International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.10 (2015), pp.99-110
http://dx.doi.org/10.14257/ijmue.2015.10.10.11

Discrete Cosine Transformer Based Visual Secret Sharing With Chaos Visual Cryptography

[1] I. Edwin Dayanand [2] and R. K. Selva Kumar

[1]*Research scholar, Manonmaniam Sundaranar University, Tirunelveli, India*
[2]*Professor, Agni College of Technology, Chennai, India*
edwindaya@gmail.com[1], rkselvam@rediffmail.com[2]

Abstract

With the increasing threats on multimedia information sharing, degradation of security is one of the most important concerns. Visual Cryptography is an emerging field for improving the security level by encoding the secret video using encryption scheme and performs computational free decoding process. The secret sharing through visual cryptographic techniques for multiple stack users is not sufficient in providing high percentage result on video sharing domain. Video sharing did not develop source key properties for individual frames and as a result the quality estimation strategy on video frame was not achieved. Moreover, the target rate constraint for video quality under the encryption-decryption was not achieved. This encryption-decryption target key rate declines on arranging multiple sequences of frames from multiple stack users. To improve the quality of visual secret video sharing scheme, a Discrete Cosine Transform Chaos Cryptographic (DCTCC) mechanism is proposed in this paper. The main objective of DCTCC is to enhance the security level of different level video frame using the encryption key properties. Initially, sender takes the video of differing frame length and compresses the video on image using the Discrete Cosine Transformer. The Discrete Cosine Transformer based visual secret sharing of video in the image takes the luminance values and provides high lossless compression. Second, the embedded video frame is encrypted to perform the secret sharing (i.e., visual cryptographic) using the chaos method. The Chaos method uses the enhanced RSA key properties to improve the video quality estimation strategy. Chaos method in DCTCC works effectively with non-linear dynamic set of video frames from users and also with the discrete time dynamical video cryptographic system. On the decryption side, the chaos method is applied in the reverse procedural order to fetch the video quality of video frames from original image. Experiment is conducted on factors such as mean square error rate, and secret video sharing efficacy level and encryption time.

Keywords: *Discrete Cosine Transformer, Video Compression, Video Cryptography, Chaos, RSA Encryption Key Properties, Frame length*

1. Introduction

In this current era, communication through electronic media has not only become an integral issue but also a significant way of everyone's life due to its simplicity and fastness. With the application of communication through electronic media on such a large scale, the issue of visual cryptography for securitizing the visual information has gained popularity. As a result for efficient information transmit in a more secured manner it has become necessary to design methods accordingly.

Two-pass Rate Control (TRC) [1] method for H.264 VBR coding, resulted in significant improvement of video quality by reducing the average peak signal-to-noise ratio using Gaussian model. However, the secret sharing of video through visual cryptographic techniques for differing users were not sufficient enough in providing high

ISSN: 1975-0080 IJMUE

percentage result on video sharing domain. Accelerated Sequence Matching (ASM) [2] method on video sequences was introduced for dealing with large volume of data using dedicated indexing structure. However, the sharing of video sharing did not ensure key properties for individual frames resulting in compromise of quality estimation strategy whereas our mechanism introduced key properties to improve the quality of video frame.

A chaotic encryption scheme in [3] was designed with the objective of improving the performance map using Modified Logistic Map (MLP). However, it was achieved by compromising the encryption time. A chaos based cryptography in [4] increased in the protection and privacy of the image using fast encryption algorithm. However, encryption time was not included. In contrast our mechanism reduced the encryption time by applying chaos cryptographic visual cryptographic scheme.

Visual cryptography is one of the cryptographic techniques that encrypt the visual information in such a manner that the method of decryption is performed without the aid of computers. Dynamic cryptography using chaos oscillations introduced in [5] provided a completely visual decoding process. Scale Invariant Feature Transform (SIFT) [6] was introduced to improve the retrieval or decoding performance using local key point descriptors. However, both the methods suffered from the computation time, whereas our mechanism provided minimum decryption time for differing frame length. Image Security Technique in Visual Cryptography (IST-VC) [7] applied blue noise dipthering principles to improve the secret images being embedded. However, high quality shared images were not obtained, which we addressed in our mechanism through chaos method.

Step construction for visual cryptography in [8] reduced the average pixel expansion using (2, 2) VCS recursively. However, efficient partition of share remained unaddressed, whereas in our mechanism we address this issue non-linear dynamic set of video frames. Quantization Index Modulation (QIM) for Biometric Encryption (BE) in [9] introduced mechanisms to reduce the false acceptance and rejection rate. Neighbor Mean Interpolation (NMI) technique [10] was introduced to improve the embedding capacity resulting in low PSNR values. However, the mean square error rate was unaddressed in both QIM and NMI which our work solved through chaos based encryption properties.

The focus of this work is to improve the quality of visual secret sharing through Discrete Cosine Transform Chaos Cryptographic Video Frame (DCTCC) mechanism. The contributions of Discrete Cosine Transform Chaos Cryptographic Video Frame (DCTCC) mechanism include the following:

- To improve the quality of visual secret video sharing scheme using a Discrete Cosine Transform Chaos Cryptographic Video Frame (DCTCC) mechanism
- To enhance the security level of different level video frame using the encryption key properties and Discrete Cosine Transformer that takes the luminance values for providing high lossless compression
- To increase the encrypted embedded video frame to perform the secret sharing (*i.e.*, visual cryptographic) using the chaos method
- To improve the video quality estimation strategy using applying the Chaos method works effectively with non-linear dynamic set of video frames from users and also with the discrete time dynamical video cryptographic system using the enhanced RSA key properties.
- To apply reverse procedural order of the chaos method on the decryption side to fetch the watermarked video frames from original image

2. Related Works

The theory of chaos has been significantly studied for several years by many researchers. As the properties of chaos are highly desirable for cryptographic applications, specific attention has been paid on the research for visual cryptography with chaos mechanisms. A circuit design for logistic map module was introduced in [11] with the

main aim of improving the precision by evaluating correlative peak interval. However, only approximate formula for evaluating correlative peak interval was obtained that may result in error rate whereas our mechanism included discrete time interval model random key stream pseudo generator. A hybrid approach was introduced in [12] using chaos to address scalability problem of key values. However discreteness was not solved. Data security and authentication in [13] addressed the security and authentication of data using scrambling operation. However, the video sequences were not encrypted in an efficient manner whereas our mechanism performs efficient encryption using enhanced RSA algorithm.

Secure Communication based on Chaos system was introduced in [14] with the purview of increasing the security. Discrete Cosine Transform Domain (DCTD) in [15] was introduced to reduce the effect of noising with the help of Hartung technique. Though noise was reduced, security was compromised which is provided by our mechanism using visual cryptographic technique. A robust watermarking with visual cryptography was introduced in [16] to protect the digital content using Robust Discrete Wavelet Transform (RDWT) and Singular Value Decomposition (SVD). Embedded Zero Wavelet (EZW) and Set Partitioning in Hierarchical Trees (SPIHT) in [17] not only provided mechanism to improve the embedded results but also to improve the compression ratio. Though noise was significantly reduced, encryption time was compromised in the above said methods, which we concentrate in our work through quantization process.

A geometry based correlation model introduced in [18] provided ways to significantly improve the decoding performance with the aid of local transformation in different images. Intensity Division was concentrated in [19] to address the issues related to noise rate using new Visual Cryptography scheme. However, dimensionality was not addressed for various images. With the objective of providing security, two algorithms were introduced in [20] with digital signature. However, the above mentioned methods lack quality of video in retrieving end. Our mechanism addresses this issue by designing visual secret video sharing scheme using discrete cosine transformer. Visual cryptography based on chaos is still in its infancy. In such a situation, our mechanism has been to improve the quality of visual secret video sharing scheme, reducing mean square error rate and enhancing the secret video sharing efficacy level.

3. Discrete Cosine Transform Chaos Cryptographic Mechanism

The visual secret sharing of video sequence on the image is carried out with the effective visual cryptographic technique to improve the quality rate on video compression. The video frame of varying frame length is taken and then the visual secret sharing procedure is employed. The visual secret sharing in our proposed work is to embed the video sequence context in the base image for reducing the threats during video communication. In order to improve the percentage of security level, the chaos visual cryptographic technique is adopted. With the application of visual cryptographic techniques, video secret sharing efficiency is improved.

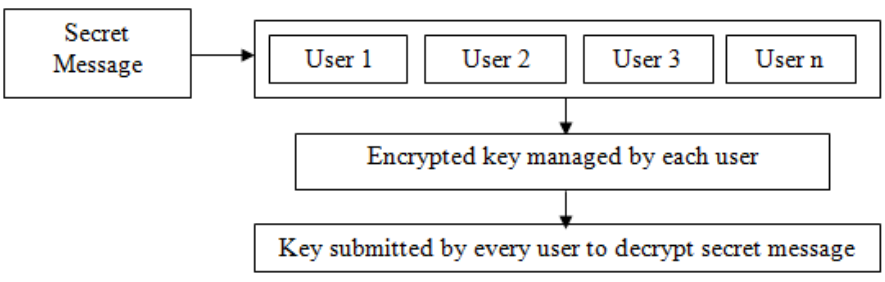

Figure 1. Visual Cryptographic Scheme for Secure Message Transmission

Figure 1 shows the visual cryptographic scheme for secure message transmission. Visual cryptography in DCTCC mechanism shares the encoded secret video frames into 'n' number of participants (*i.e.*, users). The shared information (*i.e.*, video) to the different users holds separate unique encrypted key on their side. All the participants need to submit their private key to improve the security level on visual cryptography scheme. The visual cryptography scheme in DCTCC mechanism follows the chaos method. The overall block diagram of DCTCC mechanism is shown in Figure 2.

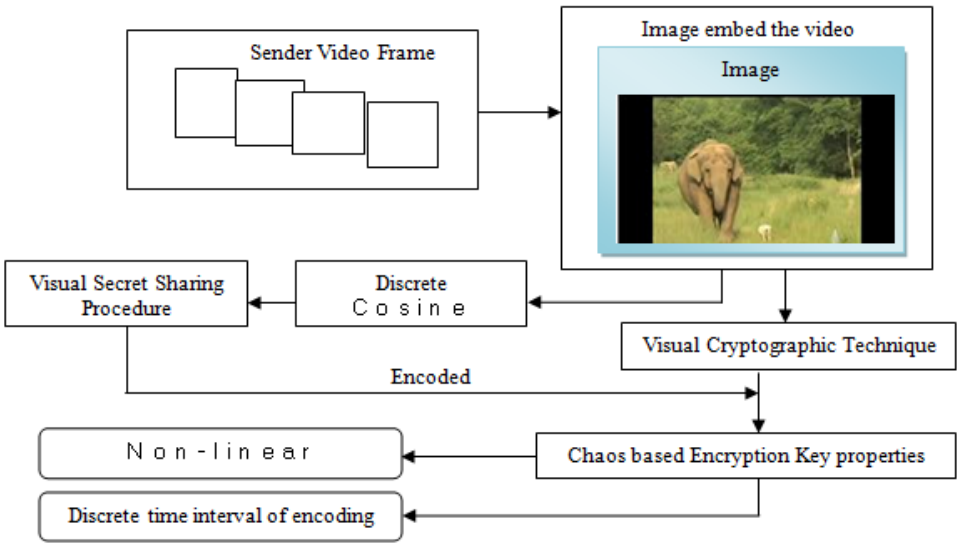

Figure 2. Block Diagram of DCTCC Mechanism

During the transmission of the video frames from the sender side to the receiver side, there may be loss of frames (*i.e.*, security level get minimized). To overcome this drawback, the Discrete Cosine Transform Chaos Cryptographic (DCTCC) mechanism is introduced. This mechanism is shown in an elaborate manner in the Figure 2, where the sender video frame is embedded in the image. The video frame follows the visual secret sharing of video procedure using the Discrete Cosine Transformer. Discrete Cosine Transformer initially starts with the zero state and other spatially high frequency video frame luminance value is computed. The visual secret sharing of video with the Discrete Cosine Transformer operates with the variable frame length, tuple and quantization step.

The video frame is encoded using the chaos cryptographic techniques. The encryption carried out using the chaos key properties which works with the non-linear dynamic set of frames on the discrete time interval. The visual secret sharing of video with visual cryptographic technique in DCTCC improves the security level of different length of the video compression. Encryption operation is done with the DCTCC mechanism using the chaos encryption-decryption method. The decryption operation is carried out through the human visual system without any computations. The elaborate description involved in the design of DCTCC mechanism is discussed in the forthcoming sections.

3.1. Visual Secret Sharing of Video Sequence

The design consideration of DCTCC mechanism starts with the visual secret sharing of video sequence. In DCTCC mechanism, the visual secret sharing is carried out to provide higher security level for content owners (*i.e.*, secret message owners). The cryptographic system alone can't provide high security levels. So the contents are secured with the visual secret sharing concept. The visual secret sharing is provided with high robustness,

invisibility, data capacity, and security. The visual secret sharing of the secret message is carried out using the Discrete Cosine Transformer and briefly described in section 3.1.1.

3.1.1. Discrete Cosine Transformer: Discrete Cosine Transformer (DCT) is a function used in visual secret sharing of video frames in an image. DCTCC mechanism transforms a signal from spatial domain to frequency domain for easier way of the data compression. The luminance value of Discrete Cosine Transformer spatially high frequency video fame is computed as,

$$DCT[Video\ Frame\ (x,y)] = \frac{4C(x)C(y)}{n^2}\sum_{i=0}^{n}\sum_{j=0}^{n} f(i,j)Cos[\frac{(2i+1)x\pi}{2n}]Cos[\frac{(2j+1)y\pi}{2n}] \quad (1)$$

Discrete Cosine Waveform based luminance value measure takes the frame of the 'x' and 'y' coordinates. The coordinates of the '4' directions are computed using the cosine formula 'Cos' where 'i' and 'j' are the pixels of video frame sequences. The luminance value can be easily identified from (1). The visual secret sharing with this luminance value provides high lossless video compression.

In order to perform efficient compression of videos using Discrete Cosine Transformer, the video is divided into '$m * m$'form of frame blocks. The video secret shared frame blocks are transferred at the receiver end using the transformed coefficients. From the left top coefficients of the frame a zigzag permutation is employed in the DCTCC mechanism to embed the secret video sequence. The zigzag permutation helps to easily embed the video sequence of variable frame length. The zigzag procedure based visual secret sharing of the video frames in image is shown in Figure 3 as,

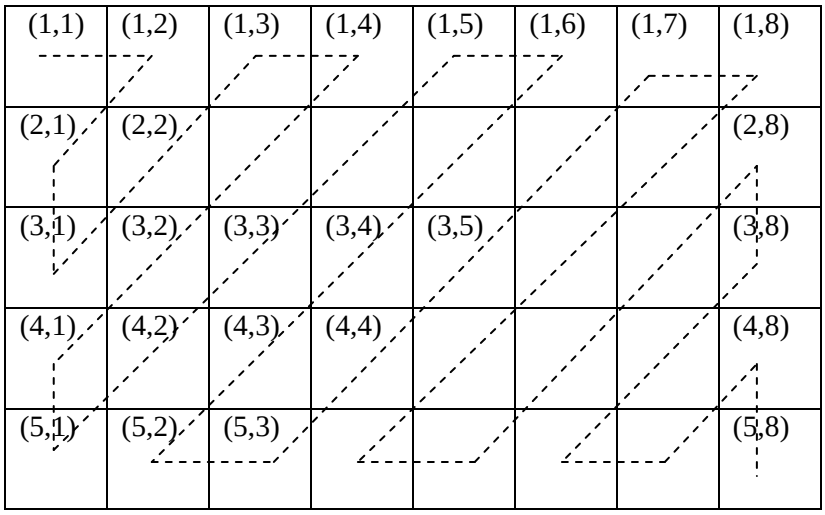

Figure 3. Video Frame Embedding Procedure

Tuple with High Luminance value is described in DCTCC mechanism with different set of start and end pixel point on zigzag fashion. The tuple is formularized as,

$$Tuple = \{[(1,1),(2,1)],[(2,1),(1,3)],[(1,3),(4,1)],[(4,1),(1,5)],[(1,5),(5,2)],[(5,2),(1,7)],[(1,7),(5,4)],$$
$$[(5,4),(2,8)],[(2,8),(5,6)],[(15,6),(4,8)],\ [(4,8),(5,8)]\} \quad (2)$$

Let us assume that a set of the image which is visually secret with the video frames is illustrated. The video frame with the tuple values are clearly described in (2). The zigzag fashion based filling shows the pixel points in which videos are embedded. The chain

processes with zigzag fashion wise video embedded in DCTCC mechanism. Quantization procedure is employed in DCTCC mechanism to maintain the quality rate of video frame. The quantization process of the embedded video frame is described as,

$$Quantization = (\frac{x,y}{m}) * m \quad (3)$$

In (3), (x , y) is the pixel range of the video frame to be embedded and 'm' is the array of the prime notational embedded system. This computation helps to easily retain high quality of the embedded video frame during reconstruction. In DCTCC mechanism, quantization process is carried out through multiplicative and divisive process. The embedded image frame pixel is divided by prime 'm' notations in quantization process, and then the remainder value is calculated. The remainder value is multiplied again with the 'm' to regenerate high quality video frame after the embedding process in our proposed work.

3.2. Video Encrypted with Visual Cryptographic Procedure

Once the visual secret sharing of video sequence using discrete cosine transformer is completed, the design considerations to be followed in DCTCC mechanism is the process of video encryption with visual cryptographic procedure. On the visual secret shared video frame, visual cryptographic scheme is implemented to embed the key with the sender message. The encrypted key improves the security level in DCTCC mechanism. The visual secret shared version of the secret video with high lossless result, extend the work of the system with the chaos encrypted key properties. The chaos encryption key with discrete time interval of encoding is all briefed in the section given below.

3.2.1. Chaos Encryption Scheme: In order to improve the security level, enhanced RSA algorithm is employed with key properties to improve the video quality estimation strategy. Chaos based encryption works with differing length of video frame on discrete time interval. Discrete time interval of video frame is described as,

$$Discrete(t_n) = Videoframe(x,y)_{t_0} + Videoframe(x,y)_{t_1} \dots\dots\dots Videoframe(x,y)_{t_{n-1}} \quad (4)$$

t_0 -Initial time state on encrypting video frame.

t_{n-1} - Final time state on decrypting video frame

The non-linear form of dynamic set of video frame encryption on discrete time interval is computed. Choas has quasi randomness special properties on key formation in DCTCC mechanism. The discrete time interval computation helps to secure the secret message with visual cryptographic system and also fastens the decryption process that is carried out by the human (*i.e.*, user) visual system.

Begin
// Chaos Encryption Step
Step1: Video Frame 'f' is initially converted into the binary bit stream 'B'.

Step 2: Binary bit stream 'B 'takes the random key stream pseudo generator

Step 2.1: Pseudo generator key stream on the 'x' and 'y' coordinate is shown as,

Step 2.2: $x_{i+1} = 1 - kx_i^2 + y_i$, x coordinate key encryption

Step 2.3: $y_{i+1} = kx_i$, y coordinate key encryption

Step 3: Two Dimensional Cover Image with the encrypted key in a non-liner form
// Enhanced RSA
Step 4: Generate the random key with 'm' prime property

Step 5: $Encryption = K(Videoframe(x, y)_{t_1})$

Step 6: Compute Quantization for improving Quality of video frame
End

Video frame is initially converted into the binary bit stream. This binary bit stream introduces a random key stream pseudo generator. In chaos encryption, the key properties are enhanced with RSA procedures in DCTCC mechanism. The pseudo generator (x, y) pixel contains the 'key' with that visual quality of video sequence frames.

The public key is encrypted and sends to the receiver end for the decryption process. On the receiver side, the private key is submitted by every user to authenticate and decrypt the message (*i.e.*, video sequence of frames). Enhanced RSA algorithm offer higher safety rate with chaos mapping form of encryption in DCTCC mechanism and this mapping using the public and the private keys.

3.2.2. Chaos Decryption Scheme: On the decryption side, the chaos method in DCTCC mechanism is applied in the reverse procedural order to fetch the visual quality of video frames from the original image. The decryption side uses the human visual private key to obtain the original message. The decryption message part first implies the reverse process of enhanced RSA. RSA helps to fetch the key properties. Then the pseudo random reverse generation is carried out. Finally, the binary bit is converted into video frame. Video frame which contains visual secret sharing of video is reversed from the cover image.

4. Experimental Evaluation

Discrete Cosine Transform Chaos Cryptographic Video Frame (DCTCC) mechanism performs the experimental in JAVA platform. The JAVA platform takes the video from the Robe Safe Driver Monitoring Video Dataset (RS-DMV). RS-DMV dataset is a set of video sequences of drivers taken in the camera which is positioned on the dashboard. The dataset currently enclose 10 video sequences which contain occlusions, changes in illumination and other process. These video sequences improve the security level. The video sequence is developed with visual cryptographic techniques.

The encrypted key properties are used to encrypt the video frames and this algorithm is compared with the existing system such as Two-pass Rate Control (TRC) [1] method for H.264 VBR coding and Accelerated Sequence Matching (ASM) [2] method on video sequences. Frames are recorded in gray-scale, at 30 frames per second, and stored as RAW video. Frame size of outdoor videos is 960x480 pixels, and 1390x480 for indoor videos. Each frame has a header, indicating frame #, capture time, size with other related information. Experiment is conducted on factors such as efficiency of visual secret sharing of video frame on images, mean square error rate, and secret video sharing efficacy level, encryption time.

The Mean Square Error (MSE) rate in DCTCC mechanism measure how close a video quality is to data points. For every data point, we obtain the distance vertically from the point to the corresponding y coordinate on the curve fit (the error), and square the value. Then we add up all those coordinate values for all data points, and divide by the number

of points minus two. The smaller the Mean Square Error rate, the closer the fit is to the data and therefore more efficient the method is. It is measured in terms of percentage (%).

$$MSE = \frac{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}{n} \quad (5)$$

The secret video sharing efficacy level measures the ratio of sent video frame to the amount of received video frame. Higher the secret video sharing efficacy level, more efficient the method is. The secret video sharing efficacy level is measured in terms of megabytes per second (Mbps)

$$Efficiency = \sum_{i=1}^{n} \frac{Received\,(f_i(x_i y_i))}{Sent\,(f_i(x_i y_i))} \quad (6)$$

Encryption time for DCTCC mechanism is the time taken to encrypt the video frames at discrete time intervals. The encryption time using DCTCC mechanism is shown below. It is measured in terms of milliseconds (ms).

$$ET = \sum_{i=1}^{n} Time\,(Video\ frame\,(x, y)t_i) \quad (7)$$

5. Results Analysis Of Dctcc Mechanism

Discrete Cosine Transform Chaos Cryptographic Video Frame (DCTCC) mechanism is compared against the existing Two-pass Rate Control (TRC) [1] method for H.264 VBR coding and Accelerated Sequence Matching (ASM) [2] method on video sequences. Table 1 evaluates the Mean Square Error rate in terms of percentage achieved with different number of frames ranging from 5 to 35 and comparison is made with the two existing methods namely, Two-pass Rate Control (TRC) [1] and Accelerated Sequence Matching (ASM) [2].

Table 1. Tabulation for Mean Square Error Rate

No. of frames	Mean Square Error rate (%)		
	DCTCC	SUP	ADPN-LP
5	35.38	40.41	47.44
10	39.44	44.47	51.50
15	43.56	48.59	55.62
20	48.22	53.25	60.28
25	45.78	50.81	56.84
30	51.33	56.36	63.39
35	46.55	51.58	57.61

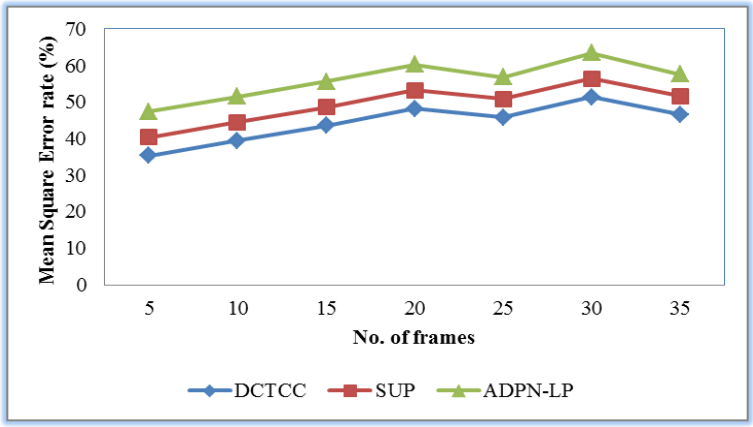

Figure 4. Measure of Mean Square Error Rate

Figure 4 describes the mean square error rate based on the number of frames using RobeSafe Driver Monitoring Video Dataset. The mean square error rate for each number of frames placed by the user is measured with the video quality to data points. From the figure it is evident that the mean square error rate using the proposed mechanism is comparatively lesser than the two other existing methods. This is because by applying the Discrete Cosine Transformer on the frames the visual secret video sharing is enhanced reducing the mean square error rate in DCTCC mechanism by 9 – 14 % compared to SUP. In addition, the Discrete Cosine Transformer takes the luminance values for providing high lossless compression further decreasing the mean square error rate by 23 – 34 % compared to ADPN-LP.

Table 2. Tabulation for Secret Video Sharing Efficacy Level

No. of frames	Secret video sharing efficacy level (Mbps)		
	DCTCC	SUP	ADPN-LP
5	63.88	58.85	50.81
10	68.75	63.72	55.68
15	71.34	66.29	58.21
20	74.88	69.83	61.75
25	70.29	65.24	58.16
30	78.35	73.30	65.22
35	81.44	74.39	60.31

Table 2 represents the comparison results of secret video sharing efficacy level and performance with 35 frames considered for experimental purpose.

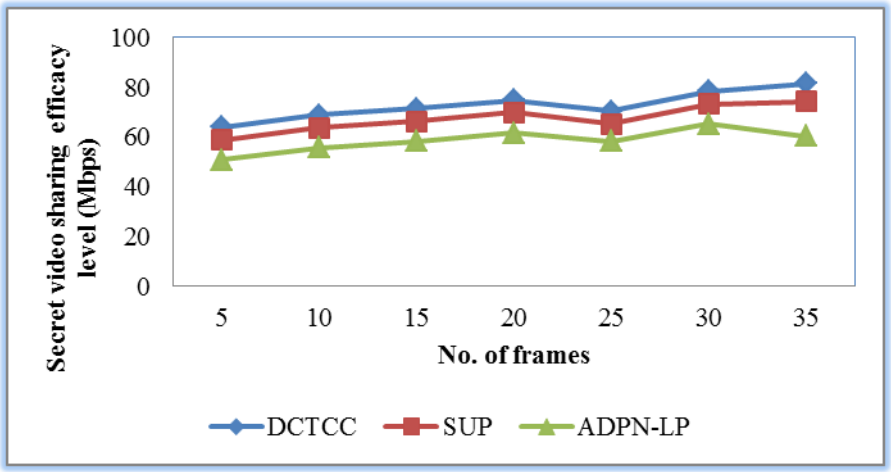

Figure 5. Measure of Secret Video Sharing Efficacy Level

Figure 5 shows the secret video sharing efficacy level of DCTCC mechanism, SUP, ADPN-LP for 5 to 35 considered frames. The performance of all secret video sharing efficacy level is improved as the number of frames increases though minimizes for 25 frames considered. But comparatively, the secret video sharing efficacy level is increased in the proposed DCTCC mechanism than when compared to two other methods. For example, for frame size of f = 20, the percentage secret video sharing efficacy level improvements of DCTCC mechanism over SUP [1] and ADPN-LP [2] are on the order of 8.65 percent and 25.94 percent respectively. This is because different types of non-linear dynamic set of video frames from users are identified using the chaos based encryption key properties in DCTCC mechanism and therefore increases the chance of secret video sharing efficacy level by 6 – 8 % compared to SUP. In addition, with the discrete time

dynamical video cryptographic system using the enhanced RSA key properties the ratio of sent video frame to the amount of received video frame is entirely increased resulting in the increase of secret video sharing efficacy level using DCTCC mechanism by 16 – 25 % compared to ADPN-LP respectively.

Table 3. Tabulation for Encryption Time

No. of frames	Encryption time (ms)		
	DCTCC	SUP	ADPN-LP
5	0.135	0.146	0.157
10	0.149	0.160	0.171
15	0.154	0.165	0.176
20	0.150	0.161	0.176
25	0.163	0.174	0.185
30	0.155	0.166	0.177
35	0.152	0.163	0.174

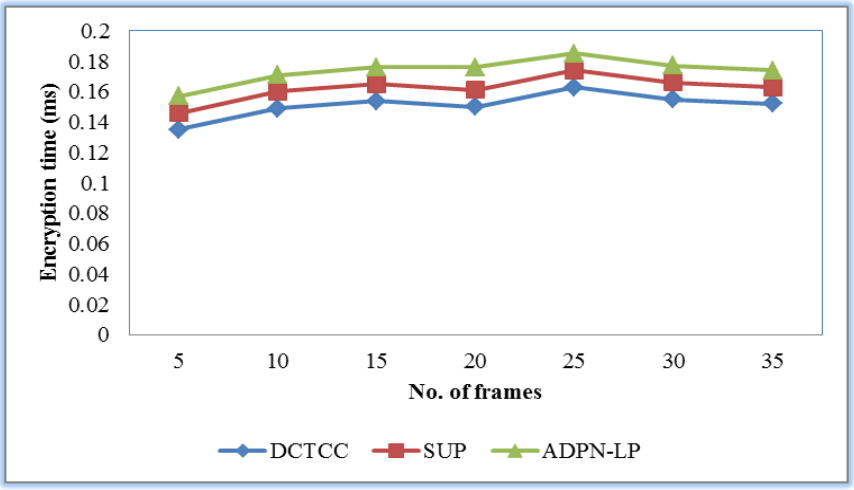

Figure 6. Measure of Encryption Time

Table 3 and figure 6 shows the encryption time on analyzing the RobeSafe Driver Monitoring Video Dataset data using the proposed DCTCC mechanism and comparison is made with two other methods with different number of frames considered. The experimental results show that the encryption time on analyzing differing video frames of DCTCC mechanism is lower than that of SUP [1] and ADPN-LP [2] respectively. This is because of the fact that the quantization procedure applied in DCTCC mechanism helps in maintains the quality rate of video frame being sent to the receiver using the Tuple with High Luminance value resulting in minimization of encryption time by 6 – 8 % compared to SUP. Furthermore, chaos encryption key with the discrete time interval of encoding using enhanced RSA algorithm takes the random key stream pseudo generator resulting in decreasing the encryption time using DCTCC mechanism by 13 – 17 % compared to ADPN-LP respectively.

6. Conclusion

A Discrete Cosine Transform Chaos Cryptographic (DCTCC) mechanism for improving the quality of visual secret video sharing scheme is presented. This mechanism has been designed to enhance the security level of different level video frame using the encryption key properties. We adopt Discrete Cosine Transformer to improve the quality

of visual secret video sharing scheme using tuple with high luminance value. Next, a visual cryptographic technique using chaos based encryption properties is designed to increase the encrypted embedded video frame to perform the secret sharing. The proposed DCTCC mechanism uses the non-linear form of dynamic set of the video frame encryption on discrete time interval to reduce the encryption time on the side of the user. In addition, the zigzag permutation process in DCTCC mechanism helps to easily embed the video sequence of variable frame length at less time and therefore reduces the encryption time. Experimental evaluation is conducted with RobeSafe Driver Monitoring Video Dataset which is positioned on the dashboard to improve the evaluation and measured the performance in terms of mean square error rate, decryption time and secret video sharing efficacy level on analyzing differing video frames of different sizes. Performance results reveal that the proposed DCTCC mechanism provides higher secret video sharing efficacy level and data prediction rate and also strengthen the overall mechanism by consuming encryption time for RobeSafe Driver Monitoring Video Dataset. Compared to the existing methods, the proposed DCTCC mechanism outperforms the state-of-art works in terms of encryption time, mean square error rate of efficiency of the system.

References

[1] J. Sun, Y. Duan, J. Li, J. Liu and Z. Guo, "Rate-Distortion Analysis of Dead-Zone Plus Uniform Threshold Scalar Quantization and Its Application—Part II: Two-Pass VBR Coding for H.264/AVC", IEEE Transactions on Image Processing, vol. 22, no. 1, January **(2013)**.
[2] M. C. Yeh and K. T. Cheng, "Fast Visual Retrieval Using Accelerated Sequence Matching", IEEE Transactions on Multimedia, vol. 13, no. 2, April **(2011)**.
[3] A. Pande and J. Zambreno, "A chaotic encryption scheme for real-time embedded systems: design and implementation", Springer, June **(2011)**.
[4] D. James and M. Philip, "A Novel Security Architecture for Biometric Templates using Visual Cryptography and Chaotic Image Encryption", Eco-friendly Computing and Communication Systems Communications in Computer and Information Science, Springer, vol. 305, **(2012)**, pp. 239-246.
[5] V. Petrauskiene, A. Survila, A. Fedaravicius and M. Ragulskis, "Dynamic visual cryptography for optical assessment of chaotic oscillations", Optics & Laser Technology, Elseiver, October **(2013)**.
[6] U. Park, J. Park and A. K. Jain, "Robust Keypoint Detection Using Higher-Order Scale Space Derivatives: Application to Image Retrieval", Journal of IEEE Signal Processing Letters, vol. 20, no. 10, **(2014)**, pp. 30.
[7] S. Kumar, V. Singh, G. Singh and A. Jhaldiya, "The Proposed Algorithm: Image Security Technique in Visual Cryptography: (IST-VC)", Open Journal of Computer Sciences, vol. 1, no. 1, May 1-6, **(2013)**.
[8] F. Liu, C. Wu and X. Lin, "Step Construction of Visual Cryptography Schemes", IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, March **(2010)**.
[9] F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis and D. Hatzinakos, "Fuzzy Key Binding Strategies Based on Quantization Index Modulation (QIM) for Biometric Encryption (BE) Applications", IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, March **(2010)**.
[10] A. Rudder, W. Goodridge and S. Mohammed, "Using Bias Optimization for Reversible Data Hiding Using Image Interpolation", International Journal of Network Security & Its Applications, vol. 5, no. 2, March **(2013)**, pp.65.
[11] Q. Ding, L. Wang and G. Chen, "Correlative Peak Interval Prediction and Analysis of Chaotic Sequences", Journal of Networks, vol. 6, no. 7, July **(2011)**.
[12] P. Hongal and Dr. S. L. Deshpande, "Policy Based Chaotic Cryptography: A Hybrid Approach", International Journal of Emerging Trends and Technology in Computer Science, vol. 1, no. 3, September–October **(2012)**.
[13] J. Kaur and R. Rajput, "A Review Paper on Data Embedding in Scrambled Digital Video for Data Security & Authentication", International Journal Of Engineering And Computer Science ISSN, vol. 3, no. 10, October **(2014)**, pp. 2319-7242.
[14] P. Karthik, P. S. Ranjith and M. Jayaganesh, "SCCE: secure communication based on a chaotic system for modern wireless communication", International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN(E): 2321-8843; ISSN(P): 2347-4599, vol. 2, no. 3, March **(2014)**, pp. 163-172.
[15] S. A. M. Al-Taweel, P. Sumari, S. A. K. Alomari and A. J. A. Husain, "Digital Video Watermarking in the Discrete Cosine Transform Domain", Journal of Computer Science, vol. 5, no. 8, **(2009)**, pp. 536-543.

[16] K. Thaiyalnayaki and R. Dhanalakshmi, "A Chaos Encrypted Video Watermarking Scheme for the Enforcement of Playback Control", International Journal of Advances in Engineering & Technology, July **(2012)**.
[17] G. Chopra and A. K. Pal, "An Improved Image Compression Algorithm Using Binary Space Partition Scheme and Geometric Wavelets", IEEE Transactions on Image Processing, vol. 20, no. 1, January **(2011)**.
[18] V. Thirumalai and P. Frossard, "Distributed Representation of Geometrically Correlated Images with Compressed Linear Measurements", IEEE Transaction on Image Processing, **(2012)**.
[19] P. K. SharmaÁ and H. M. SinghÁ, "Visual Cryptography Scheme for Gray Scale Images based on Intensity Division", International Journal of Current Engineering and Technology, vol. 4, no. 1, February **(2014)**.
[20] A. Mohanan, R. Remanan, Dr. S. B. Suvanam and Dr. Kalyankar N. V., "Audio-Video Steganography Using Forensic Technique for Data Security", International Journal of Computer Engineering & Technology (IJCET), vol. 5, no. 12, December **(2014)**, pp. 154-157.

