Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 657-669
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.70

Novel video Steganography approach with the combination of knight tour and 7th bit model of embedding data

Sharath M N, Research Scholar, Department of Computer Science, Department of Computer Science, Dayananda Sagar University, sharathmn64@gmail.com
Dr. Rajesh T M, Asst. Professor, Department of Computer Science, Department of Computer Science, Dayananda Sagar University, rajesh-cse@dsu.edu.in
Dr.MallanagoudaPatil, Associate Professor, Department of Computer Science, Department of Computer Science, Dayananda Sagar University, sharathmn64@gmail.compatil-cse@dsu.edu.in

Abstract- The art of video steganography is a promising tool in the science of secret communication by hiding the information in the cover video without any detectable changes in the cover file. The dynamic nature of the video format makes it immune to cyber-attacks which in turn helps in secret communication. As the attention to video file sharing is rapidly growing, it is vital to have enhanced and novel steganographic techniques.

New approaches have been suggested to cover the hidden message in a video file with the proposed technique in this article. The confidential data is disguised by shielding them in the 7th bit of the identified pixel and the following pixel. Whereas the pixel in which the secret data should be shielded is picked using a knight tour algorithm that applies an added security to the secret message from cyber trespassers.The competence of this novel algorithm is proved by enumerating various parameters such as PSNR, MSE, SSIM, and embedded capacity.

Keywords: Video Steganography, Knight Tour, 7th bit model, embedded capacity, Robustness

I. INTRODUCTION:

Information is the modern fuel that keeps the globe spinning. Information protection provides a major contribution to the safety of information. While there are many effective approaches for Information Security, there is still space for improvement and tuning to enhance their performance and protection. Information Security technologies are divided into two groups, i.e, information encryption and information hiding. These two methods shall be used to protect the records. Information Encryption and Data hiding strategies have been established in [1, 2]. The figure indicates the classification of security systems.

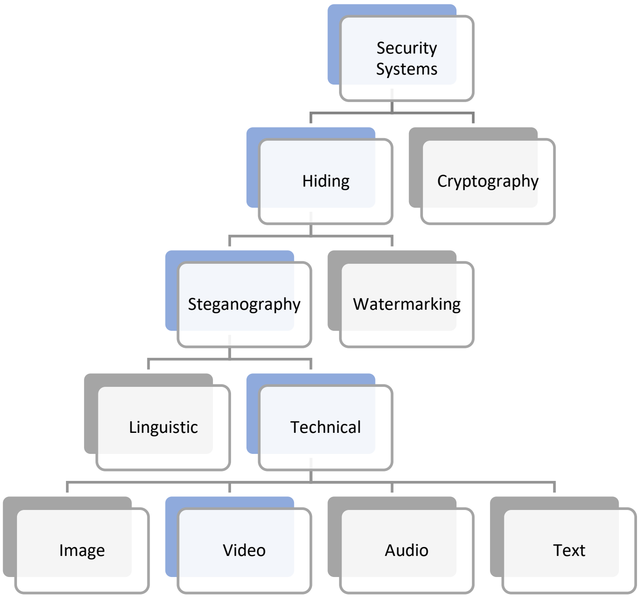


Figure 1: Classification of Security Systems

Cryptography is a technique that encrypts and sends messages in an unreadable format. It scrambles sensitive information in such a way that it appears to be a twaddle to any unintentional person. Security keys play an essential position in cryptography.

Cryptosystem refers to a collection of algorithms required to implement a security service, most commonly for confidentiality purposes. Usually, the cryptosystem consists of three algorithms: one for key generation, one for encryption, and one for decryption [3].

Watermarking was considered for many copy prevention and copyright protection applications by injecting author-related information into a signal or image. Watermark information is usually used to classify the copyright holder and to ensure that royalties are properly paid [4]

Steganography is an effective instrument of information security that communicate information in any media in a way that there is no chance of any unintended users to realize that there is a secret message being hidden in the media [5]. This unique character of steganography makes it a bullet security system in information security.

Video steganography:

Video steganography is a subdivision of data hiding, in which the secret data is hidden in the video file and is used in many areas such as medical services, enforcement agencies, trademark protection and access management, and so on[6].

The popularity of video steganography relies on two major facts. Digital Information can be conveniently modified and apprehended by users through the exponential advancement of internet applications[7].Video is an interactive medium that can be more suited than other multimedia because of the boom of strong digital video content share and transmitting tools and their scale.

In any good steganography scheme, three primary factors should be considered: imperceptibility, robustness and embeddingcapacity.

Imperceptibility is directly connected to the protection of the steganography methods that hide the hidden message in the embedded recording. Strong imperceptibility implies a low degree of alteration and decent visual consistency of the embedded video[8].

Robustness is another criterion for assessing the intensity of the steganography system against threats in video steganography. The explanation for considering robustness is that an embedded message will often not withstand a number of deliberate or accidental assaults, such as data exchange, transmission failure, frame distortion, and scaling [9]. Robustness is essential to the quality of the video steganography system, as stated in the literature in[10], extremely efficient steganography implementations ought to be robust against both signal analysis and adaptive noise.

Embedding capability is a crucial requirement and is described as the number of hidden messages that can be inserted in a visual media. The higher embedding ability ensures that more hidden messages may be inserted. However, higher embedding capability may contribute to a higher risk of poorer visual quality and an improvement in bitrate for embedded video[13].

A modern and updated approach to video steganography is applied and validated in this research report, which promises efficiency and quality enhancements. In addition, this method discusses the principal aspects of the steganography mentioned above. The relevant works are described in the next section followed by the suggested approach and algorithm. The experimental results are addressed and compared with other steganography techniques in the results section and the conclusion section reflects the inferences achieved in this experiment.

Related works

As video steganography is rapidly growing, various research and algorithms are developed. Many of the critical details are generated in a digital picture by the most significant bits[12], which will physically degrade the consistency and visual quality with the modification of the MSB's on the pixel.Hence most of the researchers choose the LSB approach to hide the hiddendata in the visual media. Hidden message bits can easily be inserted in this conventional form, by replacing the least significant bits of the image pixels.As only LSB is changed, the factor of change is so minimal that is +1 or -1 [13]. This method thus makes it uncomplicated for the intruders to assault the confidential data by picking the least significant bit.

Various enhancements to the LSB substitution method were proposed [12, 14]. However, they have not amplified the hiding ability and visual efficiency of the resultant video file [15].The hidden message is contained in themoderately significant bit of the cover picture in the literature[14]. The designed algorithm selects a replacement matrix to embed hidden messages, and the local pixel adjustment method is used to boost the accuracy of the stego-image.

But the local pixel correction procedure is not as powerful and optimal as it does not take all the bits into account. Instead, the last three bits and the fourth bit are taken into account, which is not an ideal solution[16].

Some analysts use histograms as a crucial element in embedding a hidden message and boosting dynamic range.Histogram-shifting data hiding scheme restricts the highest point in order to boost the accuracy of the stego-image[17]. The multi-dimensional and multi-layer data embedding process[18] in which two-dimensional discrepancy histogram adjustment is rendered is used to increase the hiding ability and PSNR.However, owing to its complexity and time usage, this approach is not inexpensive.

Transform domain techniques are used in steganography by manipulating the coefficients of the media in which the message is to be hidden and concealing the confidential data on the manipulated coefficients. Some literature claim that the transform domain steganography techniques are stable and secure [19]. The transformations such as fourier, discrete cosine transform (DCT), and wavelet transforms are being used in steganography. The literature [20] proposes a steganography algorithm using discrete wavelet transform difference modulation (DWTDM) and conceals secret message in adjacent DWT coefficients.

Integer wavelet transformation (IWT) is used to maximize hiding ability by mapping integers to integers[21]. Using IWT in combination with the LSB method was used for secure video steganography. [22]. Multiple group pictures technique is also implemented and evaluated their performances in video steganography [23,24].

While tremendous efforts have been made to develop video steganography techniques, there are many obstacles and challenges.Embedding on uncompressed video makes the algorithm and the hiding process not robust against compression. On contrary, the compressed video makes the process more complicated as it requires some decompression techniques for embedding the confidential data. In some approaches, all the frames are utilized without any intelligence of selecting the frame. The entire frame is still being focused on to conceal the hidden message that may contribute to the video's low visual quality. It is very necessary for any steganography technique to be safer and more resistant to 'human visual assaults.' In view of these problems and concerns, a modern improved video steganography methodology is proposed that focuses on the spatial domain.

II. PROPOSED METHOD:

The ultimate purpose of any video steganography is to mask data without compromising data quality and to keep it hidden. The suggested approach also guarantees that the imperceptibility, robustness and embedding capacities are accomplished, which are the most critical elements of steganography techniques. The first and foremost procedure is the preparation of the secret message. The message is encrypted and translated from its initial type into binary.

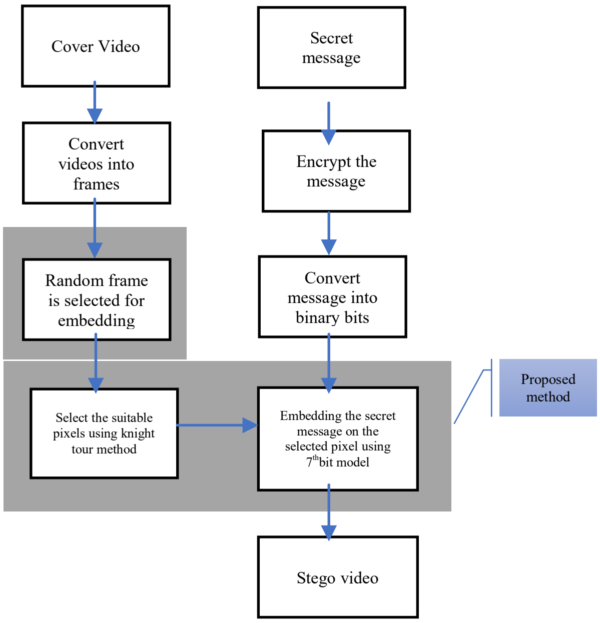

Cover Video
Secret message
Convert videos into frames
Encrypt the message
Random frame is selected for embedding
Convert message into binary bits
Proposed method
Select the suitable pixels using knight tour method
Embedding the secret message on the selected pixel using 7th bit model
Stego video

Figure 2: Proposed Architecture of Video Steganography

Selection of frames:
In this approach, the first step of the video steganography requires the selection of frames for hiding.The selection of frames algorithm uses a pseudo-random generator (PRG) which selects the frames randomly from 0th to 20th frames. This selector algorithm also ensures that there is no repetition in the frames selected [25].

Let the range selected to generate the random frame using PRG be 'n'. The initial value can be feed using the polynomial $x^1 + x^2 + x^3$ and the feedback can be $(x^2 + x^3)\ mod n$

Embedding process:

Hidden message embedding is the method of selecting the position of the pixel and hiding the secret detailsin the chosen pixel position. Pixel location selection where the coded message to be concealed is achieved using the knight tour algorithm and hiding technology is performed using the 7th bit of the chosen pixel and its successive pixel value.

Knight tour algorithm.

Instead of the traditional method of selecting the pixel location where the serial selection is involved, it is vital and more effective to select the pixel in a random fashion. The knight tour algorithm ensures random selection based on the inspiration of the knight in the chessboard [26].The chosen frame is virtually converted into a chessboard in order to make the knight do its magic.
This algorithm splits the chessboard into blocks. In the $n \times n$chessboard, the knight moves once to all squares, as seen in Figure. Via this technique, data protection can be tightened over the Pseudo-Random Number Generator (PRNG) technique as the search space is comparatively large.

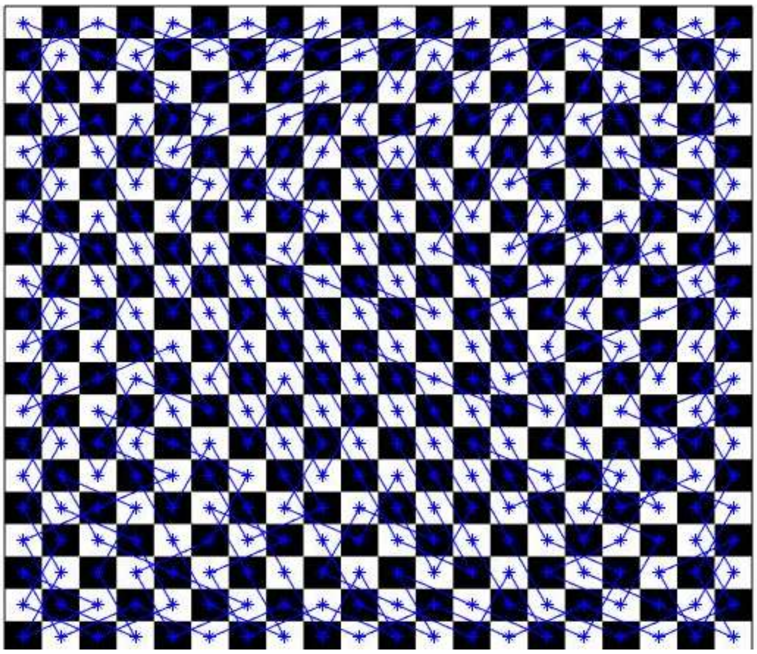
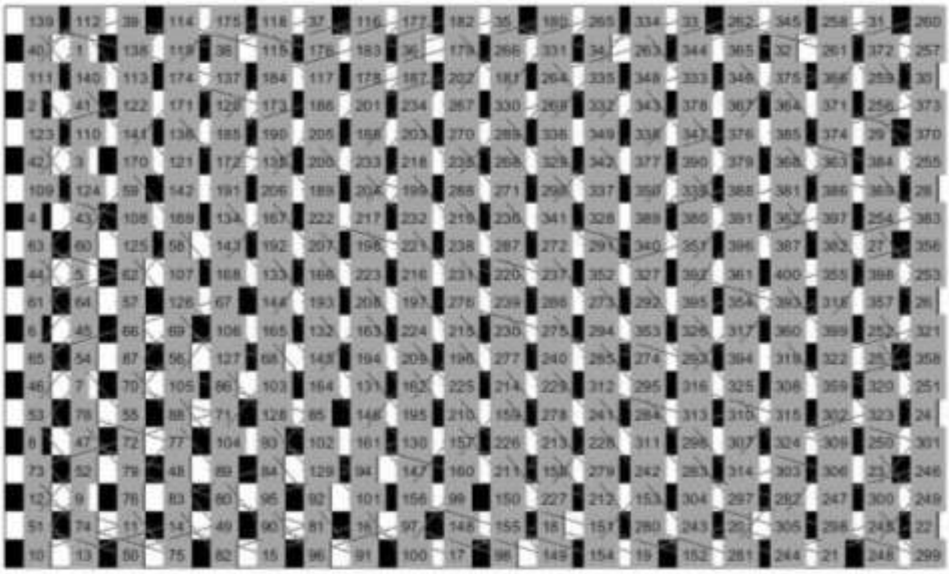


Figure 3: 20 x 20 chessboard knight tour travel

In our proposed algorithm, the chessboard of size 20 x 20 is used to ensure security by increasing the search space in the video. Also, the algorithm covers all the pixels only if the size is divisible by 4.The following table shows the pixel traversing of a 20 x 20 matrix.



139	112	39	114	175	118	37	116	177	182	35	180	265	334	33	262	345	258	31	260
40	1	138	119	38	115	176	183	36	179	266	331	34	263	344	365	32	261	372	257
111	140	113	174	137	184	117	178	187	202	181	264	335	348	333	346	375	366	259	30
2	41	122	171	120	173	186	201	234	267	330	268	332	343	378	367	364	371	256	373
123	110	141	136	185	190	205	168	203	270	289	336	349	338	347	376	385	374	29	370
42	3	170	121	172	135	200	233	218	235	269	329	342	377	390	379	368	363	384	255
109	124	59	142	191	206	189	204	199	288	271	290	337	350	339	388	381	386	369	28
4	43	108	169	134	167	222	217	232	219	236	341	328	389	380	391	362	397	254	383
63	60	125	58	143	192	207	198	221	238	287	272	291	340	351	396	387	382	27	356
44	5	62	107	188	133	166	223	216	231	220	237	352	327	392	361	400	355	398	253
61	64	57	126	67	144	193	208	197	276	239	286	273	292	395	354	393	318	357	26
6	45	66	69	106	165	132	163	224	215	230	275	294	353	326	317	360	399	252	321
65	54	87	56	127	68	148	194	209	196	277	240	285	274	293	394	319	322	25	358
46	7	70	105	86	103	164	131	162	225	214	229	312	295	316	325	308	359	320	251
53	78	55	88	71	128	85	146	195	210	159	278	241	284	313	310	315	302	323	24
8	47	72	77	104	93	102	161	130	157	226	213	228	311	296	307	324	309	250	301
73	52	79	48	89	84	129	94	147	160	211	158	279	242	283	314	303	306	23	246
12	9	76	83	80	95	92	101	156	99	150	227	212	153	304	297	282	247	300	249
51	74	11	14	49	90	81	16	97	148	155	18	151	280	243	20	305	298	245	22
10	13	50	75	82	15	96	91	100	17	98	149	154	19	152	281	244	21	248	299

Figure 4: Pixel Traversing of a 20 x 20 chessboard matrix

The below graph shows the search area required for the intruders to access the secret message based on the chessboard size.

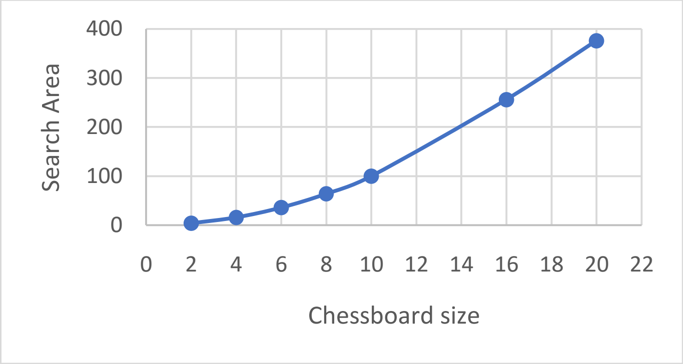


Figure 5: Comparative analysis – Chessboard size vs Search Area

7th bit model:

In the 7th bit model of the hidden message embedding, a mathematical expression is applied on the 7th bit of the identified pixel (p) and its subsequent pixel value (p + 1) which results in a 2-bit pair value. This strategy allows for four combinational bits 00, 01, 10, 11.Therefore, from each pixel 2 bit of the message can be added. This approach provides the advantage of 2 bits in one pixel without the least significant bit[27].

If C is the cover image with a size of $H * W$ pixels, the M is the N-bit hidden message, x is the pixel value and the m is the secret message bit, and then image matrix can be interpreted as,

$$C = \{x_{ij} \mid 1 \leq \mathrm{i} \leq \mathrm{H}, 1 \leq \mathrm{j} \leq \mathrm{W},\ x_{ij} \in \{0,1,\dots\dots\dots,255\}\} \qquad (1)$$

The secret message can be represented as,

$$\mathrm{M} = \{\mathrm{m_N} \mid 1 \leq \mathrm{N} \leq \mathrm{n},\ \mathrm{m_N} \in \{0,1\}\} \qquad (2)$$

Let M is the secret message, Z is the cover video, $K$is the key that can be utilized for embedding (E) and extraction of the message, $(D)$and Z' is the stego file.

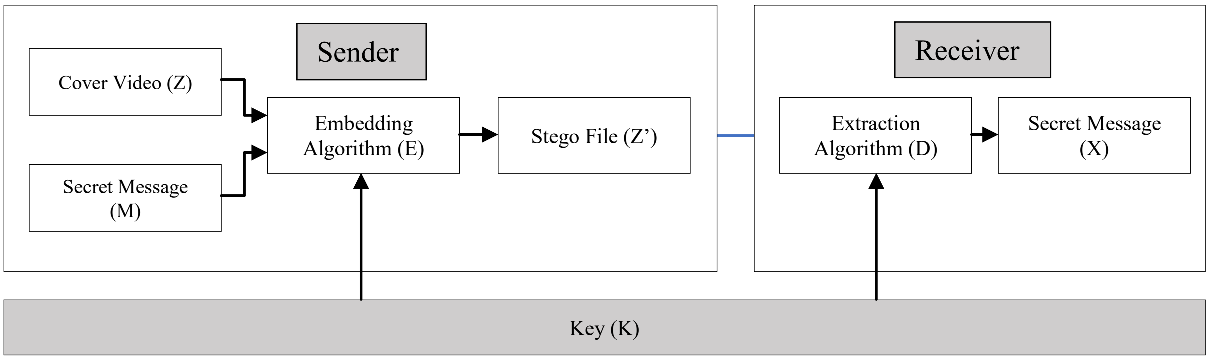


Figure 6: Block diagram of Video Steganography

The embedding of a secret message in the cover file is done using the following equation:

$$\mathrm{Z}' = \mathrm{E_K}(\mathrm{M}, \mathrm{Z}) \qquad (3)$$

In the above equation (3), $\mathrm{E_K}$ is the embedding algorithm used to hide the secret message (M) in the cover file (Z). In this approach is explained below with an example.

And the extraction process, in which the hidden message is retrieved is done using the following equation.

$$X = D_K(Z') \qquad (4)$$

Similarly, D_K is the extraction algorithm in which the hidden secret message is extracted to its original form by using the secret key (k) which is shared between the sender and the receiver. This extraction algorithm is explained clearly with a suitable example in the following section.

Consider the character *'d'* should be sent as a secret message.
The binary equivalent of the secret message '*d*' is {01 10 01 00}, and the four-pixel values selected using knight tour method are $p = \{78, 35, 68, 98\}$.

At the embedding side:

Pixel 1:
P1 = 78(01001110),
P1 + 1 = 79(01001111).
The 7th bits of P1 and P1+1 form the "11" pair, but the original two message bits to introduce are "01." Thus, we must apply **-**1 to the P1 value. Therefore,
P1′ = 77(78– 1)
where P1′ is the stego pixel.

Similarly, the bit pairs are embedded in the cover file.

Table I: Embedding of secret bits using 7th bit model

	Pixel value	Binary value	7th bit pair	Secret message bit	Additional factor	Stego pixel value
1stPixel	78 79(pixel value +1)	010011 **1** 0 010011 **1** 1	11	01	-1	77
2ndPixel	35 36	001000 **1** 1 001001 **0** 0	10	10	0	35
3rdPixel	68 69	010001 **0** 0 010001 **0** 1	00	01	+1	69
4thPixel	98 99	011000 **1** 0 011000 **1** 1	11	00	+2	100

At the extraction side

The set of stego pixels to be extracted to retrieve the secret message are {77, 35, 69, 100}.

Pixel 1:
P1' = 77(010011 **0** 1),
P1' + 1 = 78(010011 **1** 0),
The secret message bit at this pixel is 01

Pixel 2:
P2' = 35(001000 **1** 1),
P2' + 1 = 36(001001 **0** 0).
The secret message bit at this pixel is 10

Pixel 3:
P3’ = 69(010001 **0** 1).
P3’ + 1 = 70(010001 **1** 0).
The secret message bit at this pixel is 01

Pixel 4:
P4’ = 100(011001 **0** 0).
P4’ + 1 = 101(011001 **0** 1).
The secret message bit at this pixel is 00

Thus, the secret message 01 10 01 00 is extracted.
The combination of the knight tour algorithm and the 7th bit model of concealing makes this approach more effective. The imperceptibility is achieved successfully with its nature of high search area and its unreliability of LSB. The knight tour algorithm gives the freedom of expanding the embedding capacity by increasing the size of the chessboard.

III. RESULT AND DISCUSSION:

The suggested video steganography methodology was validated with different data set and evaluated using parameters such as peak signal-to-noise ratio (PSNR), mean squared error (MSE), structural similarity index (SSIM), and embedded capacity.

The peak signal-to-noise ratio is a statistical image quality measure between the actual and a processed/reconstructed image. The higher the PSNR, the enhanced image quality[28].
Mean-square error (MSE) and peak signal-to-noise ratio (PSNR) are critical picture quality indicators that empirically calculate stego file quality. MSE is the total squared error between stego file and actual file.

$$PSNR \ = \ 20log_{10}\left(\frac{max_f}{\sqrt{MSE}}\right) \qquad (5)$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1} \| \ c(i,j) - c'(i,j) \ \|^2 \qquad (6)$$

where,c is the cover file, c' is the stego file of size $m \ x \ n$ and max_f is the maximum signal value in the cover file.

The SSIM is a calculation of visual resemblance between two images. The SSIM was created by Wang et al [29] to understand the consistency of the visual system (HVS) of humans. The SSIM is classified based on the integration of three variables such as loss of correlation, luminance distortion and contrast distortionrather than conventional methods of error assessment. The SSIM is defined as:

$$SSIM = l(c,c'), c(c,c'), s(c,c') \qquad (7)$$

$$\text{where,}\begin{cases} l(c,c') = \frac{2\mu_c\mu_{c'} + K_1}{\mu_c^2 + \mu_{c'}^2 + K_1} \\ c(c,c') = \frac{2\sigma_c\sigma_{c'} + K_2}{\sigma_c^2 + \sigma_{c'}^2 + K_2} \\ s(c,c') = \frac{\sigma_{cc'} + K_3}{\sigma_c\sigma_{c'} + K_3} \end{cases}$$

In the above equation, $l(c,c')$ is the luminance comparison between the cover image c and stego file c'. Similarly, $c(c,c')$ is the contrast comparison and $s(c,c')$is the structural comparison.$K_1, K_2, K_3$are the positive constants used to avoid null denominator.

The performance analysis of the proposed method is tabulated below,

Table II: Performance analysis – MSE, PSNR, SSIM, Time

Cover Video	PSNR	MSE	SSIM (%)	Time (sec)
Video_1	84.86	0.213	100	0.133
Video_2	83.77	0.274	100	0.166
Video_3	85.53	0.183	100	0.136

Various video steganography techniques are analysed and compared with respect to PSNR in the table below,

Table III: Comparative analysis –PSNR

Cover Video	Simple LSB [12]	OMSB [14]	7th bit model [27]	Knight tour [26]	Proposed Method
Video_1	37.8642	42.353	55.401	66.525	84.864
Video_2	31.3307	41.756	55.418	62.448	83.773
Video_3	38.7242	43.156	55.477	59.904	85.532

Similarly, the MSE values are compared in the table below,

Table IV: Comparative analysis –MSE

Cover Video	Simple LSB [12]	OMSB [14]	7th bit model [27]	Knight tour [26]	Proposed Method
Video_1	0.578	0.318	0.374	0.277	0.213
Video_2	0.489	0.415	0.365	0.289	0.274
Video_3	0.536	0.378	0.326	0.227	0.183

The graph shown below, clearly compares the PSNR and MSE values of the proposed method with other methods.

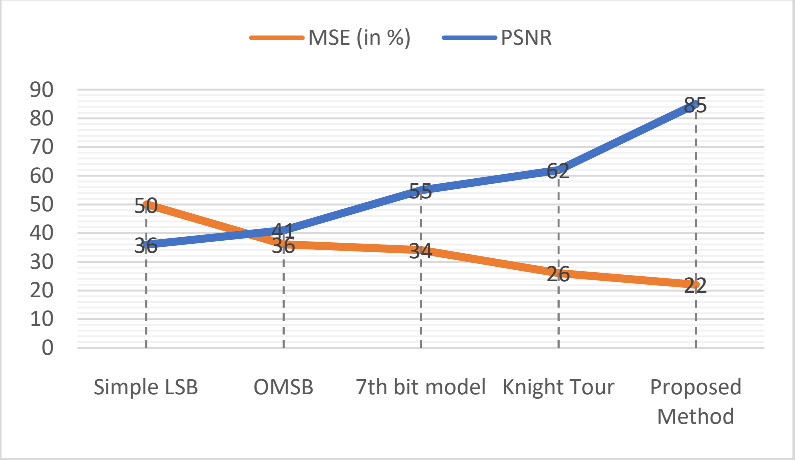


Figure 7: MSE, PSNR plot using the proposed method and other techniques

The payload is the size of the cover video's hidden message. The graph below compares the impact of the payload in the PSNR values in various video steganography techniques against the proposed method.

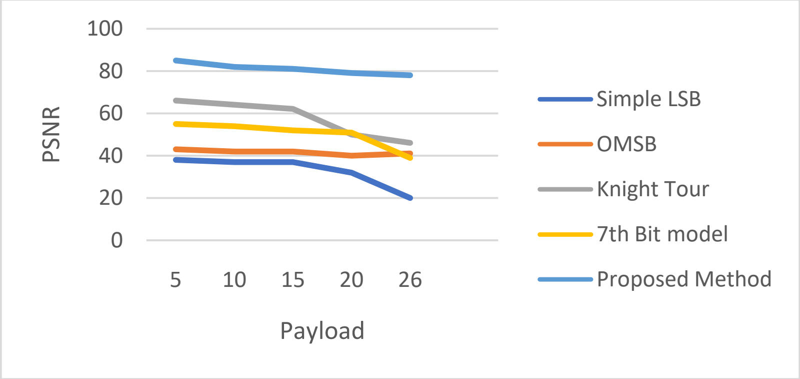


Figure 8: Payload vs PSNR for proposed method and other techniques

Embedded capacity is the rate of encrypted data in the cover file in bpp. It is defined as,

$$Embedded\ capacity = \frac{Max\ size\ of\ embedded\ \ data}{Dimension\ \ of\ video\ cover}\ (8)$$

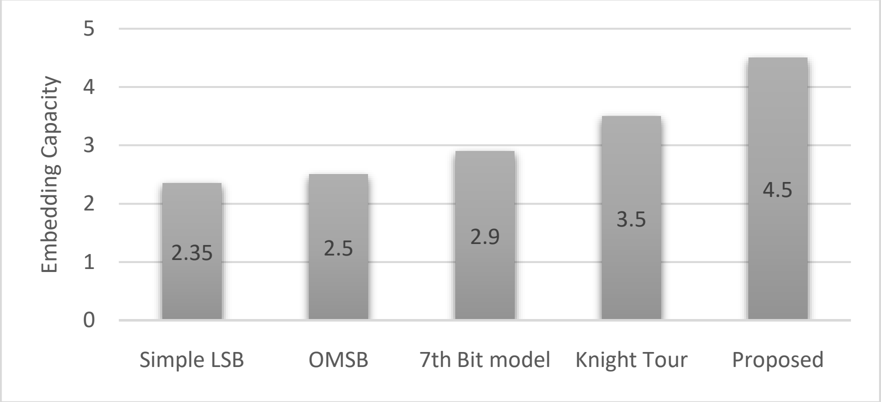


Figure 9: Comparative analysis – Embedding Capacity

The graph below clearly shows that the proposed algorithm is light wait in computation irrespective of its payload.

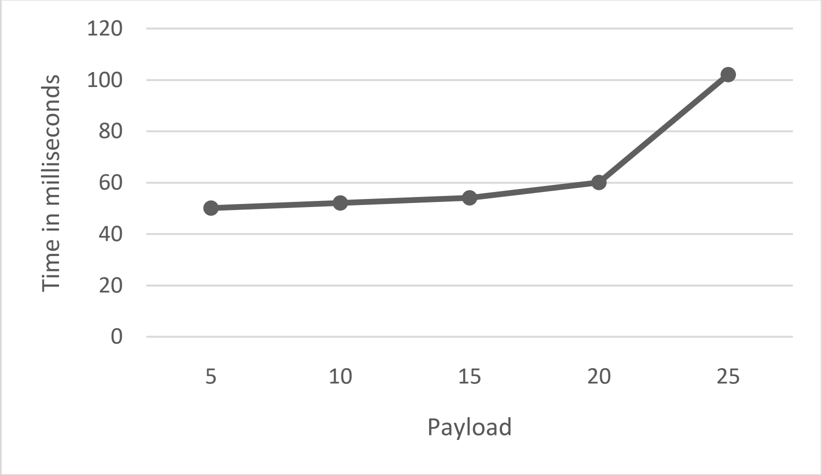
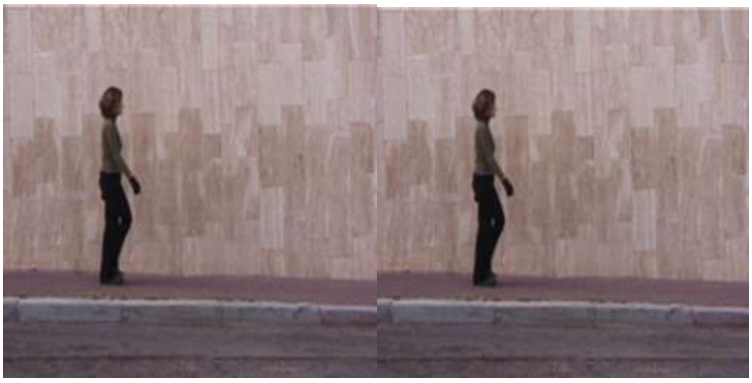


Figure 10: Comparative analysis – Payload vs Time

The following images show that there is no visual impact on the resultant video due to the process of embedding a secret message.



(a) Cover File (b) Stego file

Figure 11: Visual Comparative analysis – (a) Cover file and (b) Stego file

Thus, the experimental report clearly portrays security enhancement without sacrificing the resultant accuracy of the stego video file.

IV. CONCLUSION:

In this study, an improved video steganography technique is proposed based on the integration of the knight tour algorithm for location searching and the 7th bit model to hide the secret message. This proposed algorithm improves the security of the process by randomly selecting the frames to which the secret message to be embedded. Since the frames are randomly chosen, the frames in which the hidden message is integrated are extremely difficult for intruders to predict.This adaptive nature of the method makes it more optimized and robust. Whereas, using 7th bit model for embedding the data makes it more attack-proof by not just relying on the least significant bit like its preceding steganography techniques. The experiment is done on different data set and payload and the result shows that the PSNR and SSIM are improved greatly than other methods. We used VIRAT Dataset for the experimental analysis. In that we cropped 5000 videos with each consist of 10 seconds of play time totally 12.5hours of playtime. We achieved .2333 of MSE and the average PSNR value in this approach is around 85 which is far better than other video steganography methods. It also has the benefit of high payload and embedding power. Thus, this suggested technique proves that performance, robustness, payload power, operating time are considerably enhanced compared to other steganography techniques.

V. REFERENCES:

[1] Bender, W.,DGruhl, N. Morimoto and A. Lu (1996). Techniques for data hiding, IBM Systems Journal, Vol. 35,No. 3- 4, pp. 313-335.

[2] Petitcolas, F. A. P., R.J Anderson and M.G. Kuhn (1999). Information hiding - a survey. Proc. of the IEEE, Vol. 87, No. 7, pp. 1062-1078

[3] P. P. Hadke and S. G. Kale, "Use of Neural Networks in cryptography: A review," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-4, doi: 10.1109/STARTUP.2016.7583925.

[4] W. Hu, R. Zhou, A. El-Rafei and S. Jiang, "Quantum Image Watermarking Algorithm Based on Haar Wavelet Transform," in IEEE Access, vol. 7, pp. 121303-121320, 2019, doi: 10.1109/ACCESS.2019.2937390.

[5] Singh, Aman. (2013). A Review on the Various Recent Steganography Techniques. International Journal of Computer Science and Network. 2. 142.

[6] Liu, Yunxia& Liu, Shuyang& Wang, Yonghao& Zhao, Hongguo& Liu, Si. (2018). Video Steganography: A Review. Neurocomputing. 335. 10.1016/ j.neucom.2018.09.091.

[7] Suresh, Meenu& Sam, I.. (2020). Optimized Interesting Region Identification for Video Steganography using Fractional Grey Wolf Optimization along with Multi-objective cost function. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2020.08.007.

[8] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "Video steganography techniques: Taxonomy, challenges, and future directions," 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2017, pp. 1-6, doi: 10.1109/LISAT.2017.8001965.

[9] Sadek, M.M., Khalifa, A.S. & Mostafa, M.G.M. Robust video steganography algorithm using adaptive skin-tone detection. Multimed Tools Appl 76, 3065–3085 (2017).

[10] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," 2015 Wireless Telecommunications Symposium (WTS), New York, NY, 2015, pp. 1-8, doi: 10.1109/WTS.2015.7117257

[11] Pal A.K., Pramanik T. (2013) Design of an Edge Detection Based Image Steganography with High Embedding Capacity. In: Singh K., Awasthi A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. QShine 2013. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 115. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37949-9_69

[12] Chan, Chi-Kwong& Cheng, L.M.. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition. 37. 469-474. 10.1016/j.patcog.2003.08.007.

[13] R.J. Anderson, “Stretching the limit of steganography in information hiding,” Springer Lecture Notes in Computer Science, vol. 1174, pp. 39–48, 1996.

[14] Ran-Zan Wang, Chi-Fang Lin and Ja-Chen Lin, "Hiding data in images by optimal moderately-significant-bit replacement," in Electronics Letters, vol. 36, no. 25, pp. 2069-2070, 7 Dec. 2000, doi: 10.1049/el:20001429

[15] M. Devi and N. Sharma, "Improved detection of least Significant bit steganography algorithms in color and gray scale images," 2014 Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh, 2014, pp. 1-5, doi: 10.1109/RAECS.2014.6799507.

[16] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately significant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.

[17] Wang, Z., C. C. Chang, M. Li, S. Cui (2013). Multi-dimensional and multi-level histogram-shifting-imitated reversible data hiding scheme, Smart Innovation, Systemsand Technologies, Vol. 21, pp. 149-158.

[18] Li, X., W. Zhang, X. Gui and B. Yang (2013). A novel reversible data hiding scheme based on two-dimensional difference-histogram modification, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 7, pp. 1091-1100.

[19] Maniriho, P., & Ahmad, T. (2019). “Information hiding scheme for digital images using difference expansion and modulus function”. Journal of King Saud University-Computer and Information Sciences, 31(3), 335-347

[20] Bhattacharyya, S., & Sanyal, G. (2012). “A robust image steganography using DWT difference modulation (DWTDM)”. International Journal of Computer Network and Information Security, 4(7), 27.

[21] Jayasudha, S. (2013).”Integer wavelet transform based steganographic method using OPA algorithm”. International Journal of Engineering and Science, 2(4), 31-35.

[22] Ramalingam, M., & Isa, N. A. M. (2014). “Video steganography based on integer haar wavelet transforms for secured data transfer”. Indian Journal of Science and Technology, 7(7), 897-904.

[23] Aly, H. A. (2011). “Data hiding in motion vectors of compressed video based on their associated prediction error”. IEEE transactions on information forensics and security, 6(1), 14-18.

[24] Filler, T., Judas, J., &Fridrich, J. (2011). “Minimizing additive distortion in steganography using syndrome-trellis codes”. IEEE Transactions on Information Forensics and Security, 6(3), 920-935.

[25] k b, Sudeepa& K, Raju& H.S., Ranjan&Aithal, Ganesh. (2016). A New Approach for Video Steganography Based on Randomization and Parallelization. Procedia Computer Science. 78. 483-490. 10.1016/j.procs.2016.02.092.

[26] Younus, Zeyad&Talee, Ghada. (2020). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. Journal of Intelligent Systems. 29. 1216–1225. 10.1515/jisys-2018-0225.

[27] Joshi, Kamaldeep& Gill, Swati & Yadav, Rajkumar. (2018). A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications. 2018. 1-10. 10.1155/2018/9475142.

[28] A. Horé and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," 2010 20th International Conference on Pattern Recognition, Istanbul, 2010, pp. 2366-2369, doi: 10.1109/ICPR.2010.579.

[29] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.