I J C T A, 9(6), 2016, pp. 2923-2932 ISSN: 0974-5572

Secret Video Data Hiding with Images Embedding Using Media Data Chunking and Embedding Algorithms

Suresh G.* and K.A. Pathasarathy**

ABSTRACT

Nowadays, to share secret video data in organization or within the organization is one of the challengeable tasks due to privacy issues. There is one more challenge in the task is to build the image frame with minimal error and enhance the de-embedding rate of secret data. In literature, this paper found that many works are done in image and audio steganography using LSB (Least Significant Bit) and DCT (Discrete Cosine Transformation) Approach. However, existing system is not flexible with multi-media content and it requires additional space to recover the data. It takes long time to recover the de-embedded data and data accuracy is low. To overcome these problems, proposed approach brings the media data chunking and embedding algorithm to enhance the privacy of the video data with image cover file. Here, AES algorithm is utilized to encrypt the secret data before embedding and decrypt the secret data after de-embedding process. Here, proposed algorithm works to build the frame in matrix transformation according to the data transmission rate which avoids data collusion and packet recovery collapse issues. The algorithm also works to enhance the de-embedding image frame rate with minimal data extraction time. Based on experimental results, the Media Data Chunking and Embedding Algorithm performs well on Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR) compared than existing techniques.

Keywords: secret video data, data embedding, data de-embedding, media data chunking and embedding algorithm, mean Squared Error, Peak Signal Noise Ratio..

1. INTRODUCTION

In general meaning, the data-hiding operations will result in host signal distortion. However, distortion does not matter, how big or small and how it is going to affect the application. As per current needs, these kinds of techniques are used in medical, defense, military as well as corporate sectors to maintain high level of privacy. Data hiding approach objective is to embed some credential information into a carrier signal by varying the insignificant components for copyright privacy. In this case, it is imperative to embed the extra secret message with a reversible way so that the original video data can be perfectly restored after extraction of the hidden data. However, this method needs additional space to extract the content. In LSB method, secret message is compressed with cover image pixel co-ordination value with compressed location map. Next, it is embedded with LSB plane. Reversible data hiding methods, a spare place can always be made available to accommodate secret data as long as the selected item is compressible, but the capabilities are low.

Current methods have high MSE (Mean Squared Error) value which contains maximum number of error in cover files and it takes long time for extracting the cover file after de-embedding and decryption process. In some applications, an inferior assistant or a channel administrator wants to append some extra content, like origin information, image notation or data privacy.

* Research Scholar, St. Peters University, Avadi, Chennai, Tamilnadu, India, *Email: sureshspu.phd@gmail.com.*

** Research Supervisor, St. Peters University, Avadi, Chennai, Tamilnadu, India and Principal, Akheyaa College of Engineering, Puludhivakkam, Kancheepuram, Tamilnadu, India, *Email: kaps_wwh2003@yahoo.com*

This system is not flexible with multi-media content and it requires additional space to recover the data. Existing scheme is made up image encryption, data embedding and data-extraction/image-recovery phases. The data sender encrypts the original uncompressed image using an encryption key to produce an encrypted image. Hence, the data-hider compresses the least significant bits of the encrypted image using an image-hiding key to allocate a sparse space to accommodate the extra information. The receiver side, the embedded image creates space which can be easily retrieved from the encrypted image. It has extra information according to the data-hiding key. This system takes long time to recover the extracted data.

To solve these problems, media data chunking & embedding algorithm is proposed to enhance the video data privacy with image embedding. An AES algorithm is utilized for multiple time encryption and decryption based user requirement without any content extraction issues. In this system, embedding performance is good with video data where existing approaches produced the options to encrypt the data through image or text which are not much flexible with current requirement. Finally, it minimizes the image extraction time with high image recovery rate with system flexibility. This system avoids utilization of additional storage for image recovery. Here, proposed algorithm works to build the image frame in matrix transformation according to the data transmission rate which avoids data collusion and packet recovery collapse issues. It also works to enhance the de-embedding image frame rate with minimal data extraction time. Here, data can be encrypted based on images; this system is capable to process any kinds of data without key complexities and Key length problems. The contributions of this paper are follows as:

- Proposed Systems hides the secret video data with image embedding.
- Proposed algorithm is worked to build the frame in matrix transformation according to the data transmission rate
- It minimizes the image extraction time with high content recovery rate along with system flexibility.
- Proposed system reduces the MSE and PSNR compared than existing approaches.

The rest of the paper is presented as follows; in section 2, we mention related work which is close to the proposed mechanism. Section 3 introduces the system methodology with proposed techniques elaboration. Section 4 discuss about implemented result and system performance. Section 5 concludes the overall work with future enhancement is given.

2. RELATED WORK

In paper [1], authors designed resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the descriptor can scrutinize a low-resolution version of the image, study local statistics according to the utilization of the statistics. It decodes the next resolution level. In paper [2], authors investigated the development of the discrete Fourier transform (DFT) in the encoded domain by using the homomorphism properties of the underlying cryptosystem. In paper [3], authors focused to speed up linear operations on encrypted signals via parallel process and to minimize the size of the encoded signal. In paper [4] authors designed an efficient buyer seller watermarking approach based on homomorphism public-key cryptosystem and merged signal representation in the encrypted domain. In paper [5], authors developed a novel reversible data hiding scheme for encrypted image. With an encrypted image containing additional data, one may firstly decode it using the encryption key, and decoded version is similar to the original content.

Paper [6] implemented reversible data hiding algorithm, which can recover the original image without any distortion from the marked image. After that, hidden data have been extracted. The computational complexity of their technique was low and the execution time was short. In paper [7], authors implemented new fingerprinting protocol applying additive homomorphism property of Okamoto–Uchiyama encoded scheme. Exploiting the property, the enciphering rate of fingerprinting scheme can be close to the

corresponding cryptosystem. Paper [8] focused on reversible data hiding method that modifies the various histograms between sub-sampled images. It exploits the high spatial correlation inherent in neighboring pixels to achieve high capacity and imperceptible embedding. In paper [9] authors developed reversible data hiding scheme based on histogram modification. In paper [10], authors presented robust lossless data hiding technique, which does not generate salt-and-pepper noise. By identifying a robust statistical quantity based on the patchwork theory and employing it to cover data differentiating the bit-embedding process based on the image pixel group's distribution characteristics. It utilizes the error correction codes and permutation approaches.

In paper [11], authors focused on the improvement of overflow location map. They designed a new embedding scheme that helps user to construct an efficient payload-dependent overflow location map. In paper [12], PDA is given to significantly reduce the capacity consumption by overhead information. Paper [13], authors developed technique to enhance the distortion result at a minimal embedding capacities and mitigates the capacity control issues. In paper [14], authors implemented multiple base lossless schemes based on JPEG-LS pixel value prediction and reversible difference expansion. It employs a pixel value prediction mechanism to decrease the distortion caused by the hiding of the secret data. Paper[15] implemented efficient integer transformation based reversible watermarking which show that Tian's difference expansion (DE) technique can be reformulated as an integer transformation.

Paper [16] developed reversible watermarking algorithm with very high data-hiding capacity. Generally, it is applied for color images. Paper [17], authors developed novel reversible data embedding method for digital images. They explore the redundancy in digital images to gain very high level embedding capacity and contain to low levels distortion. Paper [18] formulated two general approaches for lossless embedding that can be applied on images as well as any other digital Objects, including audio and other structures. Paper [19] developed lossless (reversible) data-embedding technique which is applicable for exact recovery of the original host signal upon recovery of the embedded messages. Paper [20] designed a novel data hiding algorithm which contains large amount of secret data based on integer wavelet transformation. This approach recovers the original image content without any distortion from the marked image after the hidden data have been extracted.

In paper [21], authors developed LOCO-I (Low Complexity Lossless Compression for Images) technique for continuous-tone images which combines the simplicity of Huffman coding with the compression potential of context designs, thus "enjoying the best of both universes". In paper [22], authors focused on the generalization the method utilization of a decompression approach in the coding scheme for embedding data. This system proves that the generalized codes can achieve the rate–distortion bound as long as the compression algorithm achieves entropy. Paper [23] developed reversible data embedding method for digital images. They explored the redundancy of digital images with high level of embedding capacity. It contains low distortion value. In Paper [24], authors suggested a trust-overlay network over multiple data centers to develop a reputation system to maintain the trust between providers and data owners. In paper [25], author implemented a resolution progressive compression scheme which compresses an encrypted image progressively in resolution. Here, decoder can observe a low-resolution version of the image.

Paper [26] implemented a rigorous evaluation of three metrics to assess the quality of compressed images. The compression approach is used to evaluate the classical JPEG coder. In paper [27], authors designed XOR Ciphering approach which has the benefit of inserting the data without dynamic icon aggregation. Thus, it is steady for the data protector to reversibly embed accumulation in encrypted image. In paper [28], author developed an interactive buyer-seller protocol for invisible watermarking where seller does not get to know the exact watermarked copy that the buyer receives. In paper [29], authors studied the survey of digital fingerprinting with video scrambling algorithms based on partial encryption. They also developed architecture for joint fingerprinting and decryption that contain belief for better compromise between practicality and privacy of digital applications. In paper [30], author described a scheme where

each receiver of a multicast session receives a stream with a different, unique watermark; while still retain the multicast scalability.

3. SYSTEM METHODOLOGY

This section explains system design and workflow of proposed Media Data Chunking and Embedding to enhance the video data privacy with image embedding. Here, this techniques works on both side namely as receiver and as well sender sides to maintain the high level of privacy. The direct embedding reduces the data encryptions time with total number of coefficients and their background knowledge will be closer to the embedded image. This transformation makes the data an 8*8 blocks. Before starting the data embedding process, the embedded data is converted into given 8*8 blocks. Mean time, these methods assist receiver to view original video data as well recover image. Here, all blocks of data are compressed in one folder before image extraction. In embedding process, this approach puts the efforts to recover the data error, enhanced image accuracy and reduces the image extraction time. The system architecture of proposed system is explained in details figure 01.

3.1. Data Sender

Data Sender is active user who wants to communicate his secret data to his/her desired destination. Here, data sender sends the secret video data with cover file to ensure the data privacy.

3.2. Secret Video Data

Secret video data is expressed as data sender original video file. Data sender wants to contribute his/her data with data receiver in secure medium. Here, secret video data can be transmitted in any formats like. AVI, MPEG and MOV video. Based on his/her requirement, he/she can communicate the data with help of MDCE and AES algorithm to maintain the security.

3.3. Encryption and Embedding

This module elaborates the privacy, embedding details of secret data. Once, user selects the secret video data then this module assists to user to build the privacy with the help of MDCE and AES algorithm. In details, after giving input as secret video data, this mechanism feasible user to selects image cover file for embedding. Hence, it moves to encrypts the data and generate the key for secret data. Next, it applies

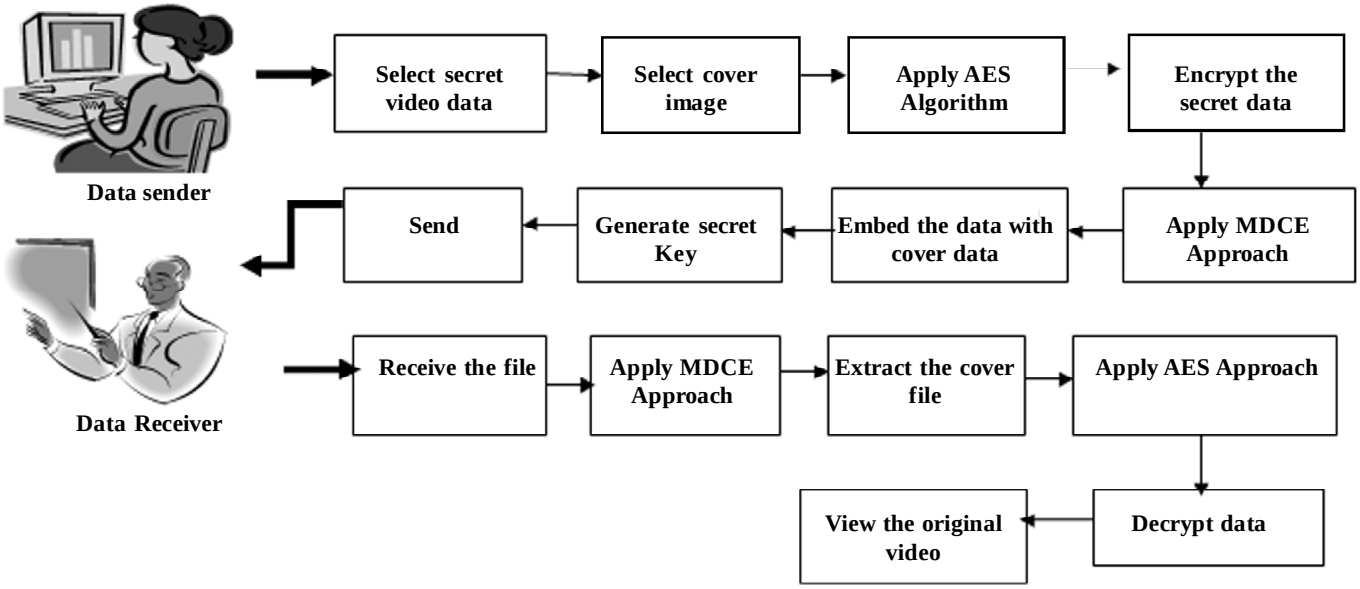

Figure 1: System architecture for secret video data hiding with documents embedding with MDCE approach

MDCE algorithm to build the cover file in frame by frame in matrix transformation and segment the image in frame by frame. After segmentation of image frame, this approach assists to embed to entire the data with cover file for avoiding malicious attacks.

3.4. Data Receiver

In this module, data receiver receives the ECF file from network. Hence, it applies AES algorithm to decrypt the EFC with Valid SK. Next, it applies MDCE algorithms to extract the ECF and recover the secret video content. With the help of MDCE approach, data receiver can receive the ORVF with minimal extraction time and low error rate.

3.4.1. De-embedding with Decryption Process

This module explores about de-embedding and decryption procedure of received content. In details, data receiver receive the file hence its move for data decryption process with the help of AES algorithms. An encrypted image containing embedded data, receiver firstly decrypts the secret data with help of secret key to decrypt the contents. The decrypted image content bits rate are retrieved correctly. Finally, He/she can open his/her secret video with without any interruption or error in proper RGB scale with correct formats with the assistance of MDCE algorithms.

3.4.2. Media Data Chunking and Embedding Algorithms (MDCE)

This section explains the introduction, feature and implementation steps of Media Data Chunking and Embedding Algorithms. The main objective of this algorithm is to maximize the image frame visual quality for multicasting the minimum-visual-quality-guaranteed constraint. MDCE build the image frame in matrix transformation and segment the image in frame by frame. After segmentation of image frame, this approach assists to embed the entire secret video data with cover file for avoiding malicious attacks. This system adapts the transmission bit-rate on network based on image quality and frame size of image content. This algorithm has following features:

- Content Distribution: it distributes the secret video to data receiver according to their channel allocation. It multicast the video in packet by packet and transmits to data receiver host.
- Image frame rate scheduling: it multicast the video in frame bit/seconds. It schedule data packet based mutilating video. Finally, it estimates visual quality even if secret information about incremental quality is not provided.
- Two-state bit rate adaptation: This system utilizes e finite-state machine to adapt the, image frame rate schedule to variable video bit rates and produce the quality of videos. This system also avoids data collusion and packet recovery collapse issues.

The mathematical procedure of MDCE algorithm is explained below in details with their pseudo code. This algorithm is distributed in two pars namely as embedding and de-embedding process.

3.5. Embedding Process

Input: *Select the secret video files (SVF) and selects the Cover file (CF)*

Output: *Embedded Cover files (ECF) with Secret Key (SK)*

Procedure: *Encrypts SVF with AES approach*

Generate the secret key (SK) to apply encryption

Apply MDCE approach to embed the SVF with CF

Construct the CF in matrix transformation in block formats

If CF constructed in block then

Multicast the SVF in frame bit rate to share on network (N)

Transmits the embedded content (EC) to data receiver successfully

Else

Move to select to SVF and CF.

End

Pseudo code 1. MDCE Embedding Process

3.6. Embedding Process

Input: *Receive Embedded Cover file (ECF) with Secret Key (SK)*

Output: *Original Retrieved Video File (ORVF)*

Procedure: *Select ECF file and enter the SK*

If SK is verified then

Dembedded the ECF

Apply MDCE approach

Extract the Secret Video Frame (SVF)

Recover the image frame by frame

View the ORVF

Else

Display Invalid ECF or SK

End

Pseudo code 2. MDCE Embedding Process

3.7. AES Algorithm

This module introduce the AES algorithms with their features the utilization procedure of the approach. AES is a block cipher which contains following block length namely as 128, 192, or 256 bits. Most of the case, it utilizes the key length is 128 bits. Secret video file (SVF) contains encryption 10 rounds to process 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Decryption process will be applicable in similarly in reverse order. Here, AES is utilized for flexibility of key length, increasing computing power and avoids against exhaustive key search attack. Except for the last round in every scenario, all other rounds are identical each round of processing includes one single-byte according to substitution step, a row-wise permutation step, a column-wise mixing steps, and the summation of the round key.

4. RESULT AND DISCUSSION

4.1. Programming Environment

In order to compares proposed mechanism with existing algorithm. The experiment is conducted on a laptop with Intel Dual Core processor (1.836 Hz), 2GB memory, and Window 7 Ultimate system. Here, this method implemented in JAVA with JDK 1.8 and Netbeans 8.0

4.2. Datasets

To evaluate the performance of Proposed approach, there are three kinds of secret video files is selected namely as avi, mpeg and mov. These dataset are used to embed with covered file as images with different formats. Datasets details are explained table 1.

Table 1
Dataset Details

S. No	*Types of Cover File*	*Types of Secret Data*
1	.bmp	.mpeg
2	.jpeg	.avi
3	.gif	.mov

4.3. Performance Matrix

In this phase, proposed scheme represent mathematical model to enhance privacy of secret data. In this scheme, security model work between data sender and data receiver. Even though, server is not trusted then also data sender secret message will be in safe during data transmissions. It displays following model separately such as Mean Squared Error (MSE), and Peak Signal Noise Ratio (PSNR).

4.3.1. Mean Squared Error (MSE)

In this section, means squared error performs the error rate of embedding image frame to ensure the accuracy of image data. Here, mathematical evaluation of MSE is expressed in equation (1). It also evaluated the height and width of embedded image frame.

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} \left(P\left(i, j\ \right) - S\left(i, j\right) \right)^2 \tag{1}$$

Where, MSE is Mean Squared error, H and W are height width of image frame and P (i, j) represents original image frame and $S(i, j)$ represents corresponding stego frame.

4.3.2. Peak Signal To Noise Ratio (PSNR)

In this phase PSNR represents the mathematic model to evaluate the noise ratio of embedding images of secret during data embedding. The mathematical equation is expressed in equation (2).

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \tag{2}$$

Where, PSNR is peak signal noise ratio of embedding, L is peak signal level for a grey scale of image frame it is taken as 255.

4.4. Simulation Results

Table-01 displays Mean Squared Error, Peak Signal Noise Ratio for .avi, .mpeg and .mov dataset. The approach is analyzed in terms of Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR) display their average values for respective parameter with dataset. Here, there proposed system is evaluate existing approach namely as Data Encryption Standard [20], TRIPLE Data Encryption Standard [6], Least Significant Bit [19], Discrete Cosine Transformation [9].

According to proposed MDCE protocol evaluation result in figure 2 and 3 for .avi, .mpeg and .mov dataset. Proposed MDCE approach is the best approach. In terms of mean squared error and peak signal

Table 2
Communication Cost (CC) Encryption Time (ET) & Decryption Time (DT) for Document, Image and Video Database

Learning Algorithms	*.AVI*		*.MPEG*		*.MOV*	
	MSE	*PSNR*	*MSE*	*PSNR*	*MSE*	*PSNR*
DES	0.49	39.27	0.485	41.27	0.48	42.27
TRIPLE DES	0. 47	44.47	0.45	48.85	0.46	43.36
LSB	0.44	49.56	0.42	50.56	0.43	50.56
DCT	0.34	52.23	0.32	50.21	0.34	51.23
MDCE	0.173	55.45	0.169	54.56	0.178	56.89

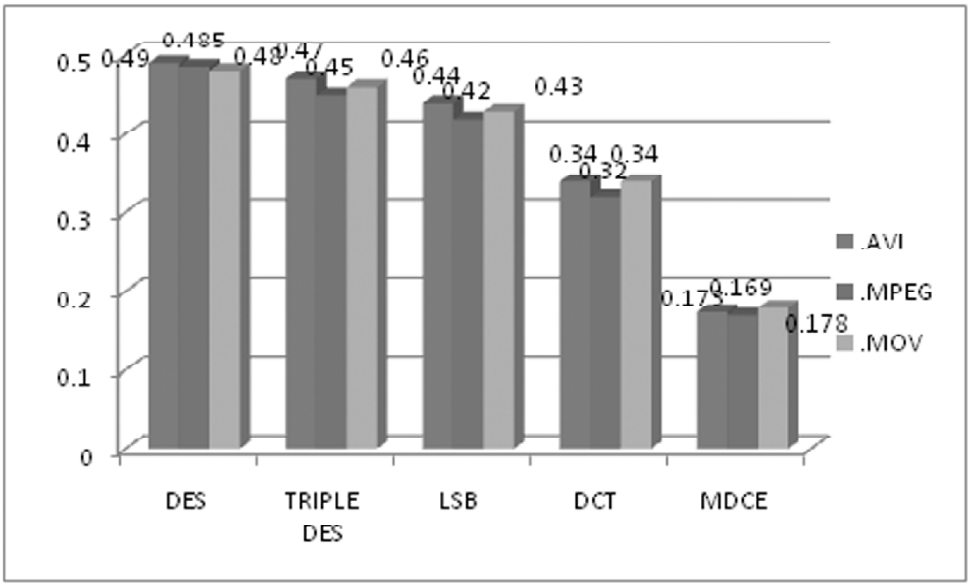

Figure 2: Mean Squared Error () for .avi, .mpeg and .mov database.

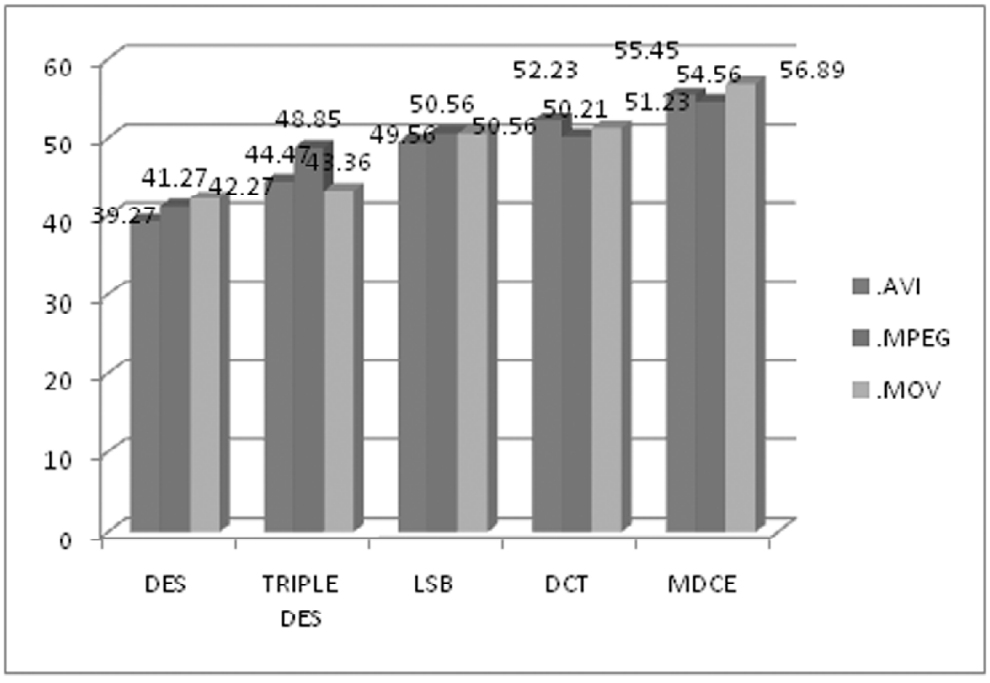

Figure 3: Peak Signal Noise Ratio () for .avi, .mpeg and .mov database

noise ration, proposed MDCE approach display that it always yields the best performance in both all graphical result as well in tabular result.

In terms MSE and PSNR with respective database, DCT (Discrete Cosine Transformation) is closest approach to proposed method. However, DCT result is too far compare than proposed approach. Therefore, this paper claims that MDCE is best approach for all dataset.

5. CONCLUSION

In this paper, MDCE algorithm is presented to enhance the video data privacy with image embedding. An AES algorithm is utilized for multiple time encryption and decryption based user requirement without any content extraction issues. In this system, embedding performance is good with video data where existing produced the options to encrypt the data through image or text which are not much flexible current requirement. Here, proposed algorithm is worked to build the image frame in matrix transformation according to the data transmission rate which avoids data collusion and packet recovery collapse issues. A proposed algorithm is also worked to enhance the de-embedding image frame rate with minimal data extraction time. It minimizes the image extraction time with high image recovery rate with system flexibility. This avoids utilizing additional storage for image recovery. Here, this techniques works on both side namely as data receiver and as well data sender sides to maintain the high level privacy. The directing embedding reduces the data encryptions with total number of coefficients and their background knowledge will be closer to the embedded content. Mean time, this method assists to receiver to view original data and as well recover the embedded contents.

Finally, this approach puts the efforts to recover embedded data with minimal error and enhanced recovered image accuracy as well. It also works to reduce the image extraction time with minimal efforts. To evaluate the performance of proposed approach, there are two parameters with respective datasets are introduced namely as Mean Squared Error and Peak Signal Noise ratio. This approach is evaluated .avi, .mpeg and.mov video datasets where it noticed that proposed approach is performed well on every respective parameters compare than existing approaches. In future, this paper work can be extended to transmit the secure in ad-hoc network, vehicular ad-hoc network to communicate the secret message among reliable users.

REFERENCES

[1] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inform. Forensics Security, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[3] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[4] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[5] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[7] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proceedings IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[8] Kim K. S., Lee M. J., Lee H. Y., & Lee H. K. "Reversible data hiding exploiting spatial correlation between sub-sampled images". *Pattern Recognition*, vol. 42, no. 11, pp. 3083-3096, 2009.

[9] Tai, W. L., Yeh, C. M., & Chang, C. C. "Reversible data hiding based on histogram modification of pixel differences", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906-910, 2009.

[10] Ni Z., Shi Y. Q., Ansari N., Su W., Sun Q., & Lin X. "Robust lossless image data hiding designed for semi-fragile image authentication", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497-509, 2008.

[11] Hu Y., Lee H. K., & Li J., "DE-based reversible data hiding with improved overflow location map", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250-260, 2009.

[12] Weng, S., Zhao, Y., Pan, J. S., & Ni, R. (2008). Reversible watermarking based on invariability and adjustment on pixel pairs. Signal Processing Letters, IEEE, 15, 721-724.

[13] Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. Image Processing, IEEE Transactions on, 16(3), 721-730.

[14] Wu, H. C., Lee, C. C., Tsai, C. S., Chu, Y. P., & Chen, H. R. (2009). A high capacity reversible data hiding scheme with edge prediction and difference expansion. Journal of Systems and Software, 82(12), 1966-1973.

[15] Wang, X., Li, X., Yang, B., & Guo, Z. (2010). Efficient generalized integer transform for reversible watermarking. Signal Processing Letters, IEEE, 17(6), 567-570.

[16] Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. Image Processing, IEEE Transactions on, 13(8), 1147-1156.

[17] Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Techn., 13(8), 890-896.

[18] Fridrich, J., Goljan, M., & Du, R. (2002, April). Lossless data embedding for all image formats. In Electronic Imaging 2002 (pp. 572-583). International Society for Optics and Photonics.

[19] Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. Image Processing, IEEE Transactions on, 14(2), 253-266.

[20] Li, Y. C., Yeh, C. M., & Chang, C. C. (2010). Data hiding based on the similarity between neighboring pixels with reversibility. Digital Signal Processing, 20(4), 1116-1128.

[21] Xuan, G., Chen, J., Zhu, J., Shi, Y. Q., Ni, Z., & Su, W. (2002, December). Lossless data hiding based on integer wavelet transform. In Multimedia Signal Processing, 2002 IEEE Workshop on (pp. 312-315). IEEE.

[22] Zhang, W., Chen, B., & Yu, N. (2012). Improving various reversible data hiding schemes via optimal codes for binary covers. Image Processing, IEEE Transactions on, 21(6), 2991-3003.

[23] Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Techn., 13(8), 890-896.

[24] Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. Internet Computing, IEEE, 14(5), 14-22.

[25] Liu, W., Zeng, W., Dong, L., & Yao, Q. (2010). Efficient compression of encrypted grayscale images. Image Processing, IEEE Transactions on, 19(4), 1097-1102.

[26] Mayache, A., Eude, T., & Cherifi, H. (1998, October). A comparison of image quality models and metrics based on human visual sensitivity. In Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on (pp. 409-413). IEEE.

[27] Rani, S. U., & Jayamma, R. (2014). Reversible Records Whacking in Encrypted Images by Reserving Possibility before Encryption.

[28] Memon, N., & Wong, P. W. (2001). A buyer-seller watermarking protocol. Image Processing, IEEE Transactions on, 10(4), 643-649.

[29] Kundur, D., & Karthik, K. (2004). Video fingerprinting and encryption principles for digital rights management. Proceedings of the IEEE, 92(6), 918-932.

[30] Parviainen, R., & Parnes, P. (2001). Large scale distributed watermarking of multicast media through encryption. In Communications and Multimedia Security Issues of the New Century (pp. 149-158). Springer US.