

Secured Medical Data Transfer Using Reverse Data Hiding System Through Steganography

S. Aiswarya* and R. Gomathi

Department of Electronics and Communication Engineering, University College of Engineering, Dindigul, 624709, Tamilnadu, India

*Corresponding Author: S. Aiswarya. Email: aaiswaryas2020@gmail.com

Received: 25 November 2021; Accepted: 30 December 2021

Abstract: Reversible Data Hiding (RDH) is the process of transferring secret data hidden inside cover media to the recipient so the recipient can securely retrieve both the secret data and cover media. The RDH approach is applied in this study in the field of telemedicine, and medical-secret data is conveyed privately via medical cover video. Morse code-based data encryption technique tends to encrypt the medical-secret data by compression using the Arithmetic coding technique. Discrete Shearlet transform (DST) compresses the selected frame from the medical cover video and the compressed secret data is embedded into the compressed frame using logical operations. On a receiver side, the reversal process is carried over and the original cover frame will be retrieved from the stego frame after secret medical data is retrieved. Password is included on the receiver side for authentication purposes. Parameters such as encryption time, compression ratio, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are calculated and at the maximum iteration of the proposed algorithm, the highest PSNR value is achieved. In terms of Structural Similarity Index Measure (SSIM), a linear increase from 0.91 to 0.99 is evident for iterations. In comparison with other techniques, the proposed algorithm reaches a higher SSIM of 0.999 after the maximum number of iterations. Thus, the proposed method provides more security and authentication to the recipient.

Keywords: Morse code; discrete shearlet transform (DST); reversible data hiding (RDH); steganography

1 Introduction

In the prior decades, sending secret data communication between one point to another was very difficult. During the world wars, special ink was used to transmit secret data because the transmission of secret data is crucial. For these kinds of secrecy, data hiding techniques are the better solutions. Cryptography, Steganography and watermarking are well-known data hiding techniques [1].

Cryptography is the process of changing information into an unreadable form. Steganography [2] is the process of embedding the data into the cover file that is no one knows the presence of data. Watermarking is used to protect the ownership of data. Public key cryptography and private key cryptography are the



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

classifications of cryptography and Advanced encryption standard (AES), Data Encryption Standard (DES) [3], Rivest–Shamir–Adleman (RSA) [4], Blowfish are some examples of cryptography techniques.

The data encryption approaches and lossless compression strategies were investigated by Singh et al. [5]. Encryption had been developed to secure confidential information. Cryptography approaches such as public key and private key techniques hold a major part of this work. Data compression is used to reduce the size of secret data by removing redundant bits.

Steganography [6] is classified based on cover medium and text, image [7], audio and video can be used as a cover file. Video Steganography [8] is a mostly used technique because of its large capacity for hiding data.

In video steganography, initially, the video is fragmented into many frames. With spatial domain steganography, the confidential data generates a sudden change in pixel intensity [9]. Least Significant Bit (LSB) [10,11], Pixel Value Differencing method (PVD) are some examples of spatial domain techniques. In the transform domain or frequency domain technique, the frame is modified by the respective transforms. After that, transform coefficients are used for data hiding by using spatial domain techniques. Discrete Cosine Transform (DCT) [12,13], Discrete Wavelet Transform (DWT) [14], Integer Wavelet Transform (IWT) [15] are examples of transforms that will be used to alter the frames. The combination of cryptography and steganography techniques provides more protection for secret data. Data hiding techniques are widely used in the field of Military, Banking, Telemedicine [16], etc.,

Lakshmanan et al. proposed a method of reversible data hiding in medical images by using a histogram modification technique in which pixel differences are calculated between adjacent pixels to hide the secret data [17]. In this paper, there is no encryption technology to provide security for the secret data and lacks authentication techniques to provide safety for medical data.

Nipanikar et al. [18] proposed a technique in which the secret data was converted to American Standard Code for Information Interchange (ASCII) code and binary then embedded into the medical image. In this paper, the features of entropy, edge and intensity help find the pixels in the image and DWT is used for hiding the secret data. However, it was not a secured one for secret data transmission because there was no encryption technique.

In the year 2017 [19], Vinita et al. proposed an algorithm to divide the secret text into sub-blocks up to a single bit in a block. Video is converted into frames and then DWT and DCT transforms were implemented for frames. Now, the bits are embedded into the DCT transformed frame. However, this proposed method is not robust to attackers and not able to provide authenticity.

In the year 2020 [20], Sari et al. established a technique for encrypting the data using AES and Huffman code for compressing the data. Image is used for data embedding and secure data transmission. This proposed method provides security to the data by using AES for encryption. The main drawback is the key value is not properly maintained; the secret data is affected by the cryptanalytic attack.

In the year 2021, Wahab et al. introduce a technique of encrypting the data using the RSA algorithm then encrypting the encrypted data using Huffman coding. The cover image is compressed using DWT transform then the compressed data is embedded using the LSB technique. This technique provides a better-quality image and provides high security. But the key calculation process is complex and time-consuming.

In the proposed method, medical secret data is securely transmitted using medical cover video. In the medical field, all particulars of patients should be kept secret and transmitted from one point to another should be more secure. In a proposed method, a reversible data hiding technique is used that is the receiver can retrieve the original cover frame and also the original secret data without any loss [21].

In the proposed method, Morse code-based encryption technique is used to avoid formal cryptographic techniques and protect from cryptographic attacks. Additionally, to reduce the number of bits lossless compression [22] that is arithmetic coding compression technique is used. Compressed secret data is

embedded into the video using the Steganography method. Cover medical video is nothing but the scanning video of the corresponding patient. Video is converted to frames and the cover frame is compressed [23] using Shearlet transform. A compressed frame is used for data embedding. Logical operations are used to embed the secret data into the cover medium.

On the receiver side, the reversal process is carried over. Secret data is obtained from the compressed stego frame and the original cover frame is also retrieved from the compressed frame. The original cover video is returned to the receiver. Additionally, the password is also included for the authentication of the recipient. The distortion between the original image and the stereographic image was evaluated using MSE and PSNR values.

The flow of the manuscript is as follows: Section 2 describes the shearlet transform. Section 3 presents the description of the proposed methodology. In Section 4, the results are discussed and compared with the prior art methods and finally, Section 5 comprises the conclusion of the study.

2 Shearlet Transform

Shearlets are a multiscale framework and allow encoding of anisotropic features in multivariate problem classes [24]. Shearlets are used for the highly efficient representation of images with edges. It is mainly used in the field of image enhancement, image denoising, edge detection and analysis and image compression. Shearlets are designed for the analysis and sparse approximation of functions $f \in L^2(\mathbb{R}^2)$. For $\psi \in L^2(\mathbb{R}^2)$, the continuous shearlet system is generated by ψ and is then defined as

$$SH_{cont}(\psi) = \left\{ \psi_{a,s,t} = a^{\frac{3}{4}} \psi(S_s A_a(\cdot - t)) \mid a > 0, s \in \mathbb{R}, t \in \mathbb{R}^2 \right\} \quad (1)$$

The corresponding continuous shearlet transform is given by the map

$$f \mapsto SH_{\psi} f(a, s, t) = \langle f, \psi_{a,s,t} \rangle, f \in L^2(\mathbb{R}^2), (a, s, t) \in \mathbb{R}_{>0} \times \mathbb{R} \times \mathbb{R}^2 \quad (2)$$

A discrete version of shearlet systems can be directly obtained from $SH_{cont}(\psi)$ by discretizing the parameter set

$$\mathbb{R}_{>0} \times \mathbb{R} \times \mathbb{R}^2 \left\{ \left(2^j, k, A_{2^j}^{-1} S_k^{-1} m \right) \mid j \in \mathbb{Z}, k \in \mathbb{Z}, m \in \mathbb{Z}^2 \right\} \subseteq \mathbb{R}_{>0} \times \mathbb{R} \times \mathbb{R}^2 \quad (3)$$

Shearlet generator ψ is defined by,

$$SH(\psi) = \left\{ \psi_{j,k,m} = 2^{\frac{3j}{4}} \psi(S_k A_{2^j} \cdot -m) \right\}_{j \in \mathbb{Z}, k \in \mathbb{Z}, m \in \mathbb{Z}^2} \quad (4)$$

Discrete Shearlet Transform is defined by,

$$f \mapsto SH_{\psi} f(j, k, m) = \langle f, \psi_{j,k,m} \rangle, f \in L^2(\mathbb{R}^2), (j, k, m) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^2 \quad (5)$$

Fig. 1 shows the shearlet transform's frame property. The shearlet domain is a robust method for image compression. Due to the superior performance of the Discrete Shearlet Transform (DST) over the Discrete Wavelet Transform (DWT) in encoding directional information, a DST-based compression algorithm is employed that provides not only a better image approximation and compression ratio, but also increases the security of images using the Advanced Encryption Standard.

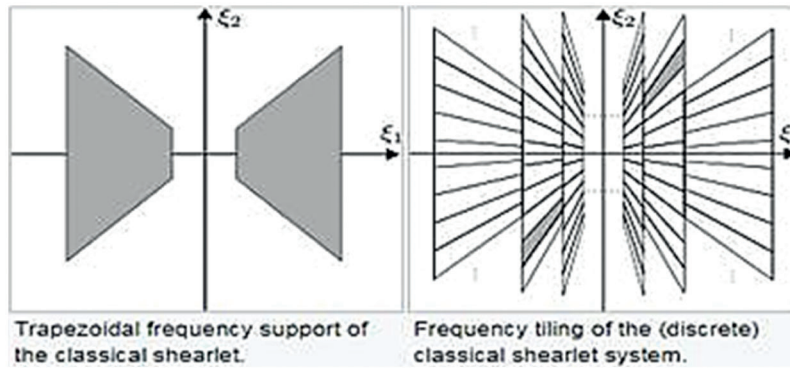


Figure 1: Discrete shearlet transform

3 Proposed Methodology

In Reversible Data Hiding (RDH) method is used for secured medical data transmission and reception using the compressed frame of medical cover video. Medical secret data such as patient’s name, ID, disease name is securely transmitted using the patient’s medical scan video. Medical secret data is encrypted using Morse code and the encrypted text is converted into binary values. The arithmetic coding method is used to compress the encrypted data. At the same time, medical cover video is converted into frames and the cover frame is selected. Discrete Shearlet Transform (DST) is used to compress the selected frame. In the compressed frame, compressed secret data is embedded using logical AND, OR functions and the resulting frame is known as the stego frame. Stego frame is placed in a corresponding place to create the stego video which is transmitted to the recipient. On the recipient side, the authorized receiver must enter the password. If the password is correct, the reversal process is carried on otherwise it shows an error. Stego frame is selected and the reversal logical operations are carried out to get the compressed secret data and the compressed cover frame. Finally, the secret medical data is retrieved after the reversal of arithmetic coding and Morse code operation and also by using the Inverse Shearlet transform, the original cover frame is retrieved. [Fig. 2](#) shows the flow chart of the proposed methodology on a transmitter side.

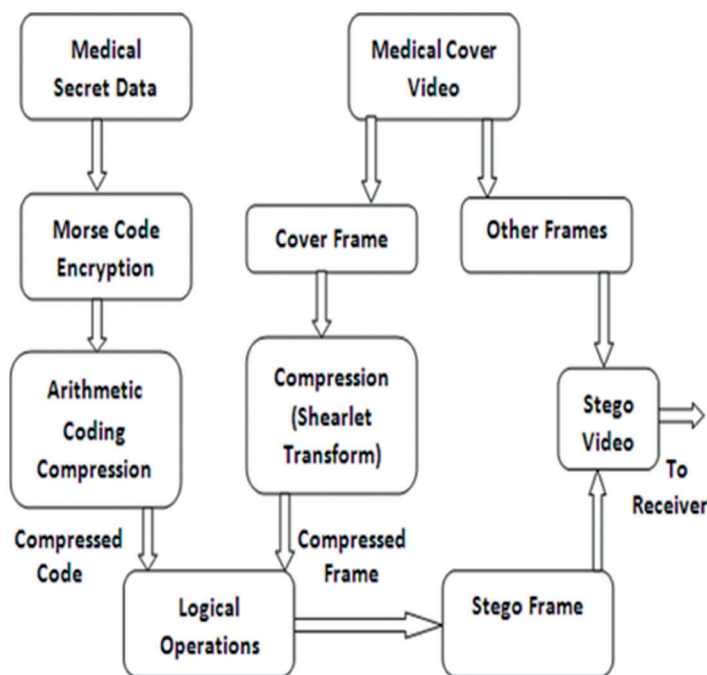


Figure 2: Proposed methodology

3.1 Data Encryption and Compression

In the proposed work, the secret data is compared with the predefined dataset and the Morse code is generated. For security purposes, the Morse code is converted to ASCII and then to binary values. So, the unauthorized person does not know what technique is used for encryption.

3.1.1 Morse Code

Morse code is a sequence of symbols that is used to represent the characters and numbers. Dots and dashes are used to represent the character. Frequently used character has a smaller number of symbols and less frequent symbol has more number symbols. It is most widely used in telecommunication for secret data communication. It converts the secret data into unreadable and undetectable symbols. Time consumption for conversion of data is less compared to cryptographic techniques. The following algorithm explains the encryption of secret data using Morse code.

Algorithm

Enter the secret data

Start

For i=1: length of secret data

{

For j=1: length of the dataset

{

i==j

Display j

}

}

Display Morse code

Converted to ASCII code

Display ASCII code

Converted to Binary Values

Display Binary values

End

3.1.2 Arithmetic Coding

Arithmetic coding is known as the entropy-based lossless compression technique. The reason for compressing is to shrink the redundancy values in the given data. Arithmetic coding converts the data into binary values and depending on the probability of occurrence of the data, the outcoming binary values change. Mostly used character is assigned with less number of bits and less probable character has more number of bits. It reduces the computation process because a fewer number of bits is used to define characters. Arithmetic coding is more flexible than Huffman coding because the major advantage of arithmetic coding is that it works well with data compression and can accept both integer and non-integer bit numbers. So, it is superior to Huffman coding. Arithmetic coding is used in image compression also.

Encrypted secret medical data is a sequence of binary values. These values are given to the arithmetic coding compression technique and this technique converts the equivalent binary values to the '0' and '1'. This compression enhances the security level for the secret data.

3.2 Preprocessing of Medical Cover Video

For preprocessing, a patient's medical three plane scan video is chosen as a cover medium. At first, the cover video is converted into frames. Depending on the video size, the total number of frames will vary. Among the number of frames, a single frame will be selected for compression.

3.3 Image Compression

Image compression is used to minimize the size of the image by removing redundant values. Compression of medical images is a challenging task [25]. DST is used for image compression. Shearlet transform is the extension of the wavelet transform. Compared to wavelet transform, it provides better performance metrics. Shearlet transform is anisotropic and it represents the edges of the image efficiently. Compared to wavelet transform, DST provides the best image representation especially edges.

Algorithm

Enter the image

While (1)

{

Take Shearlet Transform

Calculate redundant pixels

If (true)

{

Compress the image

}

Display compressed image

}

3.4 Data Embedding

The compressed secret medical data which is obtained after arithmetic coding is embedded into the compressed selected frame using logical operations. From the three-plane compressed image, R, G, B plane pixel value is calculated from the first pixel to the length of the secret data. Based on the secret data value, the R, G, B pixel value is altered and again stored in the image. The outcome image is known as the stego image. The algorithm for embedding data into a compressed medical video frame is as follows.

Step 1: Pixel values of the compressed frame are extracted for three planes.

Step 2: Binary values of secret data are calculated by using Morse code followed by the Arithmetic coding in the data encryption phase. For example, Secret text is 'e'; its compressed binary value is 01100010.

Step 3: Binary value is divided into sub-blocks for red(R), green (G) and blue (B) plane values. For example, the first three bits belong to the red value, next three bits belong to the green value and the last two bits for the blue value.

Step 4: Binary values are logically bitting ANDed with their position and if the result is bit position, then the corresponding plane value is increased.

Step 5: Update automatically the red, green and blue values and the new values are saved as new pixel values. From the above example, R, G and B plane values are updated as 171, 168 and 173 correspondingly.

Step 6: Step 1 to step 5 are repeated until all secret text is embedded in the frame as a pixel value. The secret text embedded image is known as a stego image.

The above logical operations such as AND, OR, XOR provides more security to the secret data compared to other data embedding techniques such as LSB, PVD methods. In the LSB method, the least bit value is changed and retrieval of the original pixel value is not possible. PVD is similar to the LSB method. In the projected technique, the original image can retrieve from the stego image. MSE and PSNR values are calculated between the original frame and the stego frame.

3.5 Reconstruction Process

On the receiver side, the reversal process is carried over to get the original secret data and the original cover frame. First of all, the receiver should enter the password to identify the authenticity of the receiver. If the password is correct then only the following operation is carried over otherwise the program will break. From the stego video, the stego frame is selected and the compressed secret data is retrieved by using reversal logical operations. At the same time, the compressed cover frame is also received from the reversal data hiding process. Using Inverse Shearlet Transform (IST), the original cover frame is retrieved. The compressed secret data is given to inverse arithmetic coding operation and then it is converted to Morse code. Finally, the medical secret data is securely predicted. Based on the RDH technique, secret data and the cover frame are retrieved. Fig. 3 shows the flow chart of the reversal process.

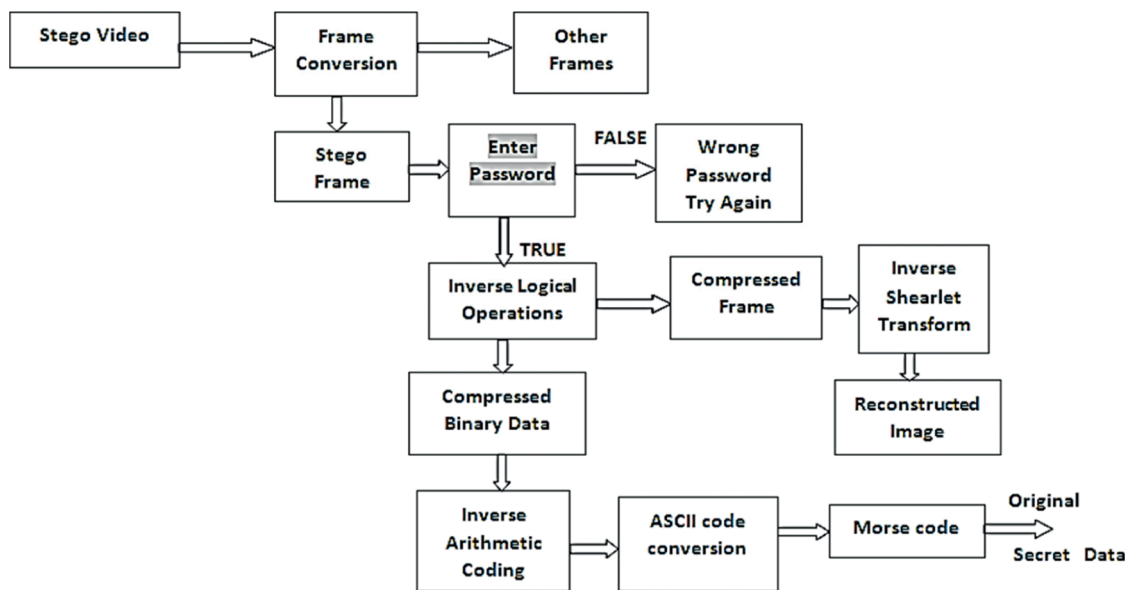


Figure 3: Flow chart of reversible data hiding

4 Results and Discussions

In the proposed method, Morse code is used to encrypt the secret medical data and arithmetic coding is used to compress the encrypted secret data. The Discrete Shearlet Transform (DST) is used to compress the selected frame from the medical video. Logical operations are used to implant the compressed secret data into

the compressed cover frame. On the receiver side, the reversal process is performed and the medical secret data and the original cover frame are retrieved successfully. MATLAB-R 2012a software is used with Windows 7 Operating System and Intel core processor with 4GB RAM (Random access memory). The source of the medical cover video is Dicom medical video from Google. The proposed algorithm can able to process any color medical video or any other videos with different sizes.

4.1 Data Encryption

Secret medical data is securely encrypted using two processes such as Morse code encryption followed by arithmetic coding compression. Fig. 4 shows an example that the sample medical secret data and compressed binary secret data and computational time. This requires minimum computational time. For the given example, 53-byte data requires 0.464085 seconds for this data encryption.

```

Medical Secret Data:
Enter Characters to Encode
NAME SWETHA ID 7659821 ILLNESS CORONARY HEART DISEASE
'N'
'-'
Compressed Binary code and Computational Time:
101101101110101100101110101101101100101101101101100:
Compressed data =0111010111111001110001101110011101001
Elapsed time is 0.464085 seconds.
    
```

Figure 4: Morse code & compressed binary data with computational time for given medical secret data

Depending on the length of the secret data, the encoding time will vary. The following Fig. 5 indicates the variations of encoding time vs. several bits. If the number of bits increases then the encoding time also increases.

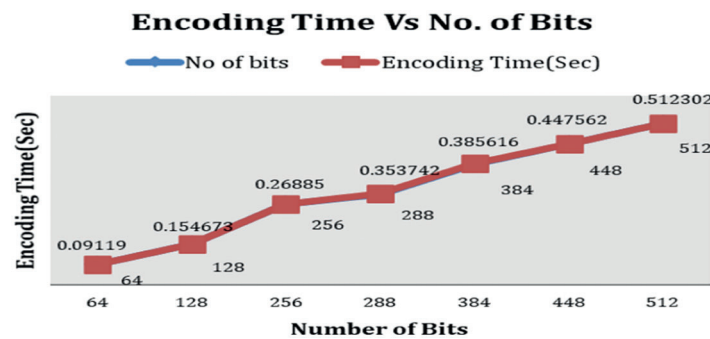


Figure 5: Graph of the number of bits vs. encoding time

4.2 Preprocessing

In preprocessing, medical cover video is converted into several frames. Among a different number of frames, a single frame is selected for compressing and to hide the compressed binary data.

4.3 Compression of Selected Cover Frame

Discrete Shearlet transform (DST) is used for cover frame compression. The performance is evaluated by using the measure Compression Ratio (CR). The CR is defined as the removal of redundant or irrelevant information and efficiently encodes what remains. It is a division of compressed image size by original cover image size.

CR = Compressed Image Size/Original Image Size

For analysis purposes, many medical videos are selected and for the input videos, the preprocessing and image compression is carried out and its corresponding CR is calculated. Fig. 6 indicates the cover frame, compressed cover frame, and compression ratio.

By using DST for cover frame compression, the average compression ratio is 76.905%.



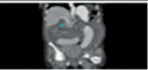
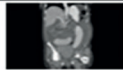


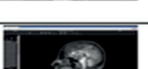





Medical Video (MV)	Cover Frame	Compressed cover frame	CR (%)
MV-1			74.5
MV-2			61.8
MV-3			75
MV-4			72.5
MV-5			93.09
MV-6			84.54

Figure 6: Cover frame, compressed cover frame and compression ratio for different medical videos

4.4 Secret Data Embedding and Frames to Video Conversion

The compressed cover frame is used for embedding binary forms of medical secret data using logical operations. The reduced size of the compressed frame is balanced with binary secret data. After embedding, the cover frame is known as the stego frame.

Stego frame is inserted into the corresponding frame of video frames and it is converted into video. This video is known as a stego video. Then it is transmitted to the receiver.

4.5 Performance Metrics

The performance of the projected method is calculated using the parameters Embedding Capacity (EC), MSE and PSNR. These parameters are used to find out the efficiency of the computational process. EC is defined as the maximum number of bits that can be embedded into the image without affecting the quality of the image. EC is calculated using the multiplication of several rows and columns with 8 for monochrome image and 24 for RGB (red, green, blue) image. MSE is defined as the average of the squared error and it is a non-negative value. PSNR is defined as the ratio of signal power to noise power.

F_O and F_S represent the original frame and stego frame respectively. The MSE and PSNR values are calculated using the following equations and the corresponding values of EC, MSE and PSNR are deliberated for different input medical videos.

$$Error(E) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [F_S(x,y) - F_O(x,y)] \tag{6}$$

$$MSE = \frac{(E)^2}{M * N} \tag{7}$$

$$PSNR = 10\log_{10} \frac{(255)^2}{MSE} \quad (8)$$

M & N denotes the number of rows and columns in the frame. MSE, PSNR values are calculated for the original cover frame and stego frame of a medical video. For the above-selected video, the MSE value is 16.3196 and the corresponding PSNR value is 36.0037. The following Fig. 7 shows different medical videos, stego frames and their corresponding EC, MSE and PSNR values. For selected different medical videos, the average PSNR value is 32.74375.







Medical Video	Stego Frame	EC (Bits)	MSE	PSNR (dB)
MV-1		181760	65.1875	29.9892
MV-2		181760	53.0002	30.8880
MV-3		36864	13.8243	36.7244
MV-4		181760	255.8675	24.0507
MV-5		65536	8.6709	38.7502
MV-6		181760	15.3602	36.06

Figure 7: Stego frames, EC, MSE and PSNR values for different medical videos

4.6 Reconstruction of Medical Secret Data

On the receiver side, stego video is converted to frames. Among that frames, the stego frame is selected. Then, the receiver has to enter the password for authenticating the receiver, if the password is matched then only a reversal process will perform otherwise the process will break. This authentication process improves the security level of the secret data and only authorized receivers can view the secret data. Fig. 8 shows the verification of the authentication process.

```
Enter the password:12345
Password is Correct
Sequence =
1011011011101011001011101011011011001011011011011
```

(a)

```
Enter the password:67895
Wrong Password: Enter Correcet Password
```

(b)

Figure 8: Verification of authentication (a) authorized receiver (b) unauthorized receiver

After checking the authenticity of the receiver, inverse logical operations are applied on the stego frame and the original secret medical data is received without any loss for future analysis purposes. Inverse shearlet transform is applied for the decompression process to get the original medical cover frame. Compare to the original frame, the received frame is more similar and the PSNR value is maximum compared to previous techniques. Fig. 9 shows reconstructed medical secret data at the receiver.

Inverse Shearlet Transform is applied on the frame after retrieving the original secret text. The original cover frame is retrieved and the PSNR values are calculated for different medical videos. Fig. 10 shows the RDH Process of the cover frame, received frame, MSE and PSNR.

Medical Secret Data:

```
'S'
'E'
'NAME SWETHA ID 7659821 ILLNESS CORONARY HEART DISEASE'
```

Figure 9: Reconstruction process













Cover frame	Received frame	MSE	PSNR (dB)
		0.3560	52.6163
		0.5948	50.3874
		2.4192	44.2941
		0.4243	51.8538
		1.0379	47.9692
		2.6512	43.8622

Figure 10: RDH process of the cover frame, received frame, MSE and PSNR

The average MSE value is 1.247 and the average PSNR value is 48.4971 dB (decibel). By using the above methods, the RDH technique is effectively used to retrieve the original medical secret data and cover frame effectively. The following [Tab. 1](#) shows the comparison of the proposed method with existing methods.

Table 1: Comparison of the proposed method with existing methods

Method	Crypt. technique	Compression technique	Steg. technique	Password	Avg. PSNR (dB)
Darbani et al.	DES	–	DCT	–	46.9
Rachmawanto	RSA	Huffman coding	DWT	–	40.310
Ramaswamy et al.	AES	Huffman coding	DWT	–	46.1878
Proposed	Morse code	Arithmetic code compression	DST	Yes	48.4971

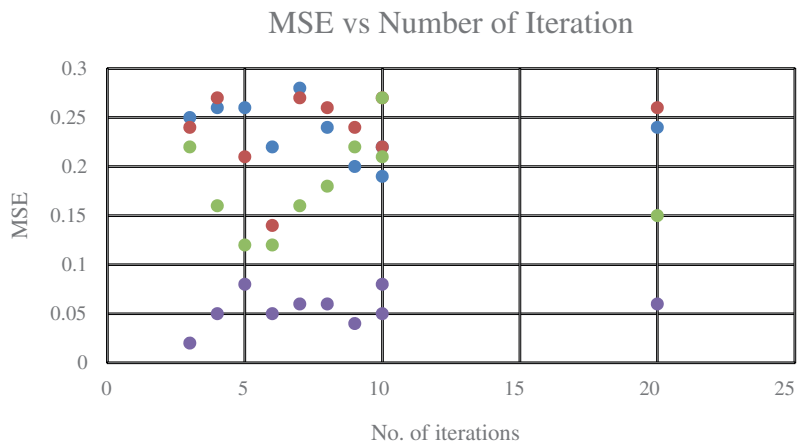
[Tab. 2](#) consists of Performance metrics [Tab. 2](#) shows the performance metrics of of proposed and existing techniques, emerged with proposed Morse code + Arithmetic coding technique in relation to DES, RSA+Huffman, AES+Huffman techniques. From the analysis, we conclude that the proposed one gives minimum MSE compared to other methods.

[Figs. 11a, 11b](#), illustrates the scatter plot graph for MSE and PSNR for the techniques like DES, RSA +Huffman, AES+Huffman techniques and proposed Morse code + Arithmetic coding technique by varying the number of iteration. Considering MSE, the proposed algorithm attains a minimum MSE of 0.01at the maximum iteration. Considering PSNR, the highest PSNR value is attained for the proposed algorithm at

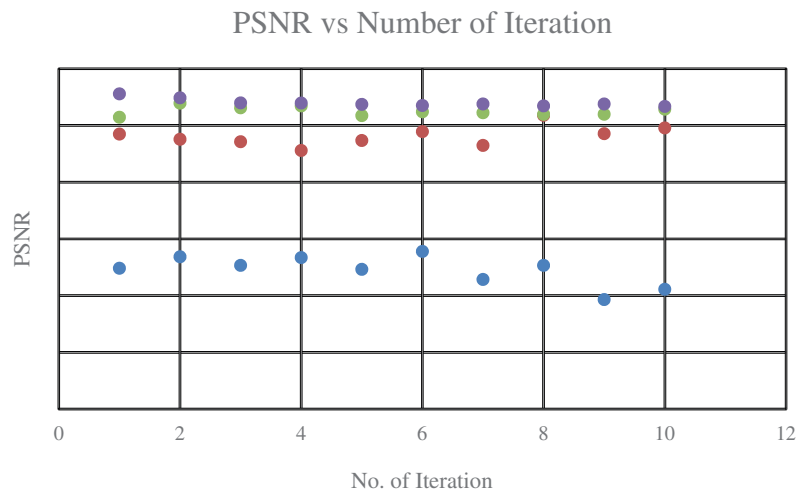
the maximum iteration. Considering SSIM, the graph linearly increases from 0.91 to 0.99 for the iterations. Compared to other techniques, the proposed algorithm attains a better SSIM of 0.999 at the maximum iteration.

Table 2: Performance metrics of proposed and existing techniques

Compression ratio	Performance metrics	Compression and cryptographic techniques			
		DES	RSA +Huffman	AES +Huffman	Proposed Morse code + Arithmetic coding
%1	PSNR	52.41	64.24	65.98	66.72
	MSE	0.42	0.12	0.04	0.02
%3	PSNR	52.35	64.56	66.97	66.98
	MSE	0.39	0.18	0.06	0.022
%5	PSNR	51.32	63.67	66.72	66.89
	MSE	0.443	0.16	0.05	0.012
%9	PSNR	49.65	63.24	65.99	66.98
	MSE	0.53	0.114	0.045	0.015



(a)



(b)

Figure 11: Scatter plot graph for MSE and PSNR (a) MSE (b) PSNR

5 Conclusion

In this paper, the Reversible Data Hiding technique (RDH) is used to securely retrieve the medical secret data and also the original cover frame. Morse code-based encryption, arithmetic compression techniques are used to encrypt the medical secret data and shearlet transform is used to compress the cover frame. In this paper, logical operations are used to embed the secret data into the compressed cover frame. On the receiver side, the password is used to authenticate the receiver and to enhance security. The computational time for encrypting the secret data is minimum. Different medical cover videos are selected to transmit the medical data which provides a better compression ratio compared to existing methodologies. The average compression ratio is 76.905%. On the recipient side, the secret data and the original cover frame is retrieved successfully and the average PSNR value is 48.4941dB. It is observed that the proposed method provides a high PSNR value. This proposed method can be used in secure data transmission in the military, cyber security, etc., In the future, the secret image will be securely transmitted by using cover video.

Future Scope

A further adaptive compression coding technique should be incorporated into the proposed work in order to enhance efficiency for the future work.

Acknowledgement: The authors with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] S. Aiswarya and R. Gomathi, "Review on cryptography and steganography techniques in video," in *Proc. Int. Conf. on Computational Intelligence and Computing Research*, Madurai, India, IEEE, pp. 1–4, 2018.
- [2] A. Darbani, M. M. A. Nezhadi and M. Forghani, "A new steganography method for embedding message in JPEG images," in *Proc. Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, Iran, pp. 617–621, 2019.
- [3] M. K. Ramaiya, N. Hemrajani and A. K. Saxena, "Security improvisation in image steganography using DES," in *Proc. Int. Advance Computing Conf.*, Ghaziabad, India, IEEE, pp. 1094–1099, 2013.
- [4] H. Anada, T. Yasuda, J. Kawamoto, J. Weng and K. Sakurai, "RSA public keys with inside structure: proofs of key generation and identities for web-of-trust," *Journal of Information Security and Applications*, vol. 45, no. 1, pp. 10–19, 2019.
- [5] S. Singh and R. Devgon, "Analysis of encryption and lossless compression techniques for secure data transmission," in *Proc. Int. Conf. on Computer and Communication Systems*, Singapore, IEEE, pp. 1–5, 2019.
- [6] L. Zhang, H. Wang and R. Wu, "A high-capacity steganography scheme for jpeg2000 baseline system," *IEEE Transactions on Image Processing*, vol. 18, no. 8, pp. 1797–1803, 2009.
- [7] I. G. Wiryawan, Sariyasa and I. G. A. Gunadi, "Steganography based on least significant bit method was designed for digital image with lossless compression technique," in *Proc. Int. Conf. on Signals and Systems (ICSigSys)*, Bali, Indonesia, pp. 98–102, 2018.
- [8] Disha and K. Saini, "A review on video steganography techniques in spatial domain," in *Proc. Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, Noida, India, pp. 366–371, 2017.
- [9] S. Hemalatha, U. D. Acharya and Shamathmika, "Mp4 video steganography in wavelet domain," in *Proc. Int. Conf. on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, pp. 1229–1235, 2017.

- [10] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.
- [11] B. Renuka and N. Manja Naik, "Secure video steganography technique using DWT and H. 264," in *Proc. Int. Conf. on Advances in Information Technology (ICAIT)*, Chikmagalur, India, pp. 19–23, 2019.
- [12] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed *et al.*, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639–649, 2018.
- [13] A. Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," in *Proc. Int. Conf. on Science in Information Technology (ICSITech)*, Bandung, Indonesia, pp. 618–621, 2017.
- [14] A. G. Selvi and K. G. Maria, "Probing image and video steganography based on discrete wavelet and discrete cosine transform," in *Proc. Int. Conf. on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, pp. 21–24, 2019.
- [15] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, "Hiding data using efficient combination of rsa cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021.
- [16] S. Lavania, P. S. Matey and V. Thanikaiselvan, "Real-time implementation of steganography in medical images using integer wavelet transform," in *Proc. Int. Conf. on Computational Intelligence and Computing Research*, Coimbatore, India, IEEE, pp. 1–5, 2014.
- [17] S. Lakshmanan and M. M. S. Rani, "Reversible data hiding using spiral order technique in medical images," in *Proc. Int. Conf. on Intelligent Computing and Communication for Smart World (I2C2SW)*, Erode, India, pp. 272–277, 2018.
- [18] S. I. Nipanikar and V. H. Deepthi, "Entropy based cost function for wavelet based medical image steganography," in *Proc. Int. Conf. on Intelligent Sustainable Systems (ICISS)*, Palladam, India, pp. 211–217, 2017.
- [19] V. V. Korgaonkar and M. N. Gaonkar, "A DWT-DCT combined approach for video steganography," in *Proc. Int. Conf. on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, IEEE, pp. 421–424, 2017.
- [20] E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 5, pp. 2400–2409, 2019.
- [21] R. Ramaswamy and V. Arumugam, "Lossless data hiding based on histogram modification," *International Arab Journal of Information and Technology*, vol. 9, no. 5, pp. 445–451, 2012.
- [22] N. Sharma and U. Batra, "Performance analysis of compression algorithms for information security: A review," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 7, no. 27, pp. e2, 2020.
- [23] J. Guo and T. Le, "Secret communication using jpeg double compression," *IEEE Signal Processing Letters*, vol. 17, no. 10, pp. 879–882, 2010.
- [24] G. Kutyniok and D. Labate, "Introduction to shesarlet," In: *Applied and Numerical Harmonic Analysis*, 1st ed., vol. 1, Birkhauser Boston: Shearlets, pp. 1–38, 2012.
- [25] G. Patidar, S. Kumar and D. Kumar, "A review on medical image data compression techniques," in *Proc. Int. Conf. on Data, Engineering and Applications (IDEA)*, Bhopal, India, pp. 1–6, 2020.