.of CSE,Koneru Lakshmaiah Education Foundation, Hyderabad.
[4]Assistant Professor, Dept.of IT, Srinidhi Institute of Science and Technolgy ,Hyderabad.
[5]Assistant Professor, Dept.of CSE, Geethanjali College of Engineering and Technology ,Hyderabad.
[6]Assistant Professor, Dept.of CSE, Keshav Memorial Engineering College ,Hyderabad.

How to cite this article: K.Sailaja, N.Madhavi, K.Sreeramamurthy, Dhanaraju Murala, K Ashwini, Swapna Vanguru (2024) An Efficient And Secure Data Hiding Technique : Video Steganography. *Library Progress International,* 44(3), 15912-15924

ABSTRACT

Now a days, most of the people are using internet in which security is the major issue which has to be maintained. Digital data, which must be protected from eavesdroppers when being stored or sent during communication via an insecure network, is the main source of information in the internet age. As the use of internet is increased, the rate at which the data is transmitted per day is also increased. Various approaches, including steganography, cryptography, and watermarking, are employed in the security sector to secure digital data inside a network.

In this paper will use a technique which is steganography-based steganography based on text, picture, audio, and video is used in safety devices. Essentially, a thorough explanation of video steganography in both the compressed and unfiltered domains is provided.

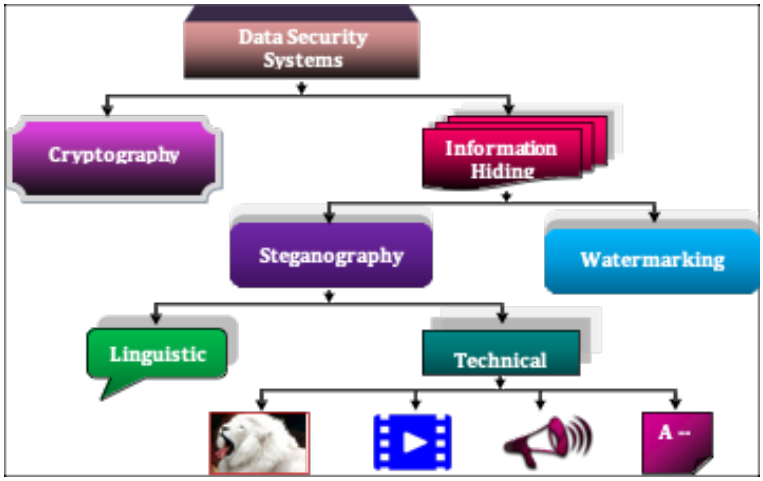
Considering a variety of transform coefficients, the suggested approach presents video steganography within a condensed domain. The confidential information is hidden by using the conversion coefficients of the non-dynamic and dynamic "Region of Interest" (ROI) of the concealed cover video screen as an intermediary subject. Through the use of powerful secret keys and efficient embedding and extraction algorithms, the suggested video steganography becomes more efficient. The suggested video steganography's level is assessed using three parameters: "robustness", which is determined by "bit error rate" (BER) and "similarity" (Sim), "embedding capacity", which is determined by "hiding ratio" (HR), and "imperceptibility", which is determined by "mean square error" (MSE) and "peak signal-to-noise ratio" (PSNR). Both a real-time video sample and a well-defined conventional video dataset have been used in experiments using the suggested technique. A thorough elaboration of the pertinent research in the domain of compressed video steganography is provided, and the outcomes are contrasted with the suggested approach using quality assessment criteria.

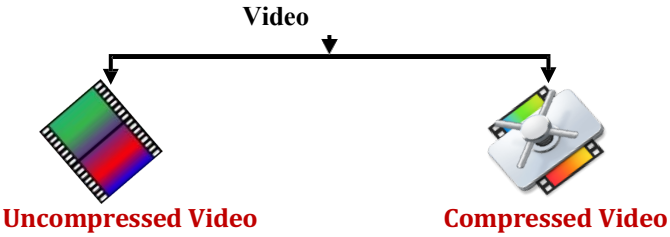
Keywords: "Steganography", "Cryptography", "Embedded data", "Watermarking".

1. Introduction

The majority of activities are now digitalised via electronic means enabling simple access, alteration, and bulk storage that is well-organised. Using digital data instead of actual material makes it easier to do tasks quickly and accurately. Additionally, it grants the user the ability to perform multiple tasks at once. The sender can transport large amounts of data between one end to another more easily because to the digital structure of the information. Furthermore, a large amount of data may be quickly and efficiently received by a distant receiver with little to no delay or loss [1]. Moreover, digital data on any issue may be conveniently gathered, examined, and deciphered to facilitate immediate decision-making.

The sole problem with digital data, despite its ability to simplify tasks, is security when communicating; this is particularly true when information is being exchanged over the widely used, insecure network [2]. It must be protected from unauthorised third parties misusing it in addition to hacking the data via the network.





As seen in Fig. 1.1 [3, 4], there are several methods accessible for the data privacy system to improve computerised data security, including cryptography, watermarking, and steganography. In order to alter, copyright-protect, and hide the information inside the carrier subject, these approaches include one-to-one encryption and decryption [5].

1.1 Cryptography

The Greek terms "Crypton," which means hidden, and "Graphein," which means writing, are combined to make the word "cryptography," which means "hidden writing." Through converting data from the initial state towards an encrypted one before sending it across an unsafe route, cryptography serves to safeguard data. The process of encryption involves converting original data to altered data one-to-one so that the primary information may be recovered using an inversion process known as decryption. A transmitter at one end of the path of communication does the encryption, while the recipient at the opposite end does the decryption. In its broadest sense, cryptography is used to safeguard text data, where various encryption algorithms, such a, b, and c, transform cleartext data into ciphertext data to increase the degree of safety of sensitive data [6].

Symmetric-key cryptography is the use of a single key for both encryption and decryption in a cryptography operation. On the other hand, public-key cryptography uses two distinct but technically connected public keys and private keys. Figs. 1.2 and 1.3, respectively, depict the overall flow of cryptography using public keys and symmetric-key cryptography.

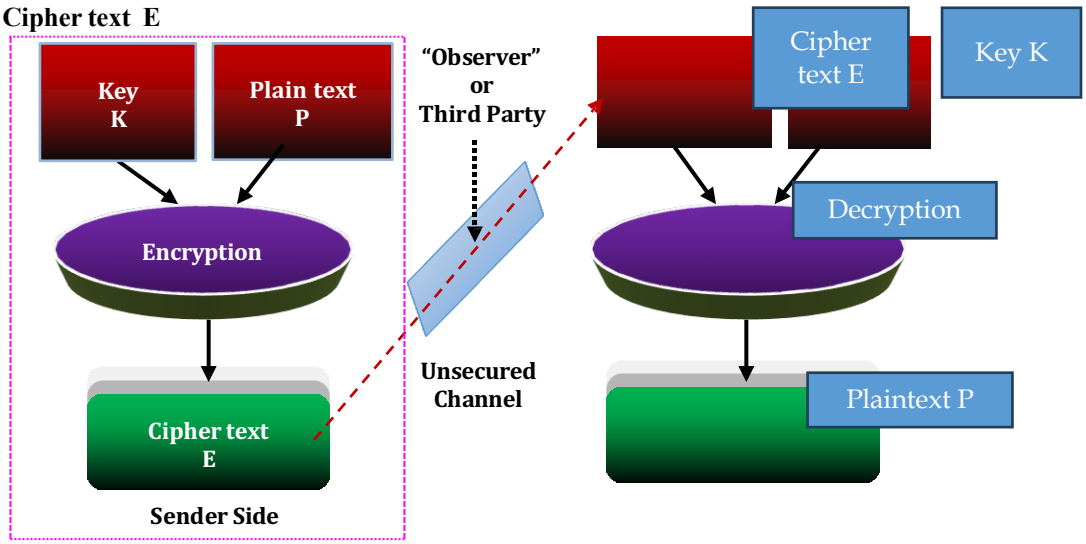


Fig 1.2 Flow Symmetric Key Cryptography

Figure 1.2 illustrates the way either confidential or private keys are used to encrypt the secret information, which is either plain text or clear text. Even if the public key generates a cryptogram as an outcome in the realm of the public, a witness (third party) can nevertheless detect the existence of an encrypted secret information.

1.2 Watermarking

The digital code is embedded into the host audiovisual material via watermarking. To stop unlawful or unauthorised copying, this electronic code verifies who owns the content [5, 9]. Using a watermark code, sometimes referred to as a watermarked item, a watermark raises the content's degree of safety. By preserving the imperceptibility alteration, watermarking integrates the watermark code into the digital data. It serves a number of purposes, including "digital fingerprinting", "copyright protection", "intellectual property protection" (IPP), and "media monitoring".

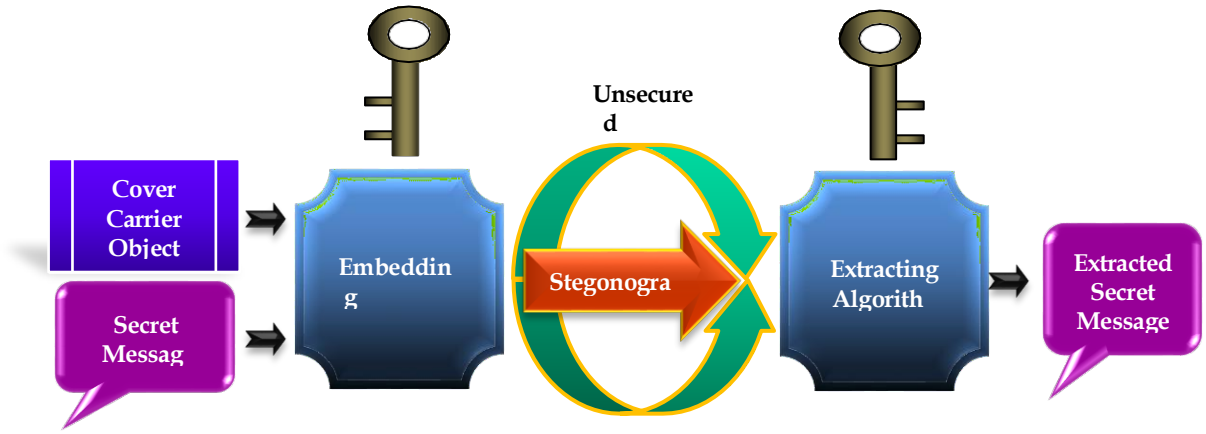
Through the use of a process called digital watermarking, the hidden message is concealed under the cover carrier item and is difficult for the human eye to recognise [7, 8]. For instance, quantum watermarking is used to hide the owners identify and specific information from quantum multimedia data, such as audio, video, and picture. Secret messages can take many various forms; some examples include the author's name or signature, the corporate emblem, and any pattern that holds symbolic meaning. The recipient must be able to retrieve a secret message that has been encoded using a certain key or technique.

1.3 Steganography

Steganography serves as a scientific approach for safely communicating confidential data over an unprotected network by enclosing it in a cover object. Steganography keeps an intruder from seeing the embedded data. The Greek terms "Steganos," which means "covered," and "Graphia," which means "writing or drawing," are combined to make the word "steganography," which has the full sense of "covered writing," or the concealment of confidential information within a cover object [1, 3, 6]. When it comes to steganography, the original and modified stego data are sufficiently similar that a third-party observer would be unable to discern the presence of the original secret message. The following is a description of the various steganographic system elements [4, 6].

Confidential data is concealed in a cover carrier item using a unique stego-key in steganography. It is an extra layer of protection that strengthens the encasement of secret communication. Furthermore, it is necessary for the recipient's side secret message extraction process. Thus, a successful steganogram consists of the covered carrier item, embedded concealed information, and stego-key.

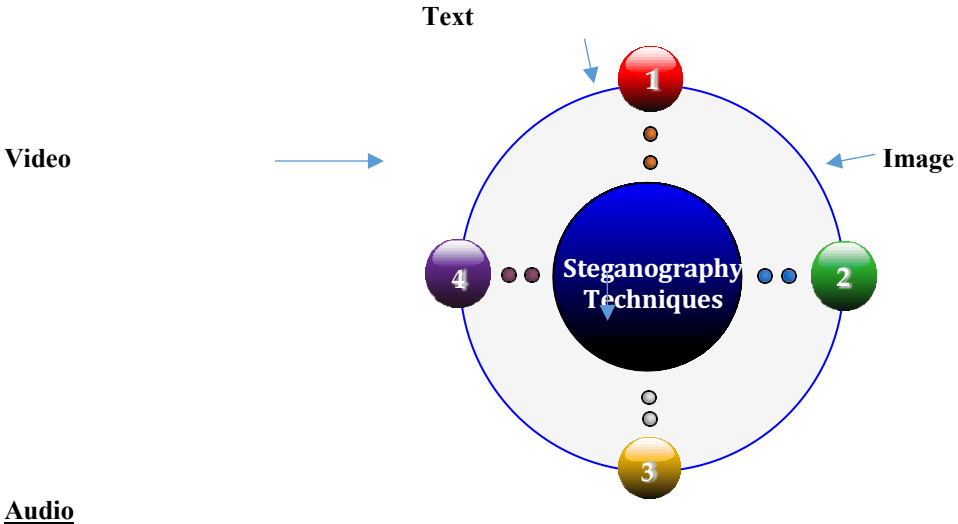
“Steganogram = Cover carrier object + Embedded secret message + Stego-key”



The solidity of the steganographic technique confirms the steganogram's strength and performance, demonstrating its ability to fend off several attacks from a witness (third party). Confidential messages are being extracted from the cover carrier object during the extraction step. The similarity coefficients comparing the original and retrieved encrypted messages are used to determine if the secret message was successfully retrieved [1, 4, 6].

Linguistic steganography collects procedures or techniques to hide any digital information inside text using some linguistic knowledge. Especially, linguistic steganography takes into account the linguistic characteristics of generated and altered text, and in certain instances, it employs language structure to conceal sensitive data.

According to the cover material employed, there are many varieties of steganography. "Character" (text), "frame" (image), "speech/sound" (audio), or a "series of frames" (video) files can all be categorised as cover mediums. Therefore, steganography techniques can be categorized as shown in Fig. 1.5.



1.4 Comparison amongst Cryptography, Watermarking and Steganography

The goal shared by the three security mechanisms—watermarking, steganography, and cryptography is to stop confidential information from being shared over an insecure channel. Due of their comparability, all three of these systems have unique security features [3, 6]. Table 1.1 presents a comparative examination of several security technologies.

Table 1.1: Comparative analysis of Cryptography, Watermarking, and Steganography Techniques

Characteristics	Cryptography	Watermarking	Steganography
Objective Satisfied:	Secret data is covert across communication channel	Copyright protection is in place to prevent unauthorised copying during communication	Whole communication channel is covert
Objective Dissatisfied:	A third party retrieves the plain-text secret message.	The watermark code is altered or deleted.	An observer recognises communication
Carrier Object:	Image or Plain- text	Video or Image	Text (character), Audio (sound/ speech), Image (frame), Video (sequence of frames)
Secret message:	Plain-text	Watermark	Text (character), Audio (sound/ speech), Image (frame), Video (sequence of frames)
Secret keys:	Compulsory	Perhaps	Perhaps
Carrier data during Extraction:	Unnecessary	Application dependent	Unnecessary

Output:	Cryptogram	Watermarked object	Steganogram
Level of Security depends on:	Secret keys	Watermarking algorithms	Embedding algorithms
Transparency of Information:	Visible	Application dependent	Invisible
Robustness:	Against deciphering	Fragile, Semi-fragile, and Robust watermarking	Against detection
Attacks:	Cryptanalysis	Signal processing	Steganalysis
Quality Assessment:	Robustness	May be Robust	Hiding capacity, Imperceptibility, Robustness, and Embedding efficiency

2. Proposed Methodology

1. Video Steganography Domains

Since video has a sequence of frames, or pictures, that may be utilised to conceal a secret message, it is employed as a messenger material. A piece of confidential data can be disguised inside the frame of the video directly, known as video steganography in the realm of space. Video frames may occasionally be changed into an altered (temporal/frequency) domain known as video steganography in the context of time prior to the implantation of private data. A stego video is made up of uncompressed (raw) domain frames placed in a certain order with encoded secret data called video steganography. While compressed domain video steganography is used to create stego videos, compression is done throughout this process. Thus, as seen in Fig. 1.10, the video steganography domains may be categorised based on modification and decompression [3, 4].

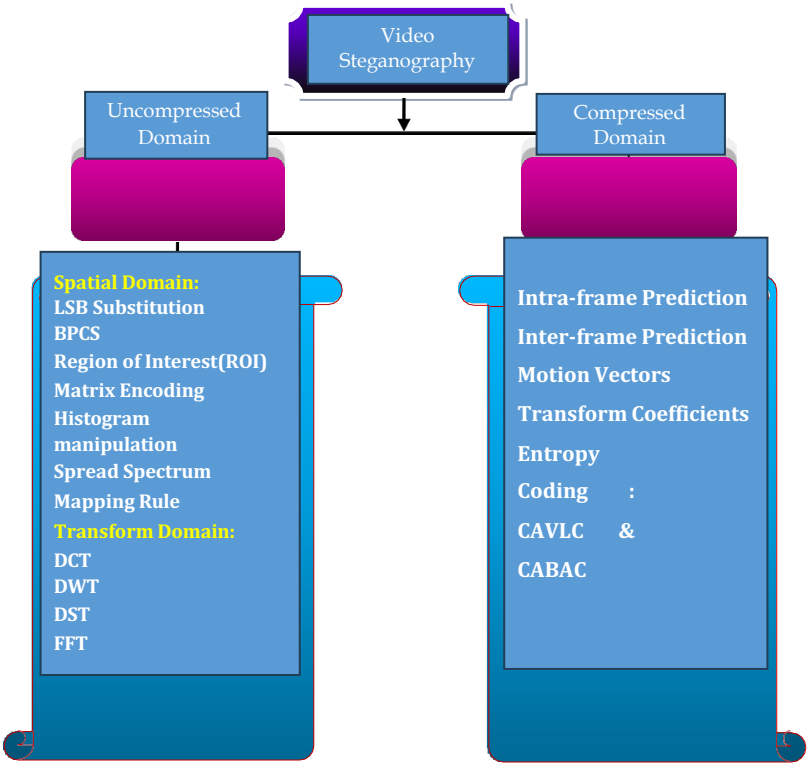


Fig. 1.10: Methods of "Uncompressed and Compressed Video Steganography"

2.1 Proposed Compressed Video Steganography over Transform Coefficients of ROI

The proposed video steganography method is classified into two different stages: The embedding stage and Extracting stage. The embedding method is the process of encrypting a confidential information within a compressed video. Additionally, the extraction procedure is the process of decrypting the hidden message from the encoded Stego movie. Fig. 3.1 depicts the overall system structure of the suggested condensed video steganography technique.

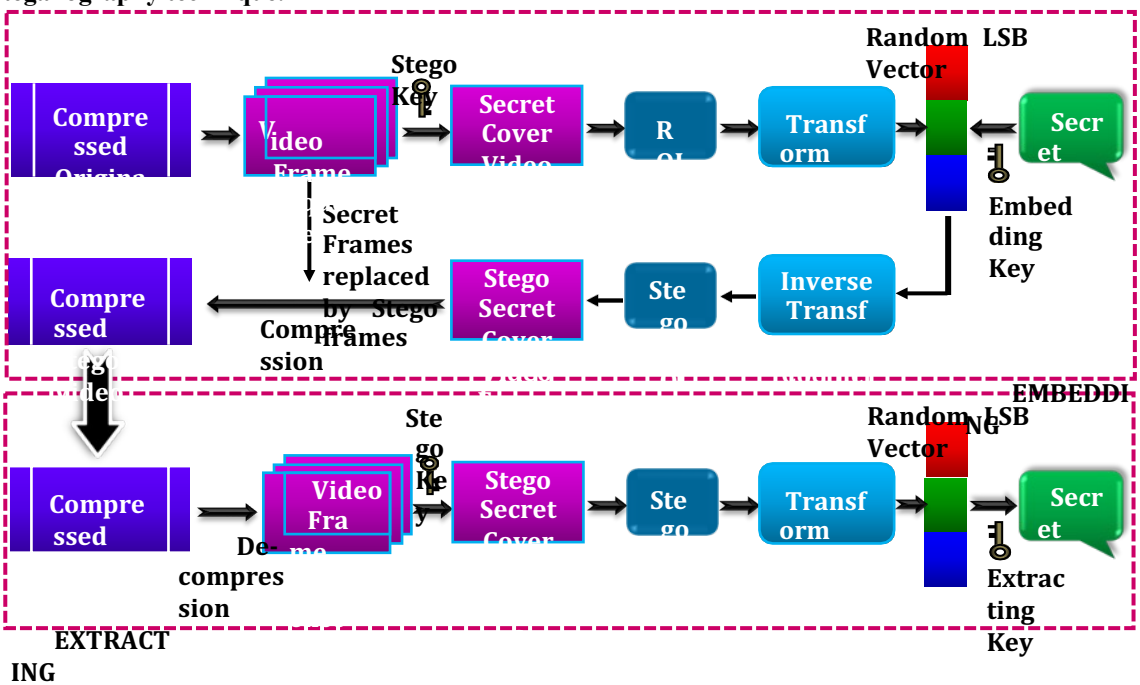


Fig 3.1 General System Architecture of Proposed Compressed Video Steganography

In the proposed video steganography method, two types of ROI can be extracted from the secret video frame: non-dynamic ROI using the AbsoluteDifference Method (ADM) and motion ROI by Exhaustive search Block Matching Algorithm (EBMA) method. Furthermore, there are three different types of transform coefficients viz. "DCT, DST, and FFT" convert the ROI from spatial to a frequency domain. Moreover, H.264 compression method is used to compose the stego video. The system architecture of the proposed "video steganography method" with the above specifications is described in Fig. 3.2.

3.1. 1 Embedding Method

In this method, a compressed video (.mp4) is taken as a cover (Ψ) and an RGB color image(Ω) is used as a secret message to be concealed into cover. Initially, a cover video is separated into a sequence of video frames using H.264 decoder. A stego key is applied to identify the number of random secret cover video frames (*F*) in which the whole or the portion of R, G, and B component of the secret message would be concealed. Further, instead of taking the whole video frame as a cover object, the specific part of a cover videoframe is considered to conceal the secret message known as a region of interest (ROI). Here, two types of ROI are chosen for embedding secret message, (i) Non-dynamic regionand (ii) Motion region.

3.1.2 Non-Dynamic Region: "Absolute Difference Method" (ADM)

The non-dynamic region is extracted from a selected secret frame in the embedding stage by applying the "Absolute Difference Method" (ADM).

"Absolute Difference Method" (ADM):

The whole distinction the non-dynamic zone, according to the method, is defined as a region that stays the same for a certain number of frames. The difference between the intensity levels of the corresponding RGB colour components' pixels in succeeding frames is used to determine it. If there isn't any variation seen between the RGB pixels of subsequent frames, the area is deemed non-dynamic.

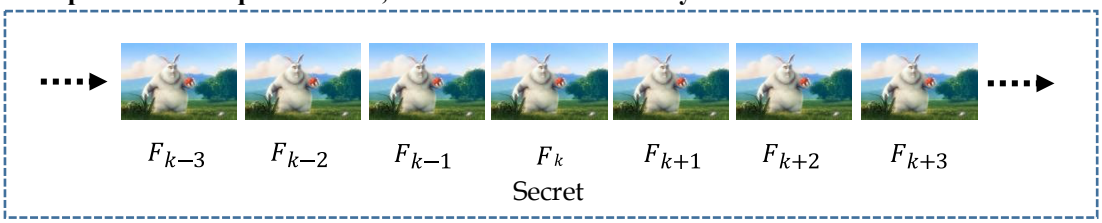


Fig. 3.3: Neighbouring frame sequence of secret frame

As shown in Fig. 3.3, let F_k is a secret frame selected by stego key from the sequenceof K cover video frames each of having size $M \times N$. The non-dynamic region from cover video frame F_k is obtained by taking the absolute difference between the corresponding pixel values of each R, G and B components of neighbourhood sequential frames $F_{k\pm i}$, $i = 1, 2, 3 \ldots t$.

The mathematical formulation of ADM is described as under.

$$d_{pq} = |F_{pq,k} - F_{pq,k\pm i}| \quad (3.1)$$

Where, $p = 1, 2, \ldots M$, M is the height of cover video frame
$q = 1, 2, \ldots N$, N is the width of cover video frame
$k = 1, 2, \ldots K$, K is the Number of cover video frames

pq is the index of pixel of cover video frame and $F_{pq,k}$ is the intensity valueof pixel of K cover video frame.
$i = 1, 2, \ldots t$, Where t is an integer indicates the number of framedifferences taken from frame k such that $1 \leq k - i < K$ and $1 < k + i \leq K$.
d_{pq} = Absolute difference between corresponding pixels of neighborhoodcover video frames

Condition:

$|F_{pq,k} - F_{pq,k\pm i}|$

$R1$

$|F_{pq,k} - F_{pq,k\pm i}| = 0$ $then$ $Non - dynamic\ pixel = F_{pq,k}$

$|F_{pq,k} - F_{pq,k\pm i}|$

B

$Otherwise$ $None$

The set of all non-dynamic pixels $F_{pq,k}$ constructs a non-dynamic region from thesecret frame F_k. The algorithm of ADM is given as under.

Algorithm 3.1: Absolute Difference Method (ADM)

Input: Cover video frames (F_k): M Rows, N Columns
Output: Non-dynamic ROI (ξ)
 # ADM : $\xi = ADM(F_k)$

1. Begin
2. for each $l = 1\ to\ 3$
3. $f_{l,k} = F_k(:, :, l)$ //Takes any channel from the RGB planes of F_k
4. for each $row\ p\ of\ f_{l,k}$ // $p = 1, 2, \ldots M$
5. for each $column\ q\ of\ f_{l,k}$ // $q = 1, 2, \ldots N$
6. $d_l(p, q) = |f_{l,k}(p, q) - f_{l,k\pm i}(p, q)|$, i is a positive integer
//Absolute difference between neighborhood frames of $f_{l,k}$
7. end for
8. end for
9. end for
10. for each
11. if all $d_l(p, q) = 0$ for each $l = 1, 2, 3$
12. $\xi(r, c) = F_k(p, q)$ // Non-dynamic Region (ξ) of F_k
$r = 1, 2, 3, \ldots R$ and $c = 1, 2, 3, \ldots C$
13. end if
14. End

Output: Non-Dynamic ROI (ξ) of size $R \times C$.

1.1 3.2 Transform Coefficients

The extracted ROI; non-dynamic region by ADM or the motion region by EBMA methodis further transformed from spatial to the frequency domain using one of the transform coefficients; Two-dimensional Discrete Cosine Transform (2D-DCT), Two-dimensional Discrete Sine Transform (2D-DST), and Two-dimensional Fast Fourier Transform (2D-FFT). These coefficients provide a variety of secret positions known as carrier object where the secret message can be concealed more securely. DCT and DST coefficients are havingtwo different types of secret positions; integer and fractional part of coefficients. Although,both the parts have their own significance in embedding the secret data but, the fractional part provides more accuracy in data hiding. Selecting the fractional part has very little impact on pixel value variation while reversing back from frequency to a spatial domain using inverse transformation. Also, FFT coefficients are in the form of a complex numberhaving real and imaginary part. Even both the real and imaginary part consists integer anda fractional part that provides a variety of secure positions for data hiding. Again, during embedding, the variation in the fractional part of both real and imaginary components causes a minor impact on pixel value variation while inverse FFT is performed. The characteristics of the kind of carrier object improve the visual quality of the embedded video. Ultimately, the imperceptibility is significantly enhanced.

The integer or fractional part of transform coefficients of RGB region of interest isconverted into binary form. The random least significant bit (LSB) vector is constructed byselecting a random bit-plane from the above binary number of each RGB component. Thesecret RGB image to be concealed is converted into binary form. The whole or partial set of bits of the secret image is embedded into a random LSB vector of carrier object using ahighly secured embedding key.

Now, by reversing the above embedding process the stego video is constructed. In this reverse process, the embedded random LSB vector of RGB component is transformedfrom frequency domain to spatial domain using inverse transform coefficient 2D-IDCT, 2D-IDST, and 2D-IFFT respectively. This inverse transformation provides the stego non- dynamic or motion region known as stego ROI (ξ). Furthermore, the stego ROI is replaced at their respective position into the secret cover video frame results as secret stego cover video frame ($\bar{F}$).

The compressed stego video (Ψ) is created by substituting the stego frames (F) at the locations of the secret frames (F) with cover video frames. In this case, the H.264 video codec handles video compression and incorporates entropy coding, motion vector estimation, transform coefficient, intra- and inter-frame prediction, and motion vector assessment [1, 2]. The three stages listed below are used to carry out the H.264 encoding procedure: First, prediction; second, quantisation and transformation; and third, bitstream encoding.

1) Prediction: Using intra- or inter-frame prediction techniques, the macroblock is anticipated from the data that has already been programmed into the system. Remaining macroblock is obtained by subtracting it from the current macroblock. The intraframe prediction approach, in its simplest form, predicts macroblocks within of frames. whereby it predicts the macroblock from its neighbouring pixels using the block sizes of 16×16 and 4×4 pixels. On the other hand, the inter frame prediction approach uses references to pixels from comparable locations in previously coded frames to forecast a 4x4 macroblock in the current frame.

2) Transform and Quantization: The generated residual macroblock in predictive mode is changed through the use of 4×4 or 8×8 integer transform using two-dimensional Discrete Cosine Transform (2D-DCT) which is specified in Eq. (4.1). Furthermore, by raising the quantisation parameter (QP), which sets more coefficients to zero, the DCT coefficients are quantised. This results in significant compression at the expense of low decoding image quality. Through dividing an integer value, the DCT converted coefficients are quantised, resulting in a block where most or all of the coefficients are zero.

3) Bitstream Encoding: Quantised transformed coefficients are encoded using various techniques, such as arithmetic coding and variable length coding, to produce the compressed bit stream.

3.2.1 Extracting Method

The stego cover video (Ψ) is used to extract the secret RGB picture (Ω) during the extraction step. Using an H.264 decoder, the stego video is first divided into stego video frame sequence. The entropy decoder decodes the encoded H.264 bit-stream. It then rescales the data using the appropriate quantised parameter and inversely transforms it using the inverse converted coefficient to produce the residual macroblock. The decoded macroblock is derived by adding the anticipated macroblock from the previously coded frames, both intra-frame and inter-frame. The retrieved video

frames were the decoded macroblocks.

The same stego key implemented in embedding process is again used to select the secret stego cover video frames ($\bar{F}$) in which the secret message has been embedded. The stego ROI (ξ); stego non-dynamic region or stego motion region is extracted from the stego cover video frame ($\bar{F}$) either by ADM or by EBMA method respectively. Furthermore, the respective transform coefficient implemented during embedding process viz. DCT, DST, or FFT is used to transform each RGB component of stego ROI (ξ) from spatial domain to frequency domain. The integer or fractional part of transformed RGB stego ROI componentis converted into binary LSB vector where the secured extracting key is applied to extract the secret RGB image (Ω).

4. **Results**

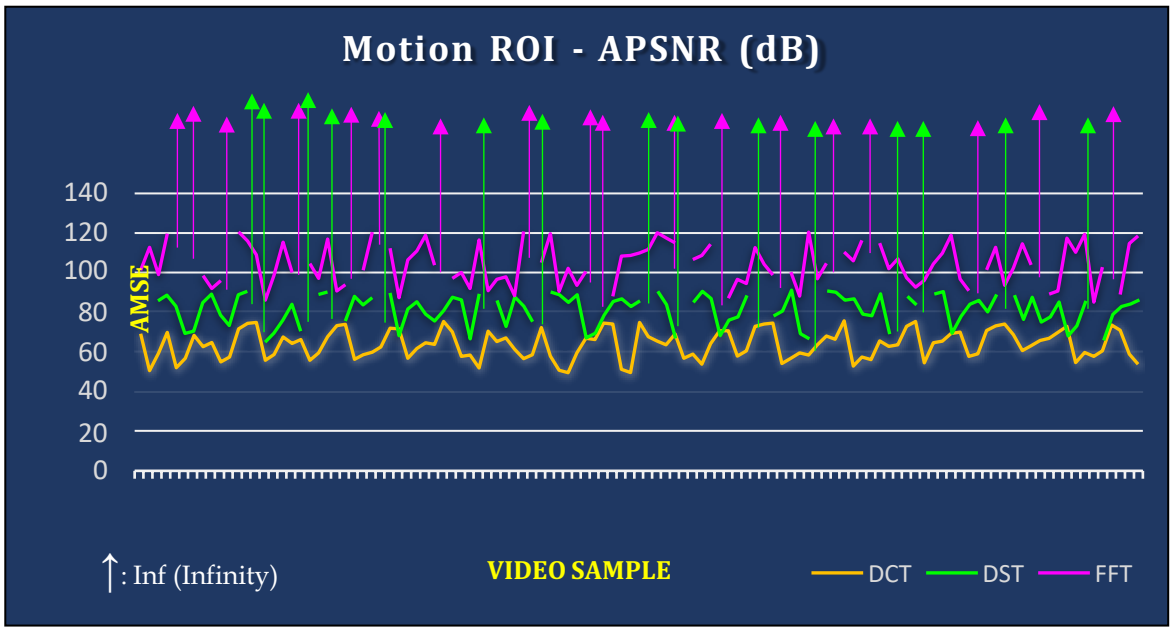
2. Comparative Analysis of Proposed "DCT, DST, and FFT" based Video Steganography using Motion Cover ROI

Sr. No.	Video Name	Cover Video Size (Height ×Width)	No. of Frames selected from Cover Video	Secret Message (SM) Name	Secret Message Size (Height ×Width	DCT				DST				FT				Embedding Capacity
						Imperceptibility		Robustness		Imperceptibility		Robustness		Imperceptibility		Robustness		
						AMSE	APSNR (dB)	Sim	BER (%)	AMSE	APSNR (dB)	Sim	BER (%)	AMSE	APSNR (dB)	Sim	BER (%)	HR (%)
1	Basketball Drive	1080 × 1920	3	SM1	242 × 150	0.0073364	69.476	1.000	0.008	0.0000599	90.358	0.918	0.029	0.0000046	101.508	0.968	0.010	0.5835
2	Basketball Drive	576 × 720	3	SM2	120 × 194	0.4900951	51.228	0.957	0.010	0.0000000	Inf	0.524	0.037	0.0000003	113.257	0.695	0.034	1.8711
3	Basketball Drive	240 × 320	6	SM3	129 × 80	0.0671708	59.859	0.398	0.481	0.0001576	86.154	0.273	0.447	0.0000077	99.249	0.058	0.486	2.2396
4	Basketball Drive	1080 × 1920	3	SM4	339 × 210	0.0062702	70.158	0.809	0.038	0.0000799	89.108	0.972	0.037	0.0000001	120.142	0.620	0.035	1.1444
5	Basketball Drive	480 × 720	6	SM5	291 × 180	0.3616432	52.548	0.535	0.565	0.0002921	83.475	0.661	0.595	0.0000000	Inf	0.343	0.451	2.5260
6	Basketball Drive	240 × 352	9	SM6	145 × 234	0.1201380	57.334	0.034	0.937	0.0071991	69.558	0.404	0.960	0.0000746	89.403	0.420	0.702	4.4626
7	BQ Terrace	1080 × 1920	3	SM7	339 × 210	0.0085878	68.792	0.968	0.016	0.0055652	70.676	1.000	0.004	0.0000000	Inf	0.986	0.027	1.1444
8	BQ Terra	576 ×	6	SM8	162 × 262	0.0314906	63.149	0.895	0.507	0.0002006	85.107	0.301	0.473	0.0000087	98.753	0.107	0.456	1.7445

	ce	704																
9	BQ Terrace	240 × 352	9	SM9	216 × 134	0.0194438	65.243	0.8046	0.0727	0.0000729	89.505	0.8395	0.0811	0.0000397	92.143	0.8380	0.0984	3.8068
10	BQ Terrace	144 × 176	9	SM10	113 × 70	0.1810424	55.553	0.8119	0.0733	0.0008466	78.854	0.8400	0.0906	0.0000159	96.117	0.8292	0.0972	3.4678
11	Cactus	1080 × 1920	6	SM11	260 × 420	0.1042030	57.952	0.9122	0.0427	0.0028509	73.581	0.8524	0.0520	0.0000000	Inf	0.9201	0.0478	0.8777
12	Cactus	576 × 720	6	SM12	170 × 275	0.0041208	71.981	0.8552	0.0536	0.0000791	89.147	0.8641	0.0558	0.0000000	121.146	0.9255	0.0404	1.8788
13	Cactus	288 × 352	3	SM13	60 × 97	0.0022217	74.664	0.9930	0.0025	0.0000517	90.992	0.9827	0.0018	0.0000001	116.508	0.9748	0.0034	1.9137
14	Cactus	240 × 320	6	SM14	105 × 169	0.0020035	75.113	0.9349	0.0438	0.0000000	Inf	0.9245	0.0441	0.0000008	109.307	0.8826	0.0568	3.8509

The comparative analysis of the results obtained by the transform coefficients DCT, DST, and FFT of motion cover ROI is described in Table 7.3.Table 7.3: Comparative Analysis of Video Steganography by Transform Coefficients DCT, DST, and FFT of Motion Cover ROI

Fig. 7.2 (a): Comparison of DCT, DST and FFT Motion ROI – APSNR



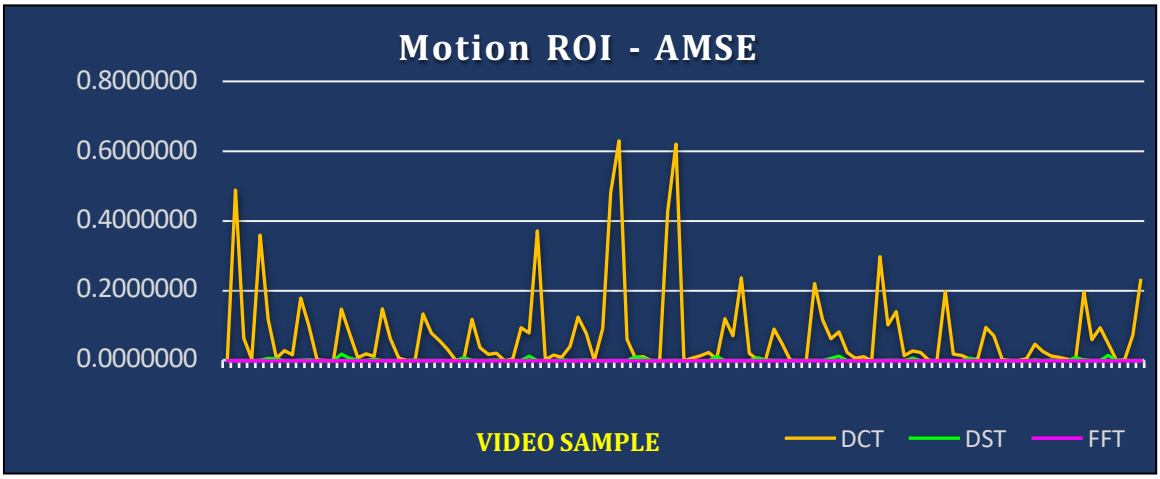


Fig. 7.2 (b): Comparison of DCT, DST and FFT Motion ROI – AMSE

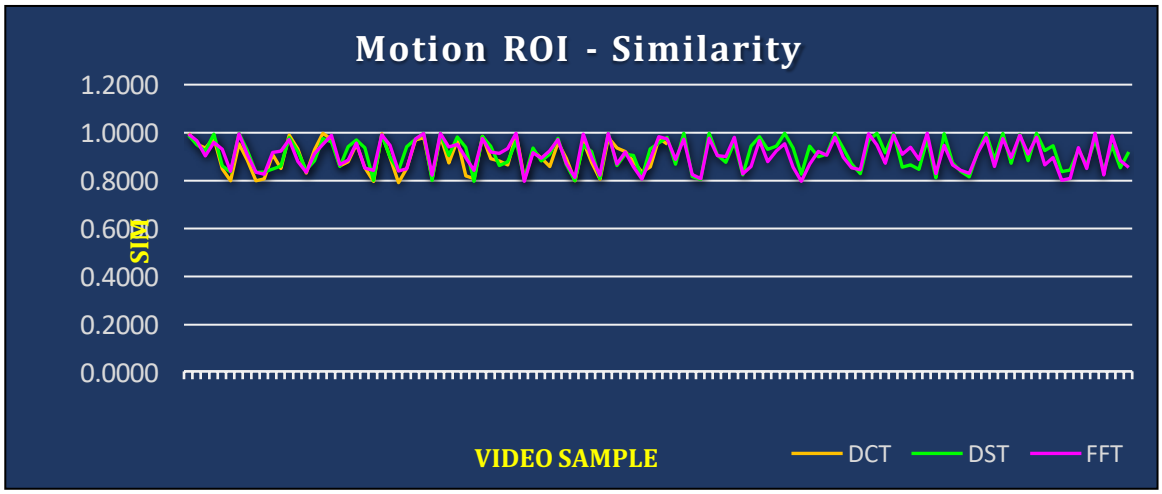


Fig. 7.2 (c): Comparison of DCT, DST and FFT Motion ROI – Similarity

The above tables Table show that the APSNR value is gradually increasing as DCT, DST and FFT-based video steganography methods are applied for cover motion ROI. Thecorresponding AMSE value for the above methods are in the range of 0.0016 – 0.6312, 0.0000 – 0.0199 and 0.0000 – 0.00019 leads the APSNR value in the range of 50.129 – 76.005 dB, 65.128 – Inf (dB), and 85.147 – Inf (dB) respectively. The increment in APSNR value improves the imperceptibility as the visual quality of stego video.

In comparing Similarity and BER for all the above methods, Sim is very much nearby 1 while BER varies from 0.00 to 0.99, which shows the high robustness of the proposed video steganography method against compression.

Furthermore, the comparative analysis of all the methods having the same HR in allthe above cases because of the resolution of cover video and secret message remains constant. The obtained HR value is always greater than 0.5% for each case indicates a highembedding capacity of proposed video steganography methods.

The comparison of video steganography based on "DCT, DST, and FFT" for Motion ROI application on real-time video dataset is also expressed in Table 7.4. The proposedmethods are compared on the basis of quality assessment parameters used as above. The results obtained for AMSE, APSNR, Sim, BER, and HR are tabulated as shown in Table 7.4.

5 . Conclusion

This chapter has discussed the proposed video steganography method in the compressed domain using three types of transform coefficients DCT, DST, and FFT of two types of ROI; non-dynamic and motion region of the secret cover video frame. Also, the ADM method used to extract the non-dynamic region and the EBMA method used for extracting the motion region from the secret cover video frame has been mathematically explained along with the algorithm. Moreover, both the embedding and extracting processes of videosteganography at the sender and receiver end have been described.

References:

1. Kousik Dasgupta, J. K. Mandal, and Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No. 2, April 2012. [DOI: 10.5121/ijsptm.2012.2201].
2. Ramadhan J. Mstafa, Khaled M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes", Multimedia Tools and Applications, Volume 75, Issue 17, pp. 10311–10333, Springer November 2015. [DOI: https://doi.org/10.1007/s11042-015-3060-0].
3. Ramadhan J. Mstafa & Khaled M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis [J]", Multimedia Tools and Applications, Volume 76, Issue 20, pp. 21749–21786, Springer October 2017. [DOI: https://doi.org/10.1007/s11042-016-4055-1].
4. Ramadhan J. Mstafa, Khaled M. Elleithy, and Eman Abdelfattah, "Video Steganography Techniques: Taxonomy, Challenges, and Future Directions", Applications and Technology Conference (LISAT), 2017 IEEE Long Island. pp. 1 – 6, IEEE 2017. [DOI: https://doi.org/10.1109/LISAT.2017.8001965].
5. Shuyang Liu, Degang Xu, "A Robust Steganography Method for HEVC Based on Secret Sharing", Cognitive Systems Research, Volume 59, pp. 207 – 220, Elsevier, January 2020. [DOI: https://doi.org/10.1016/j.cogsys.2019.09.008].
6. Mennatallah M. Sadek, Amal S. Khalifa, Mostafa G. M. Mostafa, "Video steganography: a comprehensive review", Multimedia Tools and Applications, Volume 74, Issue 17, pp. 7063–7094, Springer March 2014. [DOI: https://doi.org/10.1007/s11042-014-1952-z].
7. Feng-Cheng Chang and Hsueh-Ming Hang, "Layered Access Control Schemes on Watermarked Scalable Media", Journal of VLSI Signal Processing 49(3), pp. 443- 455, Springer 2007. [DOI: https://doi.org/10.1007/s11265-007-0095-0].
8. Hsiang-Cheh Huang, Shu-Chuan Chu, Jeng-Shyang Pan, Chun-Yen Huang, BinYih Liao, "Tabu search based multi-watermarks embedding algorithm with multiple description coding", Information Sciences Journal, Volume 181, Issue 16, pp. 3379-3396, Elsevier 2011. [DOI: https://doi.org/10.1016/j.ins.2011.04.007].
9. Jialiang Peng, Bassem Abd El-Atty, Hany S. Khalifa, Ahmed A. Abd El-Latif, "Image watermarking algorithm based on quaternion and chaotic Lorenz system", Eleventh International Conference on Digital Image Processing, Volume 11179, 111790W, ICDIP 2019. [DOI: 10.1117/12.2539753].
10. Adnan M. Alattar and Osama M. Alattar, "Watermarking Electronic Text Documents Containing Justified Paragraphs and Irregular Line Spacing", In: Proc. of SPIE, pp. 685–695, 2004. [DOI: https://doi.org/10.1117/12.527147].