Journal of Engineering and Applied Sciences 14 (11): 3690-3697, 2019
ISSN: 1816-949X
© Medwell Journals, 2019

Improved Joint Selective Encryption and Matrix Embedding Technique using Adaptive Block Size Coding in HEVC Standard

[1]P. Saravanan and [2]K.K. Thyagharajan
[1]Department of CSE-ICE, Manonmaniam Sundaranar University, Tirunelvel, India
[2]RMD Engineering College, Chennai, India

Abstract: Today, High Efficiency Video Coding (HEVC), developed by the ITU-T video coding experts group and ISO/IEC moving picture experts group is emerging as a potential video compression standard. HEVC or H.265 compared to H.264/AVC is primarily standardized to improve the compression ratio, so as to achieve an equivalent video quality. In HEVC, a joint selective encryption and data embedding technique is proposed where HEVC coding structure is separated into two groups. One is utilized for encrypting video content and the other for embedding data. However, the size of bit-streams for encrypted and data-embedded videos are increased significantly, since, the HEVC coding structure is not utilized. Therefore, in this study we have proposed an improved joint selective encryption and matrix embedding technique using block size coding decision model in H.265. In this approach, non-zero DCT coefficients are manipulated according to the transform block size in all frames. Here, matrix embedding is proposed in terms of large payloads for improving embedding efficiency and reducing coding complexity. The results obtained show that the proposed data hiding technique for H.265 provided highest embedding efficiency with reduced coding complexity.

Key words: High efficiency video coding, H.264/AVC, data hiding, coding block size, selective encryption, matrix embedding

INTRODUCTION

Cloud computing and mobile internet technologies are rapidly developing and these technologies utilize cloud for storing large amount of data. Yet potential cloud consumers are worried about the privacy and security of their data which restrict them from adopting cloud services. Therefore, factors such as cloud computing, security and privacy are to be highly improved, so as to improve cloud services (Xu *et al*., 2016). For a given cloud service, sensitive information are stored in encrypted form using encryption techniques. Then, a cloud provider is authorized for accessing the encrypted video signals. However, additional information is embedded into the encrypted video for tampering detection or ownership declaration. Hence, different data-hiding techniques are developed by many researchers to overcome such issues by directly applying these techniques in encrypted domain (Xu and Wang, 2014).

Data or information hiding is defined as a process of preventing a particular aspect of data by embedding information into a host medium thereby improving security without affecting its quality. Although, the general structure of data-hiding process does not depend upon the type of host media, the methods vary depending upon the nature of such media (Esen and Alatan, 2011). Data hiding in video sequences is performed based on bit-stream level and data level. In bit-stream level, the redundancies within the compression standards are exploited. Typically, encodershave various options during encoding and this freedom of selection is suitable for manipulation along with data hiding (Praveena and Deepa, 2013). However, these methods highly rely on bit-stream structure and hence, they cannot survive any conversion or transcoding. Therefore, bit-stream-type data-hiding methods are generally, proposed for fragile applications like authentication. On the other hand, data-level hiding methods are proposed for a broader range of applications as these methods are more robust to attacks.

Generally, various data-hiding techniques focus only on images. These methods that focus on images cannot be applied directly to video sequences, since, the structure of video coding is different from that of images. The most widely deployed video coding standard is H.264/AVC. Therefore, encrypted H.264/AVC streams are widely utilized for developing data-hiding schemes. The most significant video compression standard used now a days is High Efficiency Video Coding (HEVC) or

Corresponding Author: P. Saravanan, Department of CSE-ICE, Manonmaniam Sundaranar University, Tirunelvel, India

H.265. It is mostly utilized for doubling the data compression rate without degrading the video quality or for improving the video quality with equivalent bit rate (Sullivan *et al*., 2012). H.265 is developed according to the principles of H.264/AVC. However, coding for H.265 using selective encryption and data embedding methods such as odd-even embedding method is complex (Tew *et al*., 2016). Hence, in this study we have proposed matrix embedding for data hiding in encrypted H.265 videos to improve embedding efficiency and reduce coding complexity.

Literature review: Xu and Wang (2015) proposed data-hiding method for encrypted version of H.264/AVC videos. The proposed scheme was performed according to three processes: selective encryption, data embedding and data extraction. Here, Context Adaptive Binary Arithmetic Coding (CABAC) bin-strings were proposed for selective encryption using stream ciphers. Additional data was then, embedded into partially encrypted H.264/AVC videos by data hider based on the CABAC bin-string substitution method without plaintext access for video content. Data extraction was achieved either by encryption or by decryption process for adapting different applications. However, data-hiding techniques for compressed videos were not achieved.

Stutz *et al.* (2014) proposed a non-blind structure preserving substitution watermarking of H.264/CAVLC inter frames. This algorithm enables extreme watermark embedding efficiently using simple bit substitutions. The Motion Vector (MV) differences of non-reference frames were modified by bit substitutions. This algorithm was then used in different application scenarios where watermarking was required for preserving the length of the bit-stream units. Finally, the quality and robustness of this algorithm were evaluated.

Xu and Wang (2014) proposed an efficient Reversible. Data Hiding (RDH) method for encrypted H.264/AVC videos. In this method during H.264/AVC encoding, MV difference and the sign bits of residue coefficients were encrypted using a standard stream cipher. Then, a data-hider was used which may reversibly embed the secret data into the encrypted H.264/AVC video by modified histogram shifting method. The embedding zone was selected by scale factor in order to satisfy various capacity requirements. In addition with an encrypted videocontaining hidden data, data extraction was performed either in encryption or decryption mode. However, this method has low embedding rate.

Li *et al.* (2012) developed reference index-based H.264 video watermarking method for improving the robustness of encryption. In this method, watermark was embedded in the reference frame index and bit-stream syntax element while performing video encoding process. Then, an optimization model was provided for modifying the video content in order to enhance the watermarking robustness without degrading the quality or bit rate. This model was utilized for improving the bit rate of videos and for maintaining the visual quality of videos. However, the complexity of this algorithm was high due to encryption constraints.

Tew and Wong (2014) surveyed the information hiding techniques in H.264/AVC compressed video. Initially, information hiding was commonly discussed based on the sequence of bits. Information hiding techniques were described by different data representation methods such as bit plane replacement, spread spectrum, histogram manipulation, divisibility, mapping rules and matrix encoding. A timeline diagram was constructed to summarize the invention of information hiding techniques in compressed videos and images. However, the complexity of embedding additional data into the compressed and encrypted domains was high.

Qian *et al.*(2014) proposed RDH in an encrypted JPEG bit-stream. The primary objective of this scheme was to encrypt the JPEG bit-stream into a properly organized structure and embed secret messages into the encrypted bit-stream by slightly modifying the JPEG stream. The usable bits were identified for data hiding. Therefore, the secret data were carried by the encrypted bit-stream which may be correctly decoded. The secret messages were encoded along with the error correction codes to accurately extract data and recover images. The encryption and embedding processes were controlled by the encryption and embedding keys. However, the quality of the decrypted images was low.

Rad *et al.* (2014) proposed a unified data embedding and scrambling method that aims at maintaining high-output image quality. Initially, checkerboard-based prediction was proposed for accurately predicting the pixels of the image based on the information acquired from the image. During degradation of image quality, the locations of the predicted pixels were vacated for embedding the information. Moreover, original images were reconstructed by storing prediction errors at predetermined precision using structure side information. However, the prediction of frequency coefficients was required for improving the embedding process.

Subramanyan *et al*. (2012) proposed a robust watermarking algorithm for watermarking compressed and encrypted JPEG2000 images. This encrypted algorithm was based on the stream cipher. Watermark was extracted in decryption phase whereas it was embedded in the compressed-encrypted phase. The embedding capacity, robustness, perceptual quality and security of this algorithm were investigated briefly using different watermarking methods such as spread spectrum, scalar costa scheme quantization index modulation and rational dither modulation. However, the compression gain of this algorithm was less and computational complexity was high.

Zheng and Huang (2012) proposed Walsh-Hadamard Transform (WHT) for homomorphic encrypted domain where the transformation matrix consists of only integers. In addition, its FAST (Features from Accelerated Segment Test) algorithm was also proposed in the encrypted domain. Furthermore, the relations between thecoefficients of adjacent transforms were modified for developing WHT-based image watermarking algorithm. This algorithm was utilized for extracting watermark blindly in both encrypted and decrypted domains. However, the computational overhead was high due to homomorphic cryptosystem constraints.

Xu *et al*. (2012) proposed data-hiding algorithm for H.264/AVC along with large data payload. In this method, secret information was embedded by modulating predicting methods of luminance blocks. If the information bit mismatched with the best mode, then the prediction mode was modulated by replacing the best mode with substitute mode. Initially, secret messages were encrypted based on chaotic sequences. Then, a small number of luminance blocks were selected randomly in every macro block which are utilized for embedding process based on another chaotic sequence. The hidden information was directly extracted from the encoded stream without restoring any original video. However, the robustness of the proposed algorithm did not improve.

MATERIALS AND METHODS

This study explains the proposed technique. During encoding of the HEVC, intra/inter prediction, DCT and quantization are achieved by prediction and transformation processes that utilize Coding Units (CU) structures. In prediction and transformation processes, Prediction Block (PB) and Transform Block (TB) are utilized by the CB. The CU size ranges from 64×64-4×4 pixels in the I-frame and the rectangular blocks of size 2N×N and N×2N for N∈{48} are included and 4 Asymmetry Motion Partition (AMP) in the P/B-frames. The AMP separates the CU into two unequal rectangles. “Top:bottom and left: right”, denoted as 2N×nU:2N×nD and nL×2N:nR×2N, respectively. In this approach, the selection of PB size and nonzero DCT coefficients based on TB size are achieved using matrix embedding technique.

During encoding, PB of different sizes is introduced while handling I-, P- and B-frames. To obtain a higher payload in every I-frame all PBs required for encoding are obtained using 8×8 or 4×4 pixels. The size of the PB is assumed to be similar to that of the information to be embedded according to the matrix embedding technique. As a result, CU is encoded as N×N, 2N×N, 2N×nUornL×2N for embedding bit 0 and as 2N×2N, N×2N×nDornR×2N for embedding bit 1. The matrix embedding technique (Fridrich and Soukal, 2006) is described in section 3.1. The block diagram of joint selective and matrix embedding technique is shown in Fig. 1

Matrix embedding for selecting PB size: Let us consider that is the binary code [n, k] including priority check matrix P and covering radius of the code R_C where the block length is n and k is the k-dimensional vector Subspace of S_2^n which is the space of all n-bit column vectors $x = (x_1, ..., x_n)^t$. For any $x \in S_2^n$, the vector $S = Px \in S_2^{n-K}$ is referred as the syndrome of x. For every syndrome $\in S_2^n$, the set $C(s) = \{x \in S_2^n \mid px = s\}$ is defined as the coset. The cosets related to the different syndromes are disjoint. Hence, there are 2^{n-k}disjoint cosets and each consisting 2^k of vectors. The smallest hamming weight w with any member of Coset C(s) is defined as the coset leader $e_L(s)$. The hamming weight w of a vector x is the number of ones in x and denoted as $w(x) = x_1+, ..., +x_n$.

The distance between the two vectors x and y is the Hamming weight of their difference and given as d(x, y) = w(x-y). For any x∈C, the ball with the center x and radius R_C is denoted as $B(x, R_C)$ and is given as $B(x,R_C) = \{y \in S_2^n \mid d(x,y) \le R_C\}$. The covering radius of code C is given as follows:

$$R_C = \max_{x \in S_2^n} d(x,C) \tag{1}$$

where, $d(x, C) = \min_{c \in C} d(x, C)$ which refers to the distance between x and code C. The average distance to the code is referred as the average distance between the selected vectors randomly S_2^n from and the code C and isgiven as:

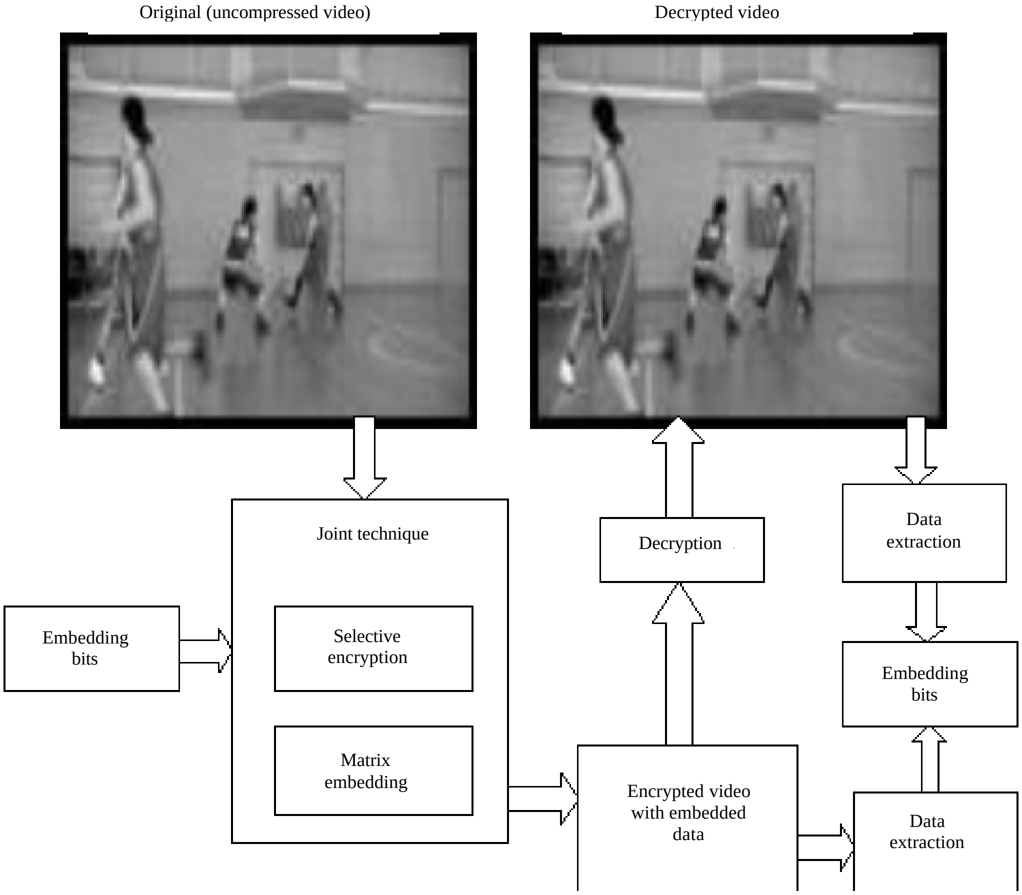

Fig. 1: Joint selective encryption and matrix embedding

$$R_{C_A} = \frac{1}{2^n}\sum_{x\in S_2^n} d(x,C), R_{C_A} \leq R(2) \qquad (2)$$

Let us consider that the set of all messages M and an embedding method on S_2^n along with distortion bound R_c is referred as the pair of embedding and extraction functions such as Emb and Ext. The embedding and extracting functions are given as follows:

$$\text{Emb}: S_2^n \times M \rightarrow S_2^n \text{ and Ext}: S_2^n \rightarrow M \qquad (3)$$

$$d(x,\text{Emb}(x,m)) \leq R_C \text{ for all } m \in M \text{ and } x \in S_2^n \qquad (4)$$

The embedding capacity is denoted as $h = \log_2|M|$ in bits and the relative payload is denoted as $\alpha = h/n$ in bits per pixel. Thus, the inequality is given as follows:

$$|M| \leq 2^n \text{ or } \alpha \leq 1 \qquad (5)$$

The embedding efficiency is further defined in terms of lower and upper bounds. The lower embedding efficiency and upper embedding efficiency are denoted as $\underline{\gamma} = h/R_C$ and $\gamma = h/R_C$, respectively. The given matrix embedding method is capable of communicating n-k bits $m \in S_2^n$ in pixels with x bits using at most R_C changes:

$$\text{Emb}(x,m) = x + e_L(m\text{-}Px) = y \qquad (6)$$

$$\text{Ext}(y)\, Py \qquad (7)$$

Here, $m \in S_2^{n-k}$ is the sequence of n-k message bits and e_L(m-Px) refers to the coset leader of the coset C(m-Px). The embedding method has distortion bound R_C which is identified by d(x,y) = w(e_L(m-p_x))≤R_C, since, C has the covering radius R_C. For Ext(Emb(x, m)) = m, Ext(Emb(x,m)) = Py = Px+Pe_L(m-Px) = Px+m-Px = m is observed.

In matrix embedding, the expected number of embedding changes for messages that are uniformly distributed in S_2^{n-k} is equivalent to the average weight of all coset leaders of C. The assumption that the messages are generated uniformly at random from is reasonable, since, they will be encrypted before embedding. The expected number of embedding modifications is equivalent to the average distance to the code. Since, any two words x, y from the similar Coset C are have an equivalent distance from C: d(x, C) = d(y, C) = w(e_L), the weight of any coset leader of and the average distance to code is defined as follows:

$$\frac{1}{2^n}\sum_{x\in S_2^n} d(x,C) = \frac{1}{2^n}\sum_{s\in S_2^{n-k}}\sum_{x\in C(s)} d(x,C(s)) = \frac{1}{2^n}\sum_{i=1}^{2^{n-k}} 2^k w(e_L(s)) = \frac{1}{2^{n-k}}\sum_{i=1}^{2^{n-k}} w(e_L(s)) \tag{8}$$

This equation is defined as the average number of embedding modifications for messages that are uniformly selected from s_2^{n-k}. The embedding efficiency based on bounds is defined below, since, there are $\sum_{i=0}^{R_c}\binom{n}{i}$ ways in which R_c is provided or some modifications in n pixels are obtained by any one of the values. Hence:

$$h = \log_2|M| \le \log_2\sum_{i=0}^{R_C}\binom{n}{i} = \log_2 V(n,R_C) \le nH\left(\frac{R_C}{n}\right) \tag{9}$$

where, V(n, R_C) refers to the volume of the ball of Radius R_C in s_2^n and $H(x) = -x\log_2 x-(1-x)\log_2(1-x)$, $0\le x\le 1/2$ refersto the binary entropy function. The inequality also provides the upper bound on lower embedding efficiency $\underline{\gamma} = h/R_c$ for the given relative payload $\alpha = h/n$ and is expressed as follows:

$$H^{-1}(\alpha) \le \frac{R_C}{n} \Rightarrow \underline{\gamma} = \frac{h}{R_C} = \alpha.\frac{n}{R_C} \le \frac{\alpha}{H^{-1}(\alpha)} \tag{10}$$

This bound is an asymptotic bound on the embedding efficiency γ:

$$\underset{\sim}{\gamma} \le \frac{\alpha}{H^{-1}(\alpha)}, \text{ for } \forall\left[n, n(1-\alpha)\right] \text{codes} \tag{11}$$

Since, the relative covering radius r = R_c/n and relative distance to code $r_a = R_{C_A}/n$ are coverage with n→∞. The upper bound on γ requires the lower bound on R_C and R_{C_A}. Since, there $\binom{n}{i}$ are possible sums of i columns of the parity check matrix P, the number of cosets whose coset leaders are having the weight i which is at most $\binom{n}{i}$. Thus, the covering radius R_{C_A} is at least equivalent to R_n for which:

$$\binom{n}{0}+\binom{n}{1}+,\ldots,+\binom{n}{R_n^{\,-1}}+\xi_n\binom{n}{R_n} = 2^{\alpha n} \tag{12}$$

In the above equation, ξ_n is the real number between 0 and 1, i.e., $0\le\xi<1$. Besides the lower bound $R_C \ge R_n$, the lower bound for R_{C_A} is obtained using the following equation:

$$R_{C_A} \ge \frac{\sum_{i=1}^{R_{n-1}} i\binom{n}{i} + R_n\xi_n\binom{n}{R_n}}{2^{\alpha n}} \tag{13}$$

Similarly, the upper bound is obtained as follows:

$$\gamma = \frac{\alpha n}{R_C} \le \frac{\alpha n 2^{\alpha n}}{\sum_{i=1}^{R_{n-1}} i\binom{n}{i} + R_n\xi_n\binom{n}{R_n}} \tag{14}$$

Manipulation of nonzero DCT coefficients based on the size of TB: Matrix embedding is implemented on the non zero DCT coefficients in each Coding Tree Units (CTU). However, the AC coefficients are restricted in the period of [8,8]/{0} and these coefficients are modified according to the size of TB. It is observed that the modification on this range is adequate to maintain the perceptual video quality while providing sufficient payload simultaneously. Based on the size of TB in CTU, the AC coefficients in the luminance channel are divided into four types: for data hiding, only AC coefficients in Z/{0} are considered.

Let us assume that the original and modified DCT coefficients are D_C and D'_C, respectively. The information bit to be embedded is considered as e_b and the embedding process is defined as follows:

$$D_C^{'} = \begin{cases} D_C+(-1)^{eb} \text{ if } \mathrm{mod}(|D_C|2) \ne e_b \\ D_C, \quad \text{Otherwise} \end{cases} \tag{15}$$

where, $D_C \in z/\{0\}$. The inserted information is extracted by considering the Least Significant Bit (LSB) of each coefficient in the specified range as follows:

$$Z = \begin{cases} [-88], \text{ if } TB_{size} = 4\times4, 8\times8 \\ [-6,6], \text{ if } TB_{size} = 16\times16 \\ [-4,4], \text{ if } TB_{size} = 32\times32 \\ [-2,2], \text{ if } TB_{size} = 64\times64 \end{cases} \tag{16}$$

Algorithm 1; Matrix embedding:

```
Step 1: Find such that $\alpha_n \ge (M/N) > \alpha_{n-1}/n/M$ is the number of bits to be
        embedded and N is the number of elements in the cover object
Step 2: Obtain the next n bits of x from the cover object and the next
        message segment m of length n-k
Step 3: Compute $\gamma$ which that solves $P_\gamma$ = m-Px
Step 4: Find the closest codeword to $\gamma$ in the list of all $2^k$ codewords and
```

```
denote (γ)
Step 5: Obtain embedding modifications such that $y = x+\gamma-c(\gamma)$ is the embedding object
Step 6: If the cover object is ended then the process is terminated.
Step 7: Else
Step 8: Move to step 1
Step 9: Extract the message based on equal embedding path
Step 10: Calculate n-k bits m from each block y of the embedding object m = Py
```

Selective encryption technique: Selective encryption technique is incorporated with matrix embedding such as to preserve the embedded data after decryption process and to extract the embedded data directly from the encrypted video without undergoing decryption process. This technique consists of three components: Transform Skip Bin (TsB), Sign Bin (SiB) and Suffix Bin (SuB).

The transform skip function (TsB allows the residual value of CU to be encoded in uncompressed or transformed-then-quantized form. This is flagged by a bin in each CU colour component with a size 4×4. If the bin is set to true, then the residual value from the prediction process is coded in uncompressed form where the inverse transform operations are carried out during decoding processes. Otherwise, the residual value of CU istransformed and quantized. These inverse transform operations are required for retrieving the original residual values at the end of decoder. During video encoding process an array of m-push Transform Skip (TsB) is randomized according to encryption key. Appropriate CU structure is selected based on randomized TsB using Rate Distortion Optimizer (RDO). This RDO is utilized for computing the trade-off between the distortion and the number of bits spent which is called cost function of each possible block size to the code for a given CU.

The Sign information (SiB) of non-zero DCT coefficients, MV and Delta Quantization Parameter (DQP) in the H.265 are stored in uncompressed form. Sufficient distortion is achieved by complete sign encryption or partial sign encryption process. The video under the control of the secret key is distorted by randomizing the sign of non-zero coefficients (coeff Signs) of each 8×8 block to maintain the parsing overhead minimal. Moreover, the signs of MV and DQP such as m-iHor, m-iVer and iDQP are randomized for generating a more distorted video.

The video compression efficiency and format compliances are maintained by exploiting binary syntax elements along with fixed-length codeword. The coefficient Suffix parts (SuB) and MV codes are encrypted securely without degrading the compression efficiency. Only the last coefficient of each 8×8 CU is considered for suppressing the processing time. These coefficients are randomly selected according to the encryption keys and their suffixes. The escape code value of these selected coefficients is encrypted by modifying the LSBsuf fixes. In addition, the magnitude of the horizontal and vertical MVs such as uiHorAbs and uiVerAbs are manipulated using the similar approach to further distort the perceptual quality in P and B frames.

RESULTS AND DISCUSSION

The proposed Matrix embedding based PB Size Selection (MPBSS) is implemented by modifying the HM16.0 reference Software. The proposed approach was analyzed by using the videos in class A (2560×1600), class B (1920×1080), class C (832×480) and class D (416×240) as test video sequences. MPBSS was compared with encrypted video susing TsB, SiB and SuB in terms of Peak Signal-to-Noise Ratio (PSNR) and time taken for encryption and decryption processes.

Peak signal-to-noise ratio: PSNR is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most commonly used as a measure of quality of reconstruction in image compression and is computed as follows:

$$\text{PSNR}(\text{dB}) = 10\log_{10}\left(\frac{\text{Maximum possible values in video}}{\text{Mean squared error}}\right)$$

Figure 2 shows the original and encrypted videos obtained by the proposed technique. Figure 3 shows the comparison of class-B video using MPBSS with encryption components such as TsB, SiB and SuB in terms of PSNR (dB). Here, the PSNR values of the proposed MPBSS with all encryption components range from -35dB to -53dB. Lower PSNR value is the desired value for a video to be encrypted. This indicates that sufficient distortion in quality has been achieved by encrypted videos there by making them more resistant to attacks.

Figure 4 compares the decrypted and encrypted class-D video using MPBSS with encryption components such as TsB, SiB and SuB in terms of time (sec).

Figure 4 shows the decoding time (sec) versus bit rate for all encryption components and their combinations. The time required for MPBSS-SiB is lesser than the time required for MPBSS-TsB and MPBSS-SuB. Moreover, MPBSS-all components require additional time for accessing encrypted bins during decryption.

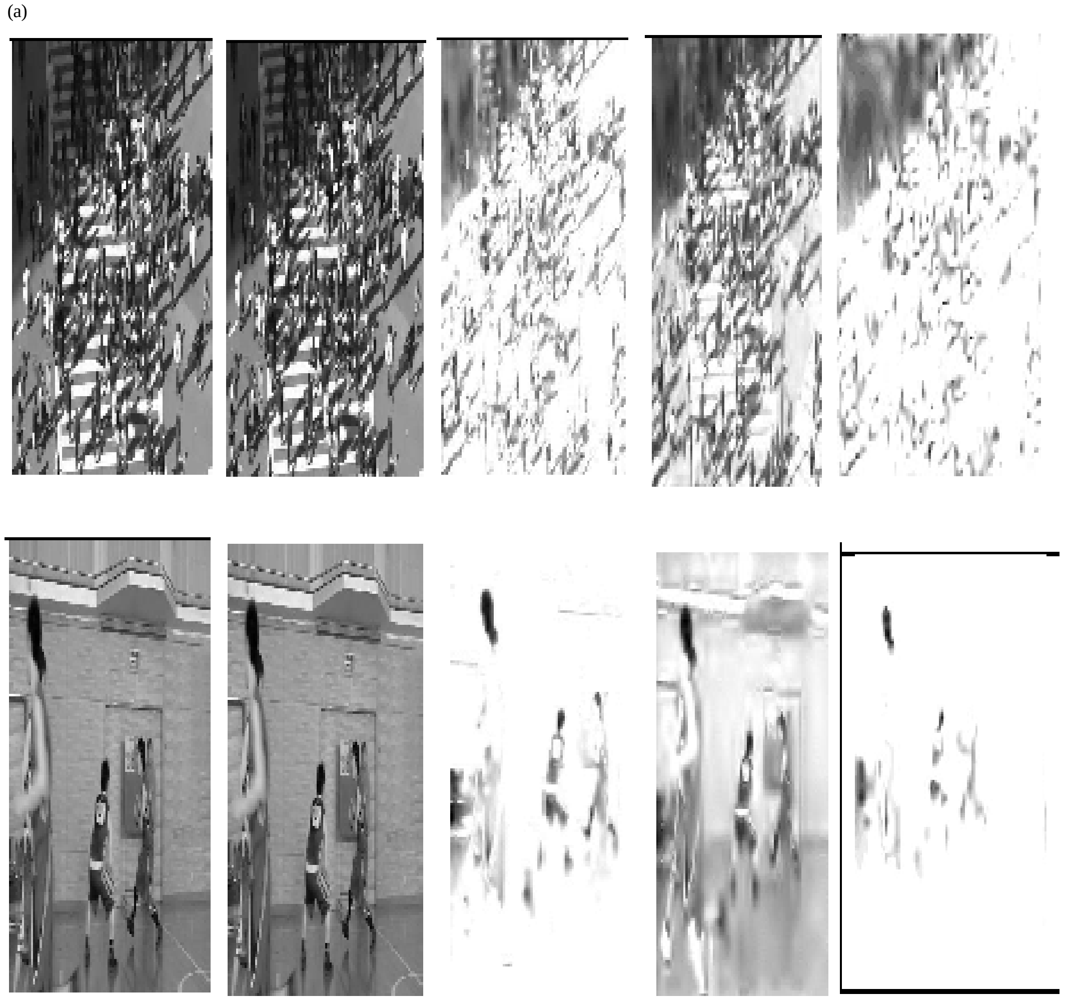

Fig. 2: Original and encrypted videos obtained using the proposed technique: a) People on street: Original; b) People on street: TsB; c) People on street: SiB; d) People on street: SuB; e) People on street: all; f) Basket ball drive: Original; g) Basket ball drive: TsB; h) Basket ball drive: SiB; i) Basket ball drive: SuB and j) Basket ball drive: all

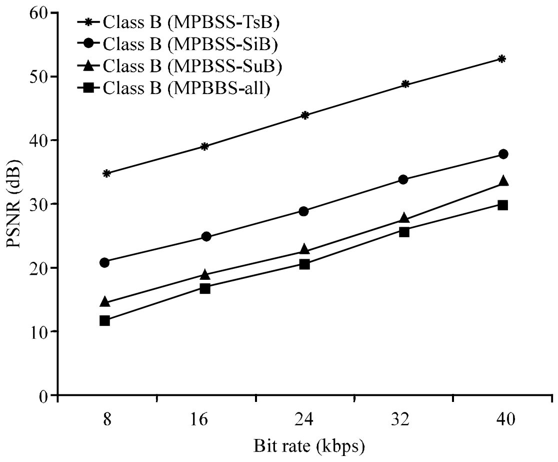

Fig. 3: Comparison of PSNR

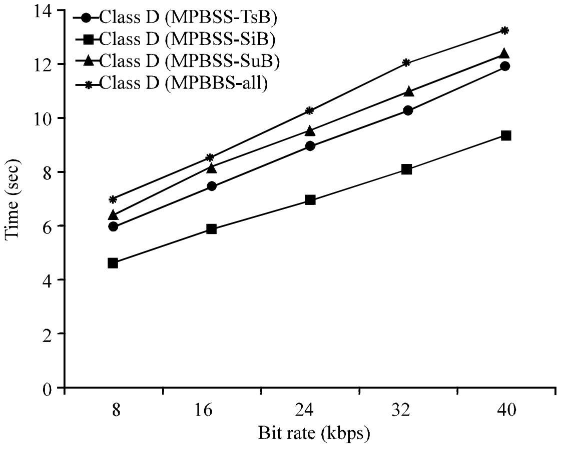

Fig. 4: Comparison of time taken (sec)

CONCLUSION

In this research, improved joint selective encryption and matrix embedding technique was proposed for HEVC or H.265. In this approach, the size of PB is manipulated using matrix embedding technique along with coding block size decision model and non-zero coefficients that fall within selective value ranges. In addition, the perceptual quality of video is achieved based on the size of TB. Thus, the embedding efficiency of large payloads is improved by applying matrix embedding the expected number of random bits embedded with one embedding change. Moreover, extraction process is applied before encryption process and after decryption process and selective encryption process is utilized for preserving the embedded information in the video content. The results obtained prove that the proposed technique has better embedding efficiency compared to other data-hiding techniques in H.265 or HEVC.

ACKNOWLEDGEMENT

Am doing my research in Manonmanium sundaranar University, Tirunelveli, study regarding my beloved guide Dr. K.K. Thyagharajan, Dean Academic supporting me to help to make papers.

REFERENCES

Esen, E. and A.A. Alatan, 2011. Robust video data hiding using forbidden zone data hiding and selective embedding. IEEE. Trans. Circuits Syst. Video Technol., 21: 1130-1138.

Fridrich, J. and D. Soukal, 2006. Matrix embedding for large payloads. IEEE. Trans. Inf. Forensics Secu., 1: 390-395.

Li, J., H. Liu, J. Huang and Y.Q. Shi, 2012. Reference index-based H.264 video watermarking scheme. ACM. Trans. Multimedia Comput., Commun. Appl., 8: 1-22.

Praveena, K. and T. Deepa, 2013. Forbidden zone data hiding in wavelet domain for digital video sequences. Global J. Adv. Eng. Technol., 2: 301-303.

Qian, Z., X. Zhang and S. Wang, 2014. Reversible data hiding in encrypted JPEG bitstream. IEEE. Trans. Multimedia, 16: 1486-1491.

Rad, R.M., K. Wong and J.M. Guo, 2014. A unified data embedding and scrambling method. IEEE. Trans. Image Process., 23: 1463-1475.

Stutz, T., F. Autrusseau and A. Uhl, 2014. Non-blind structure-preserving substitution watermarking of H.264/CAVLC inter-frames. IEEE. Trans. Multimedia, 16: 1337-1349.

Subramanyam, A.V., S. Emmanuel and M.S. Kankanhalli, 2012. Robust watermarking of compressed and encrypted JPEG2000 Images. IEEE. Trans. Multimedia, 14: 703-716.

Sullivan, G.J., J.R. Ohm, W.J. Han and T. Wiegand, 2012. Overview of the high efficiency video coding standard. IEEE. Trans. Circuits Syst. Video Technol., 22: 1649-1668.

Tew, Y. and K. Wong, 2014. An overview of information hiding in H.264/AVC compressed video. IEEE. Trans. Circuits Syst. Video Technol., 24: 305-319.

Tew, Y., K. Wong and R.C.W. Phan, 2016. Joint selective encryption and data embedding technique in HEVC video. Proceedings of the 2016 International Conference on Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), December 13-16, 2016, IEEE, Jeju, Korea, ISBN: 978-1-5090-2401-8, pp: 1-5.

Xu, D. and R. Wang, 2014. Efficient reversible data hiding in encrypted H.264/AVC videos. J. Electron. Imaging, 23: 1-14.

Xu, D. and R. Wang, 2015. Context adaptive binary arithmetic coding-based data hiding in partially encrypted H.264/AVC videos. J. Electron. Imaging, 24: 033028-1-033028-13.

Xu, D., R. Wang and J. Wang, 2012. Prediction mode modulated data-hiding algorithm for H.264/AVC. J. Real Time Image Process., 7: 205-214.

Xu, D., R. Wang and Y.Q. Shi, 2016. An improved scheme for data hiding in encrypted H.264/AVC videos. J. Visual Commun. Image Represent., 36: 229-242.

Zheng, P. and J. Huang, 2012. Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking. Proceedings of the 14th International Conference on Information Hiding (IH'12), May 15-18, 2012, Springer, Berlin, Heidelberg, ISBN:978-3-642-36372-6, pp: 240-254.