A Video Encryption and Decryption using Different Techniques

Khushwinder Kaur
M. Tech Scholar
GZSCEET, Bathinda

Swati Bansal
Assistant Professor
GZSCEET, Bathinda

ABSTRACT
Inside the current years with the development of internet technologies, video technology were widely used in television, conversation and multimedia, so protection is required on video statistics. although a good deal video encryption method has been develop however no longer provide so much performance in terms of encryption and decryption technique. a method for embedding records in scrambled AVI video is described. The embedding method is applied to the video collection collectively with the video scrambling set of rules. in this paintings extraordinary forms of clippers are used to process the encryption and decryption. In an increasing number of image and video processing issues, cryptographic techniques are used to implement content material get admission to manage, identity verification and authentication, and privacy safety. every other category of algorithms is based totally on scramble (permutation) best methods, wherein the DCT coefficients are permuted to offer confusion. Their isn't any authentication and protection in this and circulation chipper is used which eat extra time to technique the video and frame technology isn't used which provide protection and authentication to the person. i have also reviewed DCT technique for encryption and decryption this is implemented in my studies paintings and specific parameters are calculated. We are getting the accuracy 92% in the shape of PSNR in case of DCT. Becase it's far offering the compression additionally.

Keywords
Multimedia security, contents access control, video scrambling etc .

1. INTRODUCTION
Due to rapid development of various multimedia technologies, more and more multimedia information are generated and transmitted in the clinical, industrial, and navy fields, which may additionally consist of a few touchy records which must not be accessed by using or can handiest be partially uncovered to the general users. consequently, protection and privateness has grow to be an crucial. the primary aim of cryptography is keeping data secure form unauthorized attackers. consequently statistics is encrypted via process of Encryption. facts cryptography in particular is the scrambling of the content of facts, including textual content, image, audio, video and so on to make the facts unreadable, invisible or unintelligible in the course of transmission or storage known as Encryption. The opposite of statistics encryption is facts Decryption, which recuperate the unique information. The opposite of statistics encryption is statistics decryption With digital video transmission, encryption technologies are wished which could protect digital video from attacks all through transmission. due to the large length of digital movies, they may be normally transmitted in compressed codecs such as MPEG. since the cryptography first recognised usage in historical Egypt it has exceeded thru unique degrees and become affected by any important occasion that affected the way human beings treated data. within the global conflict II for example cryptography performed an vital role and become a key element that gave the allied forces the top hand, and enables them to win the battle faster, after they had been capable of dissolve the Enigma cipher system which the Germans used to encrypt their navy secret communications. In cutting-edge days cryptography is no longer restrained to relaxed sensitive army facts but identified as one of the predominant additives of the safety coverage of any corporation and considered industry wellknown for supplying statistics protection, agree with, controlling get admission to to resources, and electronic economic transactions. The authentic records that to be transmitted or saved is referred to as plaintext, the one that can be readable and understandable both by someone or by way of a laptop. while the disguised statistics so-known as ciphertext, that is unreadable, neither human nor gadget can properly process it till it is decrypted. A machine or product that gives encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how easy or complex the encryption method can be, the vital software program issue, and the key (commonly an extended string of bits), which goes with the algorithm to encrypt and decrypt the facts. inside the 19th century, a well-known concept approximately the safety precept of any encryption machine has been proposed by Kerchhoff. This theory has end up the maximum vital principle in designing a cryptosystem for researchers and engineers. Kirchhoff found that the encryption algorithms are supposed to be recognized to the fighters. therefore, the safety of an encryption system have to rely upon the secrecy of the encryption/decryption key as opposed to the encryption set of rules itself. For despite the fact that in the very starting the opponent doesn’t recognise the algorithm, the encryption device will not be capable of defend the ciphertext as soon as the set of rules is damaged. the safety level of an encryption set of rules is measured by the dimensions of its key area. the larger length of the key space is, the extra time the attacker needs to do the exhaustive search of the key area, and for this reason the better the safety stage is. In encryption, the secret is piece of records (cost of include a large collection of random bits) which specifies the unique transformation of plaintext to ciphertext, or vice versa in the course of decryption. Encryption key based on the keyspace, that is the range of the values that may be used to collect a key. the larger key area the more feasible keys can be built (these days we generally use key sizes of 128,192,or 256 bit , so the important thing size of 256 might provide a 2256 key space).

2. ENCRYPTION AND DECRYPTION METHOD

The system of converting plaintext to ciphertext is known as enciphering or encryption, restoring plaintext from ciphertext is decoding or decryption. each the encryption and decryption algorithms take a key (k) and plaintext/ciphertext as input. in the case of pix, plaintext is a hard and fast of pixel values arranged in an orderly manner. Encrypting photos/movies constitutes reordering these pixel values in order that they bring no visual statistics approximately the original photo. An photograph/video also can be encrypted within the compressed area. The DCT coefficients are encrypted in this sort of manner that the content is made illegible for the unauthorized. most effective a licensed person can get again the original content material using the decryption set of rules. In cryptography, a block cipher is a symmetric key cipher which operates on fixed length groups of bits, termed blocks, with an unvarying transformation. whilst encrypting, a block cipher might take an n-bit block of plaintext as enter and output a corresponding n-bit block of ciphertext. the exact transformation is managed the usage of a 2d input the secret key. Decryption is similar, takes an n-bit block of ciphertext together with the name of the game key and outputs the unique n-bit block of plaintext. Examples of block- ciphers are RC5, AES, DES. A block cipher operates in exclusive modes. The main modes are digital Code book (ECB) and Cipher- Block Chaining (CBC). In ECB mode, the plaintext is split into blocks and each block is encrypted one at a time. in the CBC mode, each block of plaintext is XOR with the previous ciphertext block before being encrypted. This way, every ciphertext block is dependent on all plaintext blocks processed up to that point. in this mode, adjustments within the plaintext propagate all the time in the ciphertext and encryption can't be parallelized. also, decryption can't be parallelized.

3. PROCESS OF DATA HIDING IN ENCRYPTED VIDEO

The amount of digital pictures/video has elevated hastily on the net. photo/video protection turns into more and more crucial for plenty packages, e.g., secure transmission of photograph and video , army and clinical applications. as an example, pace and comfortable transmission is vital in the clinical world. in recent times, the transmission of photo/movies is a each day ordinary and it's miles necessary to discover an green manner to transmit them over networks. The protection of this multimedia records may be accomplished with encryption or records hiding algorithms. within the current developments of the sector, the technologies have advanced so much that maximum of the people select the use of the net as the number one medium to switch information from one cease to some other. there are numerous feasible ways to transfer records the usage of the internet: thru emails, chats, and so on. The information transmission is made very simple, velocity and correct the usage of the net. but, one of the essential troubles with transmitting facts over the internet is the security risk it poses i.e. the private or exclusive statistics may be stolen or hacked in lots of approaches. consequently it's miles very important to take records safety into consideration, as it's far one of the maximum essential elements that need interest at some point of the procedure of records transmission. information safety essentially manner safety of information and presenting excessive protection to prevent data amendment from unauthorized users or hackers. statistics protection has won greater interest within the latest time frame because of the big increase in records switch rate over the internet. Separable Reversible records embedding is a delicate method. whilst the embedded picture/video is manipulated, the decoder will discover it isn't true and accordingly there can be no unique content material healing . A commonplace approach of excessive potential separable reversible records embedding is to pick out an embedding vicinity in an image/video, and embed both the payload and the unique values in this place . As the amount of information needed to be embedded is bigger than that of the hiding area, and the space saved from compression might be used for embedding the payload. DE technique has been used to discover more garage space by using exploring the redundancy inside the picture content. J. Tian employ the DE method to reversibly embed a payload into digital pictures [1]. both the payload potential restriction and the visible pleasant of embedded pix of the DE technique are a few of the great with a low computational complexity. N. Memon have offered an interactive purchaser–supplier protocol for invisible watermarking wherein the vendor does not get to recognize the exact watermarked reproduction that the customer gets [6]. but, incase the seller finds an unauthorized reproduction, become aware of the consumer from whom this unauthorized copy has originated and moreover additionally prove this reality to 0.33-birthday celebration.

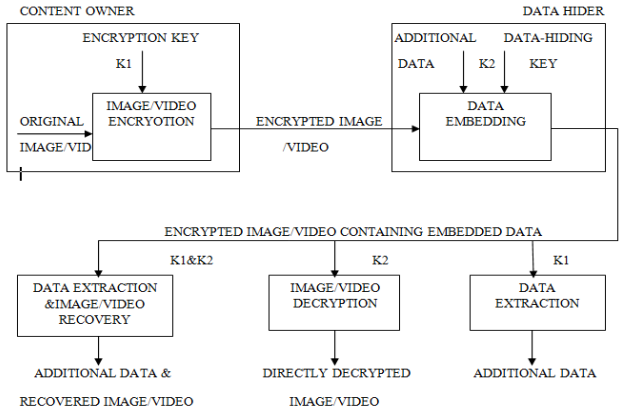

Figure 1.: Sketch of separable reversible data hiding in encrypted video.

4. PROBLEM FORMULATION

In more and more photo and video processing issues, cryptographic strategies are used to put into effect content material get admission to manipulate, identification verification and authentication, and privacy safety. any other class of algorithms is based on scramble (permutation) most effective strategies, wherein the DCT coefficients are permuted to offer confusion. Their is not any authentication and protection on this and flow chiper is used which devour extra time to process the video and body generation is not used which offer protection and authentication to the user. The data protection problem arise all through the remodel of the facts whilst the data is moved from supply to destination. The RGB color distortation problem. Processing time trouble were for the duration of the statistics scrambling. We advise a computationally green and at ease video encryption logarithm. With a few decided on parameters (interpreting time, PSNR fee ,MSE fee) This makes comfy video encryption feasible for actual-time applications without any greater committed hardware.

5. RESEARCH METHODOLOGY OVERVIEW

This consists of the facts of method and algorithm of the work this is used to layout the information scrambling for the virtual video. additionally it is the gear which can be used to design the GUI for studies work.

This is for video encoding. it is based totally upon GUI (graphical consumer interface) in MATLAB. It is an effort to similarly grasp the basics of MATLAB and validate it as a effective utility tool. There are basically specific documents. every of them includes m-document. those are the programmable files containing the information approximately the video associated statistics.

PROPOSED ALGORITHM

Step 1: Start the program.

Step 2: Reads the video and stores it as a image files in a folder

Step 3: Calculate the Frame separation and Convert Frame to image file.

Step 4: Write image file.

Step 5: Apply the DCT and Huff transformation technique encoding the video stream after the frame separation.

Step 6: Generate the Hexadecimal key for encryption.

Step 7: Apply decryption to decrypt the frames of the video.

Step 8: Apply the decoding process on video.

Step 9: Apply the encoded frame and decoded frame to check for authentication and validation.

Step 10: PSNR and MSE values and decoded time.

Step 11: Stop.

6. RESULT & ANALYSIS

This Chapter shows the implementation results of the dissertation work. Their are different figures that shows how the video is processed and how the system tools works in MATLAB.In this we upload the digiat video.

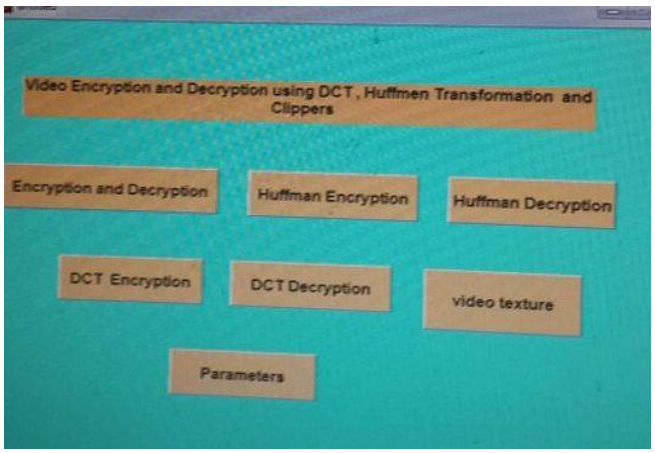

Figure 2: Input GUI window

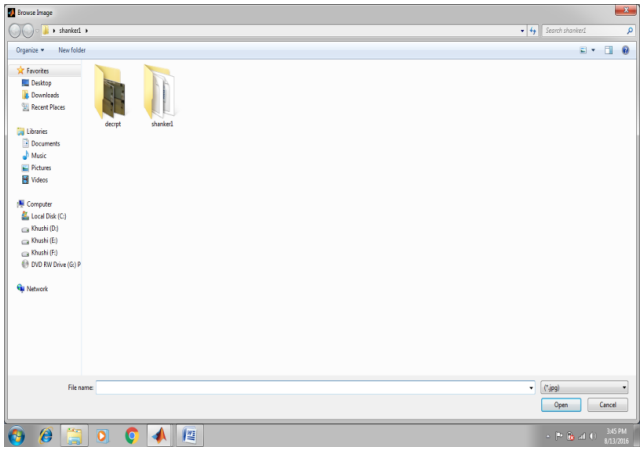

Figure 3: : Browsing the Input video

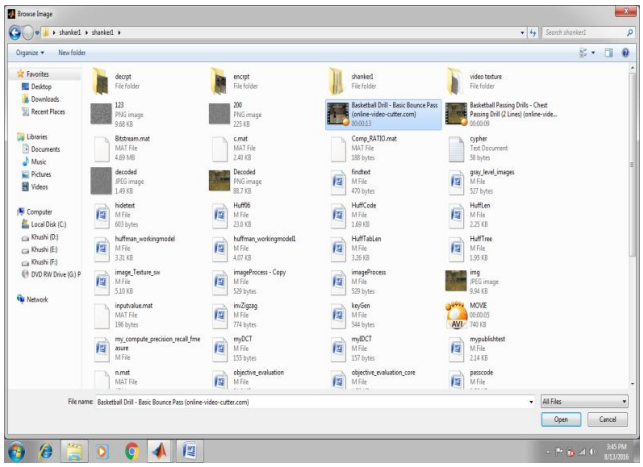

Figure 4:. Input Video Browsing

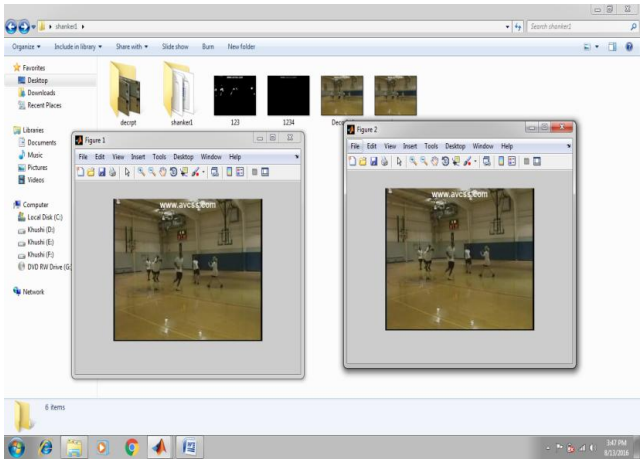

Figure 5. Simple Encryption and Decryption video

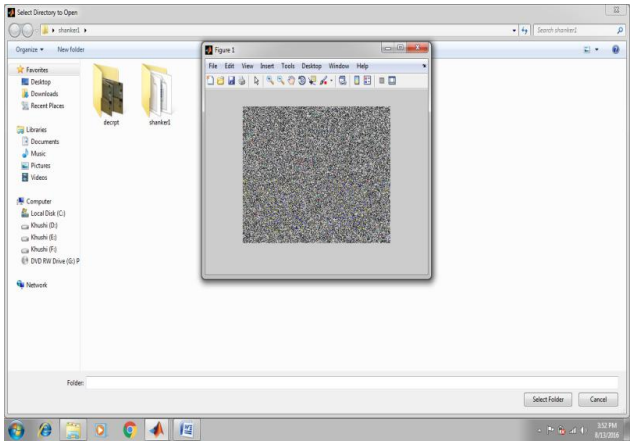

Figure 6. Encoded Frame

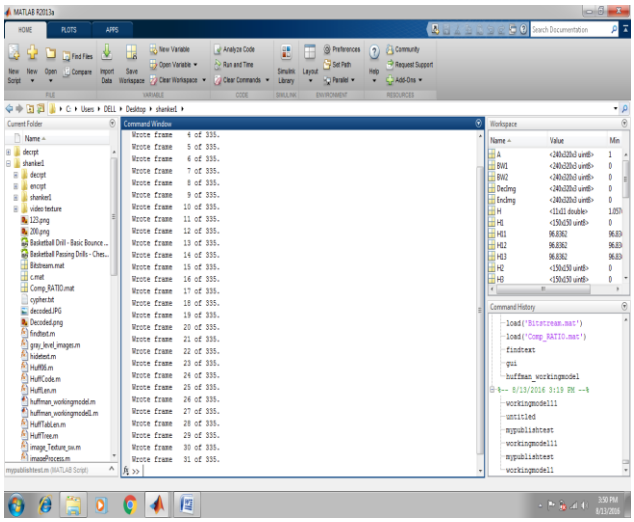

Figure 7. Video Frame Processing

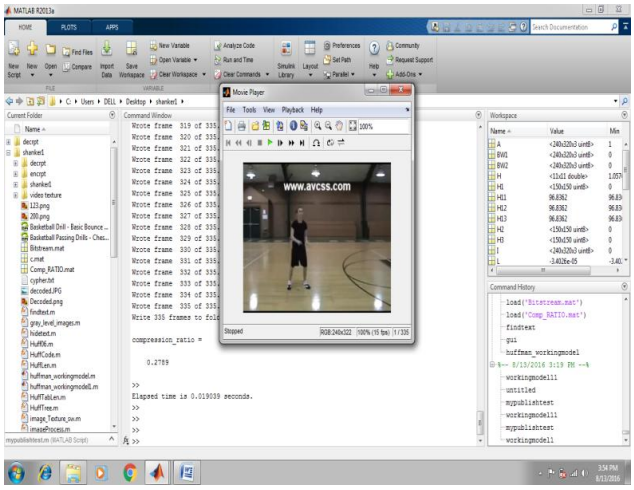

Figure 8: Input Second Video

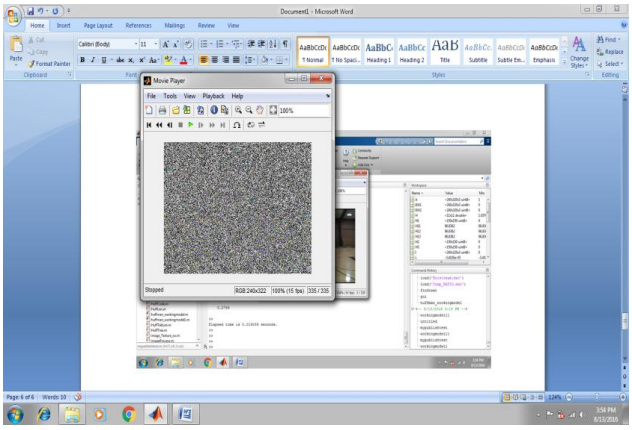

Figure 9: Encoded Video with frames

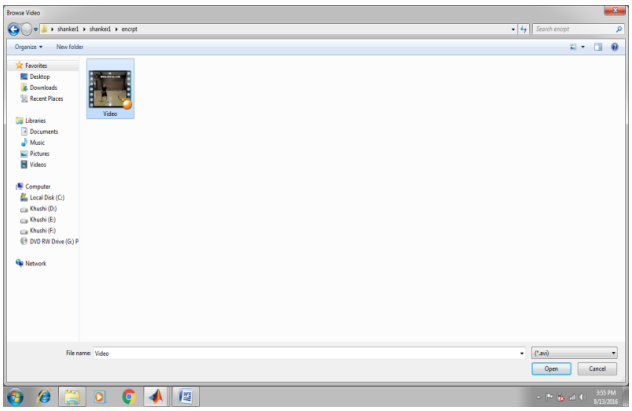

Figure 10:Browse the Encrypted video for decryption

Figure 11. Decrypted Frame with DCT

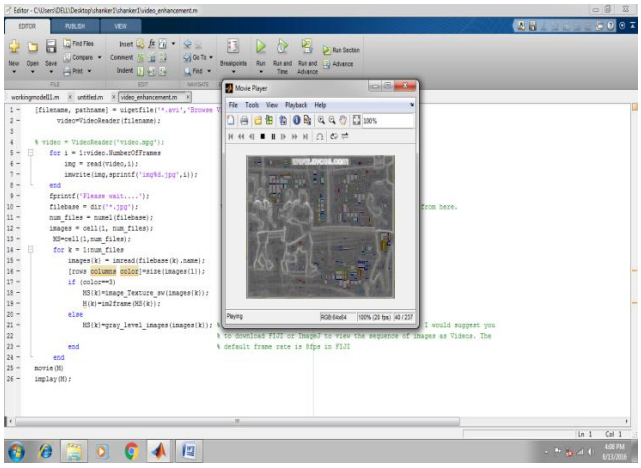

Figure 12:Taxture video processing

Table .1 Huffman Parameter table

Name of Video	PSNR	SSIM	LSS
Basketball	0.97240	0.9394	0.0048
Basketball Drill	0.72753	0.9294	0.0046
Mall	0.8045	0.9014	0.0042
Kimono (B2)	0.8563	0.8214	0.0040
Vidyo1 (E)	0.9021	0.9141	0.0045

Table 2. DCT Parameter Table

Name of Video	PSNR	SSIM	LSS
Basketball	0.79417	0.9289	0.0047
Basketball Drill	0.98022	0.7564	0.0041
Mall	0.94631	0.8540	0.0040
Kimono (B2)	0.85041	0.9102	0.0042
Vidyo1 (E)	0.96243	0.9214	0.0038

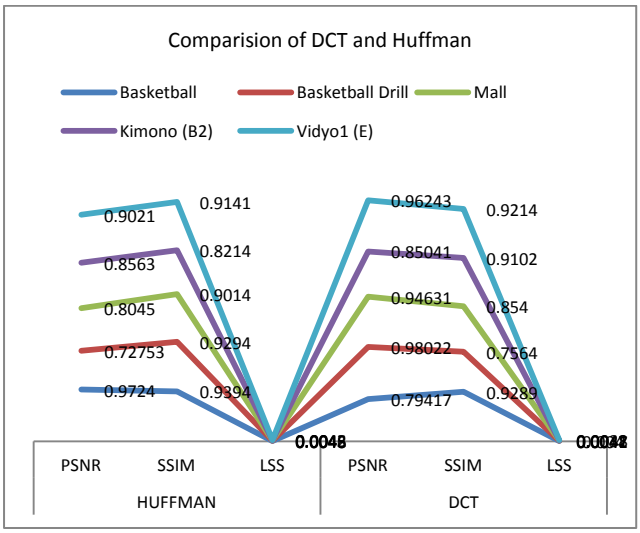

Table 3. Techniques Comparision

Author Name/ Year	Technique Used	Algorithm	Result
Preeti Gupta (2012)	DWT	encryption XOR operation	it increases the security of watermarks
Yogita Negi (2013)	selective encryption	Zig-Zag Permutation Algorithm	It is providing result on I frmae of the video.
Ci-Lin Li (2014)	Encryption scheme	H.264/SVC	They are getting 52% results only on encryption
A.Shiva Krishna Reddy (2014)	Grouping Of Pictures (GOP) Encryption	thresholding method	İt is providing the 2-D videos information and getting result 60%.
Sivakami, R. (2014)	discrete cosine transform	watermarking algorithm	It is providing the compressiona encryption and geting result 35%.
Benoˆıt Boyadjis (2015)	Selective Encryption	Scrambling algorithm	It is mainly providing the security and getting the accuracy 60 % in the form of PNSR.
Proposed	Selective Encryption with Huffman and DCT	Encryption and Decryption	In the proposed work i have used the Huffman Technique and DCT with different types of Clippers. It is the new work because everybody is doing work with DCT and Huffman Sepratelly and Clipper Seprately ,But i have Using the Combination of Clippers and DCT and Huffman. We are getting the accuracy 92% in the form of PSNR in case of DCT. Becase it is providing the compression also.

7. CONCLUSİON

This concludes the paintings on this dissertation in phrases of the various parameters that have been taken into consideration at the same time as scrambling the digital video for security.The implementation information show us the complexity worried in the actual time software and hardware implementation. the focus of this paintings is statistics scrambling in digital video. The reality that the proposed technique embeds the data without delay within the spatial area (pixel values) makes it proof against some very common mistakes, which seem in different competitive facts hiding

strategies running in the compressed area, such as artifacts and waft. Artifacts are produced by using the information hiding techniques, which use the transform coefficients for you to embed the information. Remodel coefficient modification consequences in video reconstruction errors with undesirable visible effects, including discontinuities inside the block edges. flow errors are propagating visible distortions between successive video frames as a result of embedding records inside the compressed area without re-performing movement estimation. The image compression strategies and de-blocking filter are also crucial inside the video compression strategies, but motion estimation and movement compensation are the most computationally luxurious and time consuming process in complete video compression technique. The excessive definition video has very high temporal redundancy inside the consecutive frames. This temporal redundancy may be eliminated with speedy motion seek algorithms, and movement reimbursement. This process keeps only required records within the frames and forwards to other video compression blocks. The entropy coder outputs low bit charge records as compared to the previously evolved requirements with identical video first-rate. In conclusion, the main advantages of the proposed technique are its low complexity and the opportunity of the usage of the compressed move for hiding exceptional information normally, with out first interpreting after which re-encoding the video sequence. This makes the method appropriate for real-time programs. Simulation results have proven that perceptual fine is preserved without sacrificing coding efficiency.

8. FUTURE WORK

Destiny paintings might involve a actual time implementation of the machine in order that the maximum quantity of videos is more advantageous with the help of various filters. in the future work DWT is carried out with tough and soft threshold for statistics scrambling in digital motion pictures authentications and safety.

9. REFERENCES

[1] Ci-Lin Li, Chih-Yang Lin, and Tzung-Her Chen " Efficient Compression-Jointed Quality Controllable Scrambling Method for H.264/SVC ", International Journal of Network Security, Vol.16, 2014 .

[2] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar " Fast and Secure Real-Time Video Encryption", IEEE 2008.

[3] A.Shiva Krishna Reddy ,K. Srimathi, R. Rajalakshmi, " The Indexing Algorithm for Scrambled Frames in Video Encryption " International Journal of Advanced Research in Computer Science and Software Engineering Volume 4,February 2014.

[4] G.Madhuri, B.VijayKumar, V. Sudheer Raja, M. Shasidhar "Data Embedding in Scrambled Digital Video for Security", Int. J. on Recent Trends in Engineering and Technology, Vol. 6, Nov 2011.

[5] Sivakami, R. Nagakrishnan, Ellammal "A Digital Watermarking System For Video Authentication using DCT ", Integrated Journal of Engineering Research and Technology (IJERT) Vol 01 Jan-Feb 2014.

[6] Wenjun Zeng1, Shawmin Lei, " Efficient Frequency Domain Selective Scrambling of Digital Video", IEEE 2002.

[7] Mayank Arya Chandra, Ravindra Purwar, Navin Rajpal,"A Novel Approach of Digital Video Encryption", International Journal of Computer Applications Vol 49, July 2012.

[8] M. Abomhara,, Omar Zakaria, Othman O. Khalifa, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, February, 2010.

[9] Amit Pande, Prasant Mohapatra, Joseph Zambreno," Using Chaotic Maps for Encrypting Image and Video Content", IEEE International Symposium on Multimedia, 2011.

[10] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based for Image Encryption", World Academy of Science, Engineering and Technology , 2007.

[11] Yogita Negi ,"A Survey on Video Encryption Techniques", International Journal of Emerging Technology and Advanced Engineering Vol 3, Issue 4, April 2013.

[12] Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, March 2011

[13] Preeti GuptA, " Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Vol 3, September 2012.

[14] Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, " Recent Advances in Multimedia Information System Security," International Journal of Computing and Informatics, Vol. 33, No.1, 2009

[15] J. Zhou, Z. Liang, Y. Chen, and O. C. Au, " Security Analysis of Multimedia Encryption Schemes based on Multiple Huffman Table," IEEE Signal Processing Letters, vol. 14, No. 3, 2007

[16] Sufyan T. Faraj Al-Janabi, Khalida Shaaban Rijab, Ali Makki Sagheer," Video Encryption Based on Special Huffman Coding and Rabbit Stream Cipher", Developments in E-systems Engineering 2011.

[17] Gulistan, R., & Muhammad, J. M ," Performance Comparison of Advanced Video Coding H.264 Standard with Baseline H.263 and H.263+ Standards", IEEE International Symposium on Communications and Information Technology, 2004.

[18] Zeghid, M., Machhout, M., Khriji, L., Baganne, ," A modified AES based algorithm for image encryption",. International Journal of Computer Science and Engineering, 2007.

[19] C. Shi and B. Bhargava, " Light Weight MPEG video Encryption Algorithm", in Proceeding of the International Conference on Multimedia, 1998.

[20] Chetan K.R, Raghavendra K " DWT Based Blind Digital Video Watermarking Scheme for Video Authentication", International Journal of Computer Applications Vol 4 August 2010.