International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 8336-8348

Enhancing Data Security in Video Steganography using RSA Encryption, Huffman Coding with LSB Reverse

Dr.R.Shanthakumari [1], S.Vinothkumar [2], Dr.S.Kannimuthu [3], G.Santhya [4], B.Bharaneeshwar [5]*

[1] Assistant Professor (SLG), Department of Information Technology, Kongu Engineering College, Erode.*
[2] Assistant Professor, Department of Information Technology, Kongu Engineering College, Erode.
[3]Associate Professor, Karpagam College of Engineering, Coimbatore
[4]PG Student, Department of Information Technology, Kongu Engineering College, Erode.
[5]UG Student, Department of Information Technology, Kongu Engineering College, Erode.

[1] shanabiraki@gmail.com, [2] vinoths@kongu.ac.in, [3]kannimuthu.me@gmail.com, [4]santhyagunasekaran@gmail.com, [5] bharanibala77@gmail.com

Abstract

In recent years, preventing data theft and securing the data is the main important measures in the field of digital communication technologies. For achieving the above measures, the image and video steganography are the most exceptional methodologies to hide the sensitive information in the cover medium for transferring the data over the open network. The Video steganographic algorithm has the advantage of huge concealment potential in these methods but neglects the protection when finding space. In balance the two things, each fulfills the high capacity in boost the video carrier load and can protect the confidential information securely. This paper proposes a new steganographic technique to cover the massive volume of information with the minimal distortion in a video file. In order to transfer the data with high level of security, cryptography method have been put forward. Also, this paper introduces steganography method that involves LSB reverse algorithm with RSA cryptography and

ISSN: 2005-4238 IJAST

lossless compression, so the message being sent is hidden in an exceedingly medium i.e video. The planned system is evaluated in terms of ordinary subjective measures like Mean Squared Error (MSE), and Peak Signal to Noise Ratio (PSNR). MSE and PSNR values are measured between the initial and therefore the steganographic files averaged overall video frames, to indicate the smallest degradation of the steganography video file. The experimental results show that this algorithm does not only have a nice visual and statistical invisibility, but the protection of secret information is also important and achieves the goal of protecting secret information effectively.

Keywords: Data hiding, Embedding Data, Information Security, Least Significant Bit reverse, Security, Steganography.

1. Introduction

As technology improves its vulnerabilities conjointly were increasing. Data communication involves transmission of computerized data over systems through the web medium. Several advancements have been created information communication over the past a long time. It includes Information falsification, eavesdropping and data stealing. A number of safety risks that occur throughout the data communication are unauthorized get to and watchword related dangers. Though researchers introduce a lot of subtle system for sending the information firmly over the internet medium, attackers conjointly use several intelligent ways that to penetrate it. To overcome the attacks on data communication steganography, compression and cryptography are used.

Cryptography might be a strategy of protective data and communications through the utilization of codes so solely those for whom the knowledge is implied can study and process it. It also plays a significant role in preventing the data communication and to make sure that solely approved recipient receives the message. Cryptography is particularly utilized once the information is exchanged over an untrusted medium. Cryptography involves changing the plaintext into cipher text that is referred to as encoding then back once more cipher text is born-again into plaintext referred to as decipherment. The algorithm used for encoding and decipherment is the RSA algorithm. RSA is an algorithm utilized by computers to encode and decode messages. It is an asymmetric cryptographic algorithm. The fast development of the web coupled with the dangerous upgraded in information communication has activated the need for safe forms of data communication[1-2]. The word "Steganography" comes from the Greek words "Stegano" or "Stegos" meaning covered or concealed and "Graphia" or "Graptos" meaning writing.

Therefore, a steganographic system embeds secret content in cover media (such as text, image, audio, and video) so that a snoop does not detect its existence. Image is used as a cover media in image steganographic ways to conceal the hidden data. Video steganography is one of the data hiding approaches, since the human eye is incredibly vulnerable to any alteration between the initial and altered texts, and is simply detected [3-4]. There are two parameters to analyze the performance of any steganographic technique in particular capacity refers to the amount of secret information that would be concealed inside the carrier, and protection relates to a masquerade 's versatility to figure out the hid details. Both capability and protection are considered in this paper to evaluate the performance of the planned steganographic methodology based on video. Much of this research is to get a vital increase in the amount of secret data concealed inside the cover

ISSN: 2005-4238 IJAST

medium, and also develop and use stego keys to improve security. LSB reverse algorithm and RSA encoding and decipherment is used to realize this objective. The Huffman code data compression technique is used in the proposed work for capacity increase to compress the secret data. The Huffman code algorithm is applied directly to the encrypted secret data in the proposed work, therefore the planned methodology reduces the computational complexity and also increases the capacity of the secret data. The rest of the paper is built in as follows. The related work is clarified in Section 2. The planned work is discussed in Section 3, and experimental results are listed in Section 4. Finally, the paper concludes in Section 5.

2. Literature Review

Some numerous ways and techniques within the field of video steganography were projected by the scientists. Inside the film, secret data such as text, image, audio or various video frames are concealed in video steganography. The cover video which hides information is called stego video. The video contains several image numbers known as frames. In video steganography, a specific frame from the video is extracted, and therefore the secret information is hidden in this frame when data concealing the frame is replaced in its original position within the video. A number of the papers associated with video steganography during which different ideas applied for video steganography are as follows. Dengre et al., [5] given the impact of audio Steganography with image watermarking in the video. In this process, the hidden message is encoded into the carrier audio file (.wav) in the form of an audio file. The output would be close to the carrier at the transmitter end, with the hidden message inserted inside. The intruder is blind by the signal it transmits. The initial message is recovered at the receiver end, with none injury. The complete device is simulated, and their corresponding waveforms and analysis of the results and graphs prove this method's effectiveness. Abbas et al. recommended a procedure in video steganography by utilizing the Cuckoo look calculation in [6]. In this strategy, at that time five diverse sorts used to show the bits of each byte were isolated into byte by byte in the mystery message. By calculating the similarity between the pixels and assorted byte sort, the Euclidian distance was used along these lines to select a better pixel. A while later, the levy flight randomwalk is utilized to exchange from one pixel to another arbitrarily, at that time, the LSB strategy was utilized for embedding the mystery message interior the video outline.

Mahesh et al. [7] declared the importance of efficient data transmission and therefore the confidentiality of the data to be transmitted. The protection of sensitive information remains a vital topic from the past time to the current time. A unique strategy is usually recommended during this paper to cover the message's presence therefore it is tough for an intruder to notice it. This paper deals with video steganography algorithms that use patch wise code creation techniques to conceal video file within a particular video. Pooja Yadav et al., [8] along with cryptography, recommended a model for secure data transmission using video steganography. Video steganography is employed in this scheme to hide a hidden stream of videos in a cover video feed. Each secret video frame was broken into individual elements, then reborn into 8-bit binary values, and encrypted using XOR with the secret key and encrypted frames are hidden in the least significant bit of each frame using sequential video cover encoding. An increasing amount of secret frames will be stored according to a BGRRGBGR pattern in cover frames to boost greater protection.

Sahu and Mitra presented a video steganography strategy in 2015, using the LSB strategy and the Advanced Encryption Standard (AES) strategy [9]. In this strategy, using the AES method the information about the mystery was scrambled. The frames used to implant the information were then selected arbitrarily, and the pixel swapping algorithm was used to upgrade the security. After that, the LSB strategy was utilized to insert the

ISSN: 2005-4238 IJAST

mystery information inside the selected video outline. Rahul Paul et al., [10] presented a new model that uses video steganography to cover large quantities of data. In this process, the video file as the cover file is used to replace the Least Significant Bit (LSB) technique, and the details are embedded in the frames where the scene has changed in the video series. In addition to that, the pixel positions randomized for additional protection where the information bits are stored by creating an indexed chaotic sequence and arranging the location of the pixel according to the sequence. In 2016, Sethi and Kapoor used the AES cryptographic algorithm and the genetic algorithm to display a video steganography strategy [11]. A while later, the AES calculation was used to exchange the compressed message into the content of the cipher, and after that the encoded message was inserted into the image using a genetic algorithm and the LSB strategy, where the genetic algorithm is used to select the pixels used to implant the information using the LSB method.

In 2016, Saleema and Amarunnishad proposed a strategy in the field of image steganography by using an arbitrary determination of image pixels used to insert the mystery message within it and by using the LSB method to implant the image inside the information and by using partial Fuzzy Neural systems to boost image quality after insertion [12]. Alsaffawi proposed a strategy in 2016 by using LZW to play down the measure of mystery message by using EMD and knight tour algorithm to implant the image's inner secret message [13]. Ashish et al.,[14] suggested a prototype to hide text from the video. The well-known traditional approach uses image as a cover which has an embedded dimension limit and the cover will be a video to fix the limitations of embedding dimensions. The use of video-based steganography is now widespread, and numbers of steganalysis tools are available to check whether or not the video is stego-video. Most tools search hidden information with the help of LSB, DCT, Frequency Domain Analysis, etc. and find out if the video has secret data or not. Within this paper, LSB and Random Byte Hiding techniques are applied and implemented to simulate the results, based on MATLAB. In 2016, Solichin and Painem proposed a technique called the Less Important Frame (LIF) approach in video steganography[15]. In this strategy, it depended on the movement of the outline using the highlights of an optical stream to choose the outline that had the mystery message.

In 2016, Rezagholipour and Eshghi displayed a video steganography strategy based on frame development where the mystery message was embedded within the motion vectors of the moving outlines [16]. In 2017, by using an AES-128 bit strategy to encode the picture, the video steganography method was proposed by Putu et al. The LSB technique was then used to insert the encoded image within the video [17]. In 2017, Mumthas and Lijiya implemented a new video steganography method by using RSA and arbitrary DNA to encrypt the mystery message and then compressed the encoded message using the Huffman encoding. After that, the 2D DCT is used to insert the details about mysteries to expand system security [18]. Chandra Prakash Shukla et al.,[19] proposed a new method with steganography and cryptography to ensure that the message is of high protection. Another conceals the presence of the message and the other distorts the message itself. RSA Algorithm is one of the most efficient and reliable algorithms for encryption here. Shanthakumari et.al [20-29] suggested the exchange of hidden data in steganography of photographs using only the spatial domain.

Manpreet Kaur et al.,[30] proposed a framework handing with video steganography, cryptography, hash-LSB associated degreed a rule for encoding. This system uses a hashing perform to make a mask pattern for the cover video's data bits within the RGB pixel values of LSB. This strategy guarantees that before concealment during hiding in a cover video frame, the message is encrypted. If the cover video frames are exposed in any case by the cipher text, the intermediate person apart from the recipient cannot read the message as a result of it is encrypted. So, the Hash-LSB technique is a lot of economical and effective in transmitting essential knowledge on any unsafe path. Ravneet Kaur and Tanupreet Singh [31] developed a model that emphasizes

ISSN: 2005-4238 IJAST

the use of digital video/images as a cover for data hiding and steganography is used to insist on more security via encryption. The suggested approach encrypts the message in an image with ECC and covers encrypted images in cover video using LSB. It gives the attacker a high degree of protection, safety, and resistance against extraction. As ECC provides better protection with smaller key sizes, this results in quicker processing, lower power consumption as well as saving memory and bandwidth.

Prajna Vasudev and Kumar Saurabh [32] projected a video steganography model that was achieved with DCT quantization of 32*32 vectors. Past academic work has targeted on vector quantization of 16*16 in the combination of many different algorithms. Video steganography is healthier than image steganography, as a result of a lot of pictures truly be combined into it; video could be a mixture of various slices of film. This technique embodies combining DCT with an assortment of laws, which may be either fuzzy or neural. Zeyad et al.[33] projected a intelligence concealment technique in the video using the Less Significant Bit (LSB) method and lifted it by using the knight tour algorithm to conceal information in the AVI video file and using a key encoding process to encrypt the hidden message. In our projected methodology, safety and capacity problems are thought of. The RSA algorithm is straightaway used to the key knowledge and therefore the attained knowledge is compressed through the huffman algorithm. LSB reverse algorithm is employed to cover the key knowledge into the video. The projected technique will increase the hiding capacity increases and will also reduce computational complexity. In addition, the use of steganography keys further enhances safety. The proposed method is mentioned in the next section

3. Proposed Methodology

The primary purpose of this approach is to conceal a large volume of data with high quality stego video and achieve high protection for hiding information within the cover video. This section describes the approach suggested, which is divided into two phases of embedding and extraction phases. The secret message on the sender side is written with the alphabetic English. The secret message is then encrypted using the RSA algorithm and then compressed using the huffman algorithm to increase security and then embedded with the LSB reverse algorithm into the video. The obtained stego video is sent through the communication channel. On the receiver side the stego video is received from the communication channel. Then the secret message is extracted from the video using the LSB reverse algorithm. Then the message is decompressed using Huffman algorithm and then the secret message is decrypted using the RSA algorithm, so that the original message can be obtained. The different steps utilized within the implanting stage are appeared in Figure 1.

3.1 Embedding Phase:

The encoded secret message is embedded in video frames during this stage, using the Random Number Generator and LSB reverse method. Here, the video is broken down into frames and regenerated into a series of images. The frames used as s cover are then chosen randomly using a random number generator. The reverse LSB technique is then used to cover the encrypted and compressed message within the frame chosen. This method was applied to the picture set until the secret message was executed. Then, the image set was regenerated to the frames. Finally, the video frames are built in to trigger stego video.

.

The steps of getting ready the secret message is surveyed as:
Input : Confidential message
Output: Compressed confidential message
Step 1 : Get the Confidential message

ISSN: 2005-4238 IJAST

Step 2 : Select two different random prime numbers a and b.
Step 3 : Compute n=ab.
Step 4: Compute N=(a-1) (b-1).
Step 5 : Select a value for d that is relatively prime to N.
Step 6: Calculate e using the formula e*d=1modN
Step 7: For encoding use p^e mod n.
Step 8: For decoding use c^d mod n.

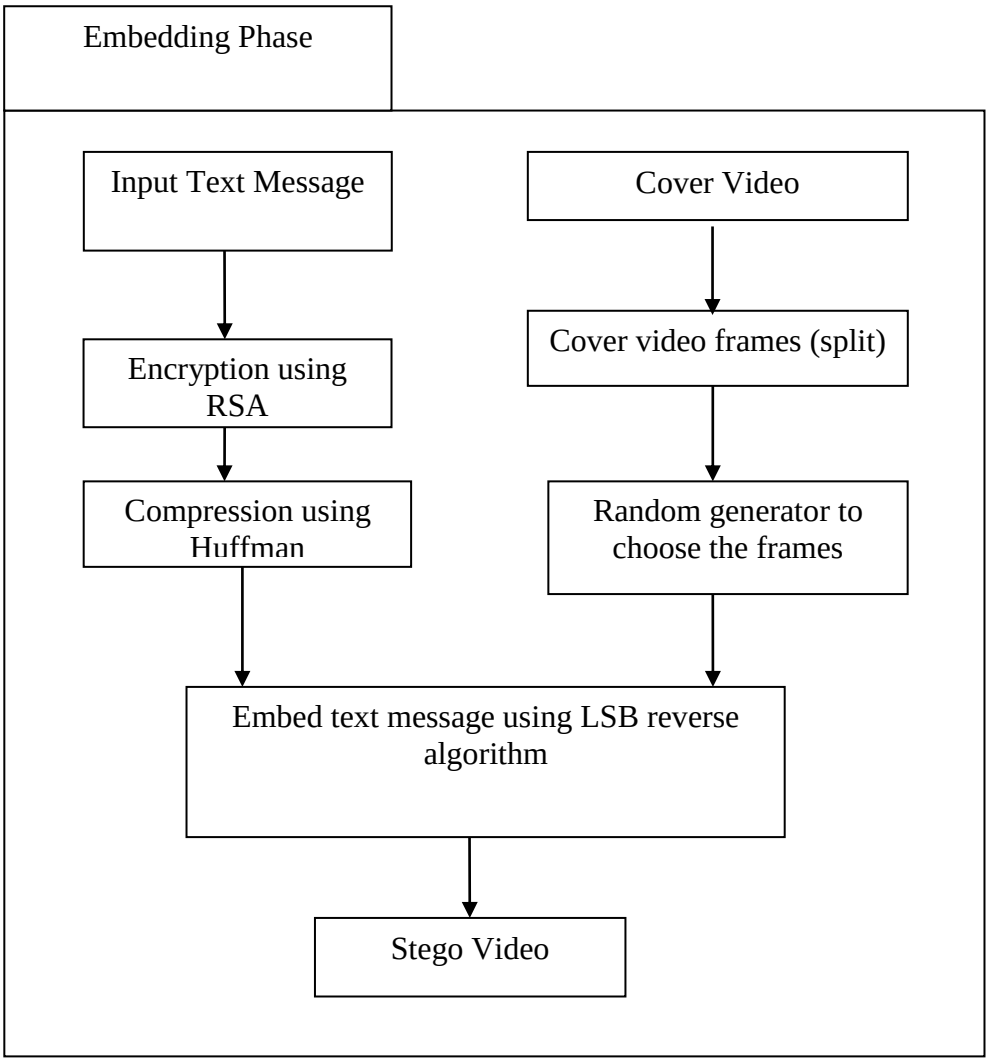

Figure 1. Embedding Phase

Lossless compression of the Huffman calculation is simple to execute. It may be a variable code word length. The concept behind the calculation is to form the tree bottom-up approach whose leaves are labeled with the weights.

Step 9 : Huffman algorithm is administrated by encrypted information that includes the many steps:
Step 9.1: Explore for the two hubs having the slightest frequency, which are not yet assigned to a parent hub
Step 9.2: Couple these hubs along to a substitution insides hub
Step 9.3: Add each the frequencies and assign this value to the new interior node
Step 9.4: The procedure has to be repeated until all nodes are combined together in a

ISSN: 2005-4238 IJAST

root node

Step 10 : After that Huffman process is completed, the binary input is an output

Step 11: Audio Video Interleave (AVI) is utilized as a hiding place for concealment of the mystery data. The cover video file is decomposed into the number of frames

Step 12: To pick out the frames, pseudo random number generator is utilized. Seed ought to be changed between the sender and receiver. The seed are found out based on the primary two prime variables and the sum of these two prime variables gives the primary frame number where the mystery information is covered up. At that point, the next two continuous frames, the same secret data is hidden. This procedure is repetitive three times within the frames at a balanced of the entirety of the prime components.

Step 13: LSB reverse method is used to hide a secret message. The text data is converted into a single row of binary bits in step 9. The frame in which the message is to be hidden is split into blocks in such a way that, every block consists of four pixels. Each pixel in a block is given a grey code cluster 00, 01, 11, 10 respectively. According to this algorithm, two bits are hidden in a block containing four pixels. In a block, the pixel, whose grey code cluster matches with the two bits of the message, is chosen and its LSB is reversed. The LSB of the remaining three pixels of the block is reversed to the opposite bit of the chosen pixel's LSB. This process is continued for second and third LSB's positions until all the message bits are embedded within the specific video frames.

After the embedding process, the frames are integrated into a single video called stego video and it is sent to the receiver.

3.2 Extraction Phase:

The different steps utilized within the extraction stage are appeared in Fig. 2.
Input : Stego Video
Output : Secret message

Step 1 : Open the stego video, the stego video file is split into individual frames.

Step 2 : Convert the video frames into images; determine the chosen frame using a Pseudo-Random Number Generator.

Step 3: LSB reverse method used to recover a secret message. The chosen frames are grouped into blocks in such a way that each block consists of four pixels. Now the LSB of each pixel in a block is extracted and each of them is given a grey code cluster 00, 01, 11, 10 respectively. The odd bit among those four pixels is pointed out. The message bits equal the grey code cluster of the odd bit. Now the binary bits are extracted from the first, second, and third LSB's positions.

Step 4 : Binary data is decompressed by using the Huffman algorithm

Step 5 : Decompressed data again decrypted using the RSA algorithm, finally get the secret message

4. Results

As explained in Figure 3 below, the suggested methodology uses videos of different sizes as a dataset for evaluation. The methods performance was evaluated and compared on the basis of the following measures:

- Mean Squared Error (MSE)
- Peak Signal to Noise Ratio (PSNR)

ROBUSTNESS:

ISSN: 2005-4238 IJAST

Robustness determines the system's ability to withstand diverse attacks. The quality of the system established is clearly specified in it. The accuracy of the original video is therefore contrasted with that of the stego video. Mean Squared Error (MSE) is the parameter used to describe device robustness efficiency. MSE is the Mean Squared Error that defines the inconsistency between the original video and the stego video.
MSE is calculated using equation 1:

$$MSE= (1/m*n)\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j)-K(i,j)]^2 \quad \text{------ (1)}$$

Where, m * n speak to the dimension of the video frame, while I(i,j) and K (i,j) indicate the estimation of the pixel before and after the data implanting interior the video frame.

PSNR is characterized as the video as the video quality by comparing the original video to the video in the stego. The unit used for PSNR measurements is decibels (dB). The higher the PSNR value, the greater the video quality. PSNR is determined by means of equation 2:

$$PSNR=20*\log10 (MAX_i)-10*\log10(MSE) \quad \text{------ (2)}$$

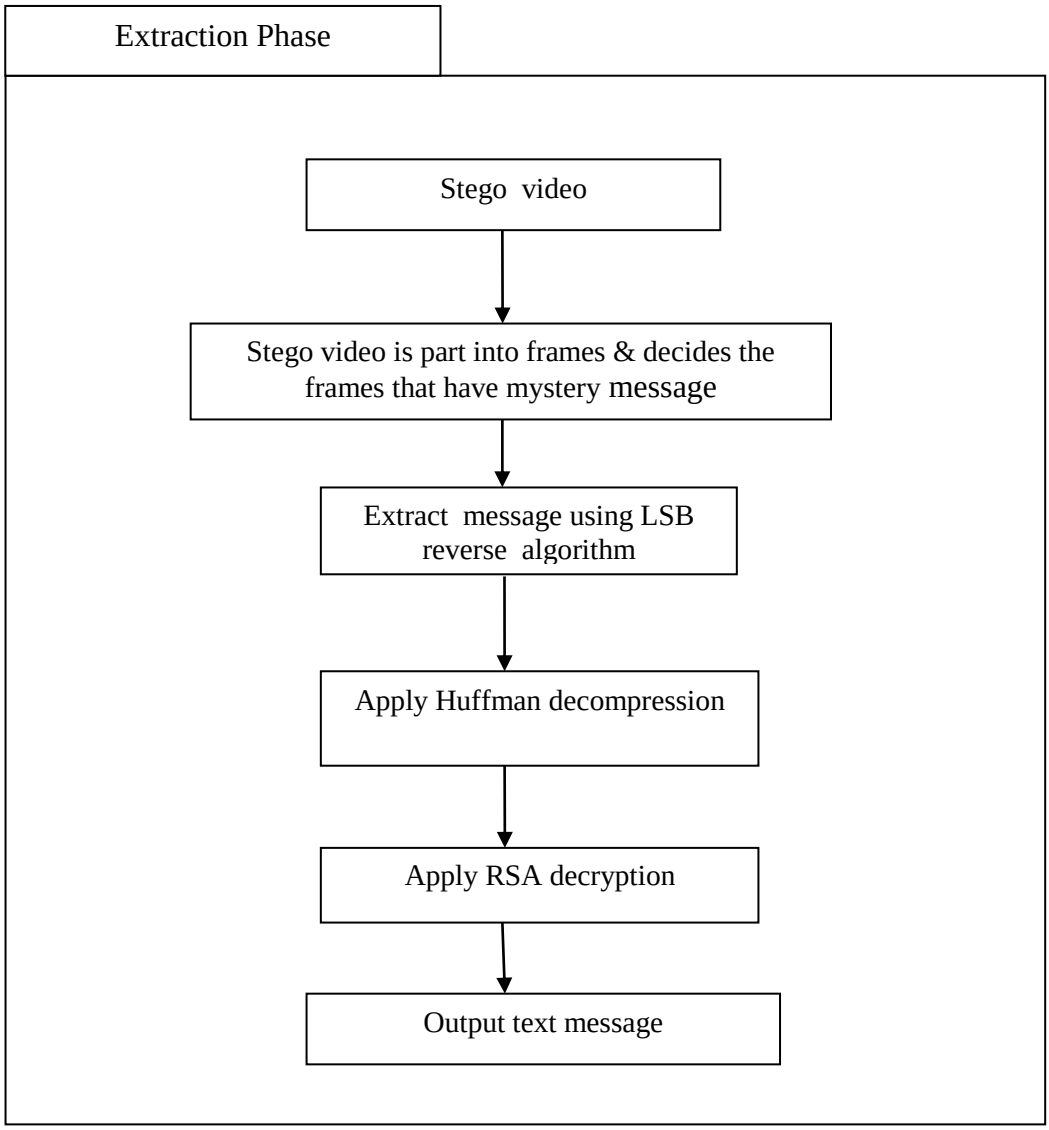

Figure 2. Extraction Phase

ISSN: 2005-4238 IJAST

Newsreader.avi	Coastguard.avi	Rhinos.avi

Figure 3: Test videos dataset utilized for assessing the proposed method

Table 1 demonstrates the results of embedding a disparate size of secret message in the different sizes of cover video used to assess the proposed method
.

Table 1: The Exploratory Outcomes of the Proposed strategy

Test video dataset	Estimate of outline in video	Capacity	MSE	PSNR
Newsreader.avi	512*512	48000	0.0098	65.2185
Coastgurad.avi	512*512	48000	0.0102	62.0448
Rhinos.avi	512*512	48000	0.0199	61.1423

From the above Table, note that the PSNR estimate is high while the MSE estimate is low when 48,000 characters are embedded inside videos with a frame size of 512 * 512. PSNR results are still high, as well as the MSE value is still low, meaning that the original videos are closer to the stego videos. The same size of the video frame and number of characters are used for assessing or checking the new method and the old methods, namely, the Sahu and Mitra method and the Zeyad method. Table 2 shows the contrast between the proposed method and the Sahu and Mitra method and the Zeyad method using a video frame size of 256 * 256 and the 3000 character payload used to embed the video within. The experimental results show that in all videos used for comparison the PSNR and MSE values for the proposed method are better than the previous method

By comparing , PSNR values against the embedding capacity of 3000 characters, in the Figure 4, the proposed method is better than the existing methods. For the "Newsreader.avi" frame with the payload of 3000 characters, the obtained PSNR is 73.21.This value is better to that of the Sahu and Zeyad methods whose PSNR values are 66.52 and 63.19 respectively. The proposed method earns better PSNR in all the cases.

Table 2: The Experimental Results of the proposed approach with the existing approach

Approaches	Test video dataset	Video frame (Size)	No.of characters	MSE	PSNR
Proposed Method	Newsreader.avi	256*256	3000	0.1798	73.2185

ISSN: 2005-4238 IJAST

Zeyad et.al., method				0.2843	66.52
Sahu et.al., method				0.6991	63.1972
Proposed Method	Coastguard.avi	256*256	3000	0.1567	71.654
Zeyad et.al., method				0.2753	67.4661
Sahu et.al., method				0.6371	63.2714
Proposed Method	Rhinos.avi	256*256	3000	0.1325	69.1248
Zeyad et.al., method				0.2140	68.0999
Sahu et.al., method				0.5428	65.4914

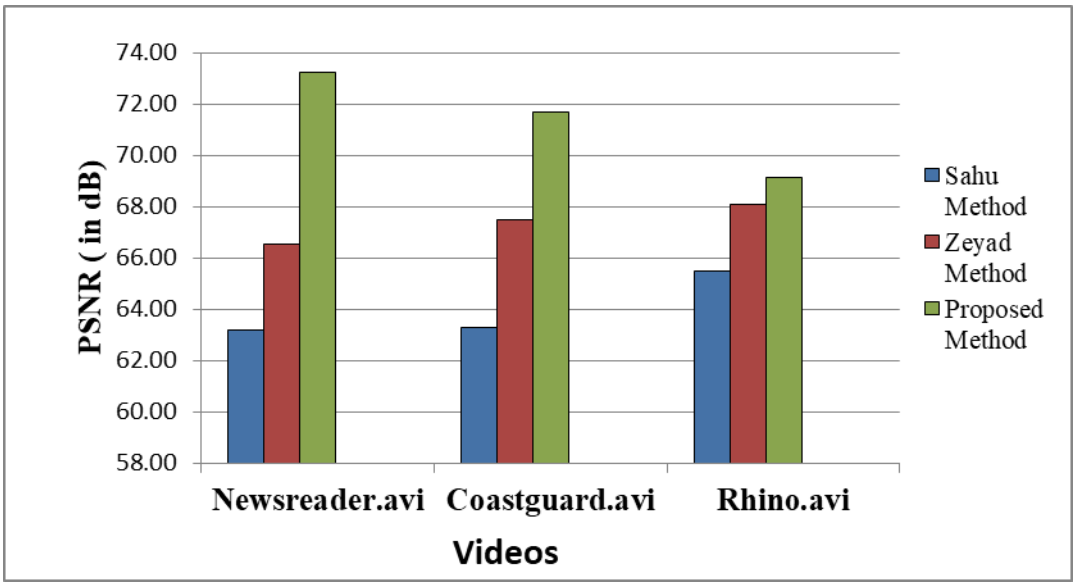

Figure 4: PSNR Values for various videos

ISSN: 2005-4238 IJAST

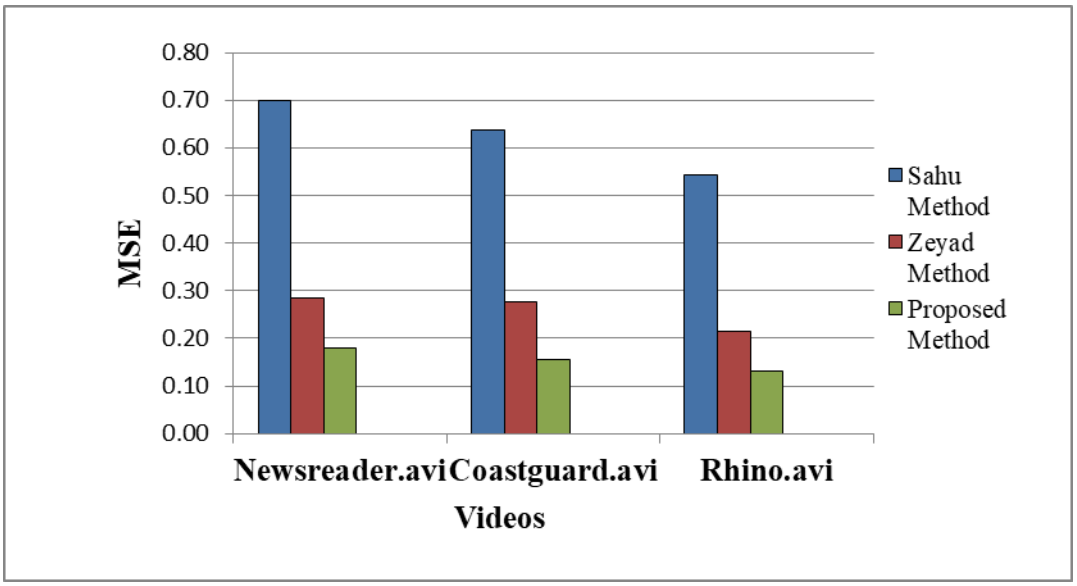

Figure 5: MSE Values for various videos

A comparative analysis of the proposed method with the existing methods video steganography strategy has been done on the premise of the parameter MSE for various videos by embedding the 3000 characters inserted as shown in Figure 5. A lower value for MSE implies minor errors. From Figure 5, it is confirmed that the MSE value of the proposed method is decreased by 39% than Zeyad method, by 75% than Sahu method.

5. Conclusion

In this paper we have proposed an effective video steganography technique by mixing RSA cryptographic algorithm, Huffman code compression with LSB reverse. The RSA encryption is preferred to give enough security for the huge size video file and reduces the complexity of final video message. The outcome of this proposal is revealed that when video steganography is combined with cryptography and compression, the level of safety and efficiency is enhanced with robustness at the higher end. The distortion is negligible; thus, the high PSNR values and low MSE values have improved data protection through this analysis.

References

[1] N. Johnson, Z. Duric, S. Jajodia, "Information hiding, and watermarking- attacks countermeasures", in: Advances in Information Security, **(2001)**.

[2] F.K. Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata", Int. J. Eng. Sci. Technol, vol.17, **(2014),** pp. 85–94.

[3] C. Karri, U. Jena, "Fast vector quantization using a Bat algorithm for image Compression", Int. J. Eng. Sci. Technol.**(2015).**

[4] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding", IBM Syst. Journal, vol.35, **(1984)** ,pp. 313–336.

[5] Dengre , A. R., Gawande, A. D. Deshmukh, , A. B., "Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 2, no.6, **(2017)**,pp. 2319 – 4847.

[6] S.A. Abbas, T.I.ElArif, F.F.Ghaleb and S.M.Khamis, "Optimized video steganography using Cuckoo search algorithm", in IEEE Seventh International Conference on Intelligent Computing and Information Systems**,(2015)**, Doi: 10.1109/IntelCIS.2015.7397279.

[7] K.Rajalakshmi, K.Mahesh ," Video steganography based on embedding the video using PCF technique", International conference on Information Communication and Embedded Systems, **(2017)**, pp.1-4.

[8] Yadav P, Mishra N, Sharma S, "A secure video steganography with Encryption based on LSB technique", IEEE International Conference on Computational Intelligence and Computing Research, **(2013)**.

[9] U.Sahu and S.Mitra, "A secure data hiding technique using video stegnography", Int,J.Comput.Sci.Commun.Netw, vol.5, **(2015)**, pp. 348-357.

ISSN: 2005-4238 IJAST

[10] Rahul Paul et.al. , " Hiding Large Amount of Data Using a New Approach of Video Steganography", Confluence 2013: First International Conference on Information Technology, Communications and Computing , **(2017).**
[11] P. Sethi and V. Kapoor, "A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography", Int. Conf. Comput. Sci, vol. 87, **(2016)** , pp.61–66.
[12] A.Saleema and T.Amarunnishad, "A new steganography algorithm using hybrid fuzzy neural networks", in International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST-2015), vol.24, **(2016)** ,pp.1566-1574.
[13] Z. S. Y. Alsaffawi, "Image steganography by using exploiting modification direction and knight tour algorithm", J. Al-Qadisiyah Comput. Sci. Math. (QJCM),vol. 8, **(2016)**,pp.1–11.
[14] Ashish T. Bole, Rachna Patel, "Steganography over Video File using Random Byte Hiding and LSB Technique", International Conference on Computational Intelligence and Computing Research, IEEE, **(2012)**.
[15] A. Solichin and Painem, "Motion-based less significant frame for improving LSB-based video steganography", in: *IEEE International Seminar on Application for Technology of Information and Communication (ISemantic)*, **(2016)**, doi: 10.1109/ISEMANTIC. 2016.7873834.
[16] K.Rezagholipour and M.Eshghi, "Video steganography algorithm based on motion vector of moving object", in: IEEE Eighth International Conference on Information and Knowledge Technology, **(2016),** doi:10.1109/IKT.2016.7777764.
[17] A.Putu, M.Gusti and M.Ni, "A MP4 video steganography using least significant bit(LSB) substitution and advanced encryption standard", J,Theor.appln.Inform.Technol,vol. 95, **(2017)**, pp.5805-5814.
[18] S.Mumthas and A.Lijiya, "Transform domain video steganography using RSA, random DNA encryption and Huffman encoding", in 7th international conference on Advances in Computing and Communications, 115, **(2017)**, pp.660-666.
[19] Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar, "Enhance security in steganography with cryptography", vol. 3, no.3, **(2014).**
[20] S.Dhaarani., R.Shanthakumari.," A Reversible Approach for Information Hiding in Dual Images", CiiT Journal on Digital Image Processing, vol.8,no.1,**(2016)**,pp.1-6.
[21] R.Shanthakumari., "A spatial Domain-based Image in Image hiding scheme using Particle swarm optimization", International Journal of Recent Trends in Engineering and Research, vol. 2, no. 7, **(2016)**.
[22] R.Shanthakumari., S.Malliga., S.Dheepika, " Secure data hiding in images", International Journal of Advanced Research Trends in engineering and Technology, vol. 2, no. 8, **(2015)**, pp.144-148.
[23] R.Shanthakumari., Dr.S.Malliga.," Information Hiding in Digital Images using Modified LSB substitution with Multi-pixel Differencing and HL code", Asian Journal of Research in Social Sciences and Humanities, vol 7, no.1, **(2017)**, pp.198-207
[24] Shanthakumari, R and Malliga, S "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm",International Journal of Multimedia Tools and Applications, vol. 79, no.5, **(2020)**, pp. 3975-3991.
[25] R.Shanthakumari, Dr.S.Malliga., "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment ", Sadhana-Academy Proceedings in Engineering Sciences, vol. 44, no.5, **(2019),** pp. 1-12.
[26] R.Shanthakumari., S.Malliga., S.Dheepika., "Data Hiding Scheme in Spatial Domain", International Journal of Computer Science Engineering and Technology, vol.4,no.12, **(2014)** , pp.400-403.
[27] R.Shanthakumari, Dr.S.Malliga.," Digital Image-in-Image Watermarking For Copyright Protection of Images Using the Slant Transform ", International Journal of WSEAS Transactions on Computers, vol. 16, **(2017)**.
[28] S.Parvathavarthini., R.Shanthakumari., "An adaptive watermarking process In Hadamard Transform", International Journal of Advanced Information Technology, vol. 4, no. 2,(**2014)**.
[29] R.Shanthakumari., Dr.S.Malliga., "Data Hiding in Image Using Tree-Based Parity Check with LSB Matching Revisited Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 6, **(2015)**, pp. 5472 – 5479.
[30] Manpreet Kaur, Amandeep Kaur, "Improved security mechanism of text in video using steganographic technique", International journal of advance research in computer science and management studies, vol.2, no10, **(2014)**.
[31] Kaur, R. and Singh, T,"Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography", International Journal of Computer Applications,vol.117,no.18,**(2018)**.
[32] Prajna Vasudev,Kumar Saurabh, " Video steganography using 32*32 vector quantization of DCT", International Journal of Software & Hardware Research in Engineering, vol. 1,no.3, **(2013)**.
[33] Zeyad Safaa Younus and Ghada Thanoon Younus, " Video steganography using Knight tour algorithm and LSB method for encrypted data, J.Intell.Syst.vol29,no.1, **(2020),** pp.1216-1225

Authors

ISSN: 2005-4238 IJAST

	**Dr. R. Shanthakumari is** working as an Assistant Professor (SLG) in the Department of Information Technology, Kongu Engineering College, Tamil Nadu, India. She has completed Ph.D, in 2020 from Anna University Chennai. Her main research area is Networks, Network Security and Digital Image Processing. She has guided many UG and PG projects. She has published 21 articles in international journals and presented more than 25 papers in national and international conferences in her research and other technical areas.
	**Mr.S.Vinothkumar** is currently working as an Assistant Professor in the Information Technology department of Kongu Engineering College. His main research area is Network Security and Block chain Tehnology. He has guided many UG and PG projects. He has published 5 articles in international journals and presented more than 5 papers in national and international conferences in her research and other technical areas.
	S. Kannimuthu is currently working as an Associate Professor at Karpagam College of Engineering, Coimbatore, Tamil Nadu, India. He is also an In-Charge for the Center of Excellence in Algorithms. He did PhD in Computer Science and Engineering at Anna University, Chennai.
	**Santhya G** is currently pursuing M.Tech Information Technology at Kongu Engineering College, Tamil Nadu, India. Her area of interest is Network Security.
	**Bharaneeshwar B** is currently pursuing third year of B. Tech in Information Technology at Kongu Engineering College, Erode. He is divergent towards finding a solution to the problem statement that is provided and is keen on his research works. His area of interest is Network Security.

ISSN: 2005-4238 IJAST