A Novel Approach for Codeword Substitution using Encrypted H.264/AVC Video Streams for Data Hiding

Nikita Ramdas Bodke
Student of BE Information Technology BVCOE & RI, Nasik, Maharashtra, India. Savitribai Phule Pune University

Jayashri Shantaram Khule
Student of BE Information Technology BVCOE & RI, Nasik, Maharashtra, India. Savitribai Phule Pune University

Premlata Uttam Shinde
Student of BE Information Technology BVCOE & RI, Nasik, Maharashtra, India Savitribai Phule Pune University

Sandip Nathu Kapse
Student of BE Information Technology BVCOE & RI, Nasik, Maharashtra, India Savitribai Phule Pune University

Kavita S. Kumavat
H. O. D,IT Dept., BVCOE & RI, Nasik, Maharashtra, India Savitribai Phule Pune University

ABSTRACT
Because of the privacy-preserving, data hiding is a new technique that had drawn attention. Access control and transaction tracking, data hiding techniques can be used to insert a private message and private image into a video bit stream for copyright protection. To an encrypted format, for security and privacy digital video need to be stored in the system and then processed. This will preserve the private information of data. video encryption, data insertion, and data extraction, in data hiding in encrypted of H.264/AVC video stream H.264/AVC it contain. to produce encrypted video. Using codeword substitution methods ,cloud server or data hider may insert additional data in domain, in an encryption H.264/AVC video is encrypted with encryption key using the stream cipher. The data extraction process can be done in the encrypted domain or decrypted domain. The codeword of residue coefficients are encrypted, in an stream cipher codeword of intraprediction modes, the codeword of motion vector difference. Is restricted maintain the video file size in an encryption and data insertion. To hide or secure private message, images in video bit format, for protection, data hiding technique can be used. So that edge quality information and number of bits of block can be hide, to maintain security and privacy bit streams processed in an encrypted format. Experimental result can maintain file size of video, degradation in video quality is quite small.

Keywords
Data hidden, encrypted domain, H.264/AVC, codeword substituting.

1. INTRODUCTION
The widespread use of the Internet offers great convenience to the transmission of a large amount of data over networks, which are open but insecure channels, exposing many private and secret data to dangerous situations. Today, ensuring that information transmission over the Internet remains safe and secure has become extremely important. A types of various techniques have data hiding is one of the protective techniques in data security, to keep the unauthorized user away from the transmission information. this dissertation proposes a reversible data hiding based on reserving room before encryption (RRBE) technique and VQ-compressed images, inspired by the SMVQ technique and vacating room after encryption (VRAE) technique. Today, ensuring that information transmission over the Internet remains safe and secure has become extremely important. A variety of techniques have been proposed; to hide data this is the best protective techniques in data security, to keep the unauthorized user away from the transmission information. image from an embedded image after the embedded message is extracted, this scheme can completely recover the original VQ cover. The proposed scheme employs block match coding (BMC) to reduce the complexity and preserve a satisfactory embedding capacity, compared to the SMVQ technique that is very time consuming to set up a state codebook and then search the nearest codeword. low embedding rates, high complexities, or high bit rates, the main problems in the former works are low embedding capacities. To improve these problems, the proposed scheme applies the BMC prediction to encode indices, and thus can obtain a higher embedding capacity, higher embedding rate, higher processing efficiency, and lower bit rate simultaneously. Data hiding defined more as by which a message signal or signature is imperceptibly embedded into a host or cover to get composite signal. Information insertion into a multimedia host should not incur any perceptual distortion to the host. The data are recoverable after the composite multimedia signal has undergo a variety of processing, intentional / unintentional, to remove the embedded data. the another words, the hidden data must be robust against a various attacks. here would like to embed as too many bits into the host as possible or the capacity of the insertion system should be high. Various applications have various specific requirements of robustness and the volume of embedding. Most applications, however, require near-perfect perceptual transparency.

Which are considered or defined in this thesis, there are several other design issues, based, again, on the target applications. Providing graceful improvement in the quality of recovered signature data as the attack strength reduces, this include maintaining statistical transparency to conceal the presence of embedded data .Figure 1 shows normal encryption technique which contain encoder and decoder for message passing.

In Fig.1 Producing digital images or pictures is easy than before, because of advanced improvement of information

technology. To significantly reduce the size of digital images saving storage space and transmission bandwidth, many compression techniques have been presented. Picture compression techniques can be briefly classified into three types spatial domain methods , frequency domain methods , Compressed methods. The target of spatial domain compression method is pixels of an image. The another side, the focus of frequency domain compression method is coefficients of a transformed image. In terms of computation cost because spatial domain compression method needs not to transform into frequency domain, spatial domain compression method is more efficient than frequency domain compression method. In other words, spatial domain compression method is more suitable for low power environment Vector quantization (VQ) has widely been used for signal processing due to its excellent compression performance. Data hiding techniques in the VQ-compressed domain can relish advantages of both data hiding and compression for a multimedia distribution, achieving a secure channel and bandwidth space saving for data transmission storage. This chapter reviews the all existing approaches for data hiding. It summarizes the research work carried out by different researchers for data hiding, the techniques used by them and the result of the research work.

2. PROBLEM DEFINATION

Due to exponential increase of size so it is called multimedia files in recent years the reason of the substantial increase of reasonable memory storage on one hand and the wide spread to the other hand. This system motivates the extensive research into retrieval systems image. The research into what is referred as data hiding and compress the image using vector quantization for that reason the small database is required, to overcome these types of difficulties it motivates. This chapter follow the all existing approaches for data hiding. First part is H.264/AVC video encryption, second part is data embedding and the last one is data extraction, a novel scheme of data hiding in the encrypted version of H.264/AVC videos consist of three parts. To produce an encrypted standard video stream the content owner can encrypts the original H.264/AVC video stream by using standard stream ciphers with encryption keys. After that without knowing the original video content the data-hider can insert the additional data into the encrypted video stream by use of codeword substituting method. The hidden data extraction can be successfully completed in encrypted or decrypted domain at the receiver end.

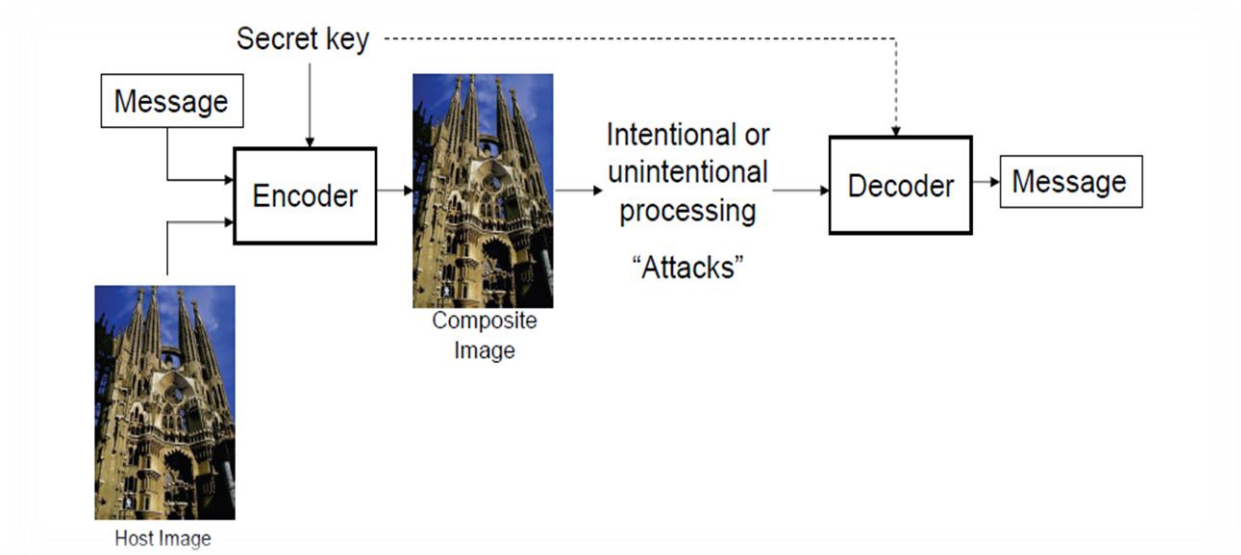

Fig 1: Normal Encryption Technology

3. LITERATURE SURVY

The techniques of data hiding can be classified in two ways, first technique is reversible data hiding and second technique is irreversible data hiding schemes. Irreversible data hiding extract only secret data and restoration of cover images is not available .The private data can be withdraw by retrieval data hiding schemes and original and simultaneously cover the original image. two types of method are used in data hiding techniques. first method is that index modifying method and second one is side match VQ (SMVQ), this two methods are used to embed secrete data into a VQ-compressed image .Different index- modifying data hiding techniques and side match data hiding techniques in (SMVQ) are develop by many researchers. An index-modifying data hiding scheme was easy to realize but it was an irreversible data hiding scheme so the original cover image can't be restored and data hiding capacity was small. For an SMVQ- based data hiding developed an adaptive data hiding based on a VQ-compressed image, in which image blocks are divided into embeddable and uninserted blocks based on the variances and side match distortions. It can be high insertion capacity, quality of the reconstruction pictures are reduces as the quantity of the private data increases. Is a case of the irreversible information hiding. The scheme, the VQ and SMVQ are applied to hide secret data, and higher embedding capacity and lower bit rate can be yield. Moreover, it is a reversible data-hiding scheme. In year 2007, Chang et al. [10] developed another index-modifying data-hiding scheme with recovery capability. Indicators are added in front of the most encoded indices and only two clusters can be used to hide secret data in their 2-bit hiding scheme, resulting in low embedding capacity and high bit rate(BR). In general, high embedding capacity can be achieved with SMVQ based data-hiding schemes, in which a state codebook is used to encode each index, yet they require more encoding time than that of the index-

modifying techniques. A reversible data hide scheme are used for embedding the private data in VQ-compressed codes based on the declustering strategy is proposed. The scheme can achieve higher embedding capacity but requires many computations to decluster a codebook into a number of groups .P. Tsai [12] in the year 2009, proposed the scheme which uses more pairs of peak and zero points in the histogram to achieve the hiding process. Although the scheme is reversible and with formal indices as output, the hiding capacity is rather low, and the distortion of the embedded image increases as the hiding capacity increases. C. C. Chang, G. M. Chen, and M. H. Lin [5], proposed a technique in which SOC and original index value are employed to hide private bit 0or 1. C. C. Chang, T. D. Kieu , W. C. Wu [13] and J. X. Wang , Z. M. Lu[14] in the year 2009 developed the JNC scheme encodes the encoding index and insert private data using the difference between the encoding index and one of its neighboring indices, which can obtain a high embedding capacity and a high B R simultaneously. K. Hwang and D. Li [18] in the year 2010, trust-management scheme enhanced with data coloring. Software watermarking, in which encryption of data and coloring offer possibilities for downloading the privacy and integrity of the data. In year 2010, C. C. Chen and C. C. Chang [17] proposed a data hiding scheme in which both VQ and SMVQ are used to hide secret data in and a 1-b indictor is always required for every index but only one secret data can be inserted in every index when the VQ technique is applied. similarly, more than one bit secret data can be inserted in every index when the SMVQ technique is applied. J. D. Lee, Y. H. Chiou, and J. M. Guo [18] in 2011, developed a data hiding scheme in which SMVQ indices are divided into three parts, and indices in part 1 are used to hide secret data. Moreover, search order coding (SOC)-based and joint neighboring coding based hiding schemes, which use the processed neighboring indices to set up a search path. In [23], Zhang divided the encrypted image into several blocks. Hong et al. [27] ameliorated Zhang's method at the decoder side by further effort the spatial correlation using a various estimation equation and side match technique to achieve low error rate. Compression of encrypt data are formulation in as source code with side information at the decoder [20], in which a typical method is generating the compressed data in less loss manner by effort the syndromes of parity-check matrix of channel codes. The method in [28] compressed the encrypted LSBs to vacate room for additional data by finding and the information used at the receiver is also the spatial correlation of decrypted images.

4. SYSTEM OVERVIEW

A. **Encryption of H.264/AVC Video Stream**

In Fig. 2(a) Shows Video encryption standard is requires the process is a time effective to meet the requirement of real time and format compliance. It is not encrypt the whole compressed video bitstream alternatively, only a fraction of video details encrypted to improve the efficiency while still achieving sufficient security. The key issue of encrypted video steam is that it concentrate on how to select the sensitive data to encrypt. An H.264/AVC video encryption scheme with good performance consist of security, efficiency, and format compliance is proposed. The encryption algorithm is performed not only in H.264/AVC encoding but also in the H.264/AVC compressed domain. Encryption of H.264/AVC Video Stream compressed domain has been presented on context-adaptive variable length coding (*CAVLC*) and context-adaptive binary arithmetic coding(*CABAC*). By analyzing the property of H.264/AVC codec, there are three sensitive parts are encrypted with the stream ciphers. The system have improved and enhanced the previous proposed approach by encrypting more syntax elements. The proposed system encrypt the IPMs codewords, the MVDs codewords, and the residual coefficients codewords.

B. **Data Embedding**

In Fig. 2(b) Shows the data embedding process few methods are proposed to embed data into H.264/AVC bitstream directly. No anyone methods are implemented in the encrypted domain. In these process the levels of sign are encrypted, so that data hiding should not affect the levels of sign. In the codewords substitution following three types of limitation are satisfied. First limitation is that, the codeword substituting after bitstream must remain syntax compliance so that it can be decoded by standard decoder. Second limitation is that, the bit-rate remains unchanged, to take care that the substituted codeword and the original codeword having the same size. Third limitation is that ,data hiding does causes the visual degradation but having impact should be kept minimum. That is after video decryption, the embedded data has to be invisible to a human observer. So the level corresponding the substituted codeword value should be close to the level corresponding value to the original codeword value.

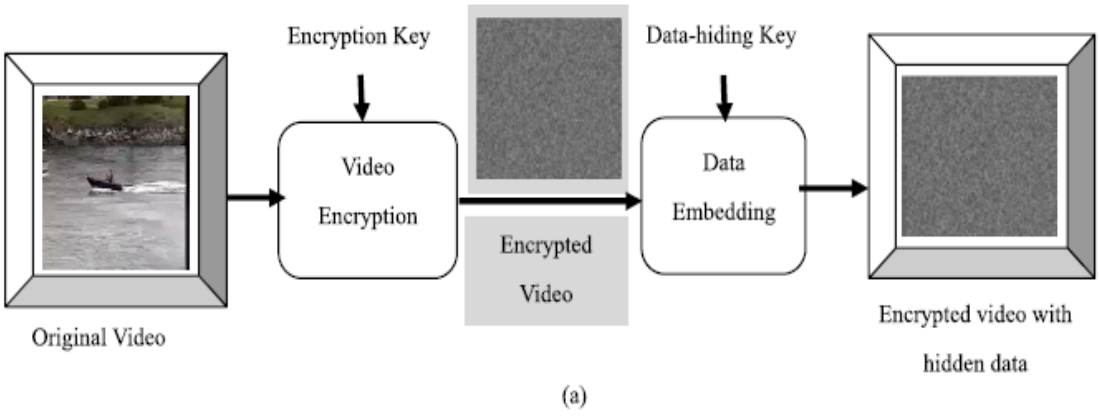

Fig. 2 (a) : Video encryption and data embedding at the sender end

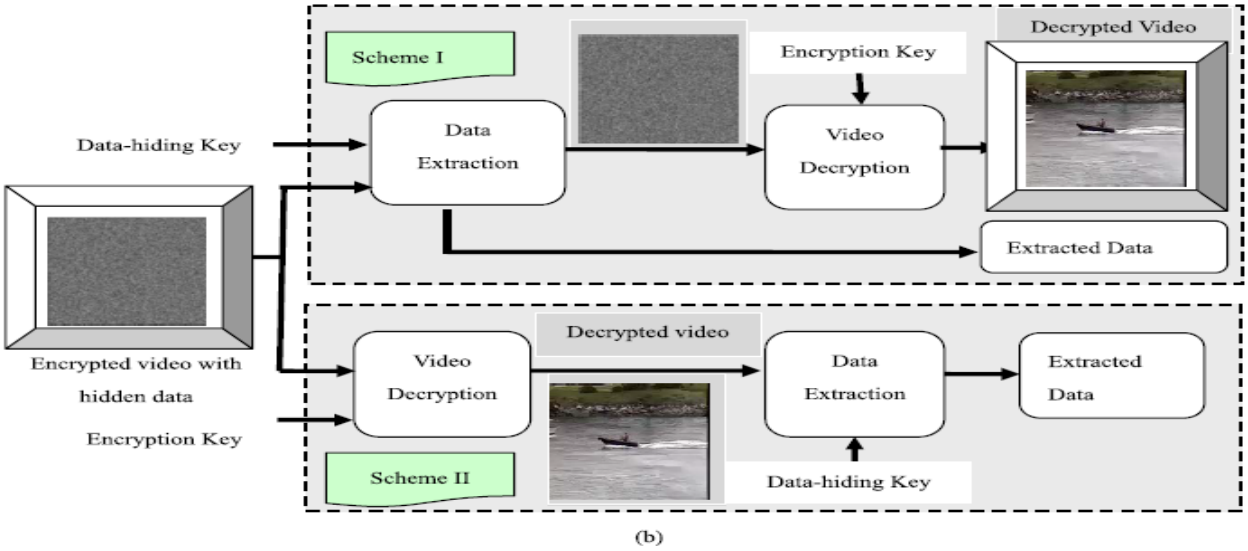

Fig. 2(b) Data extraction and video display at the receiver end in two scenarios

C. **Data Extraction**

In data extraction process the hidden data can be extracted either in Encrypted domain or in decrypted domain. The data extraction process is the fast and simple. In the encrypted Domain Extraction a database manager only access the data hiding key and to manipulate data in encrypted domain for purpose of protecting privacy. In this case data extraction in encrypted domain guarantees the feasibility. In encrypted domain, encrypted video with hidden data is directly send to the extraction module. The codeword is a part of codespaceC0, the bit of data extracted is "0". The codeword is part codespaceC1,the bit of data extracted is "1". In that way the data hiding key, the equal chaotic pseudo-random sequence P was used in the embedding process can be generated.

5. ALGORITHMS

- Privacy of Encryption Algorithm

Video encryption scheme, the privacy includes both cryptographic privacy and perceptual privacy. Cryptographic privacy denotes the privacy against cryptographic attacks, which depends on the ciphers adopted by the scheme. The protect stream cipher is used to encrypt the bitstream, and chaotic pseudo-random sequence generated by logistic map is used to encrypt the additional data. They have been proved to be protect cryptographic attacks. Perceptual privacy refers to whether the encrypted video is unintelligible or not. It depends on the encryption scheme's properties. Encrypting only IPM cannot keep protect enough, since the encrypted video is intelligible .The encrypts IPM, MVD and residual coefficients, which keeps perceptual privacy of the encrypted video. The demonstration and an original frame from each video is depicted, and their corresponding encrypted results are depicted in Other frames have a similar effect of encryption. Due to space limitations, do not list the results of all frames. It should be mentioned that not every video can be degraded to the same extent. The perceptual quality of high-motion videos with a complex textured background becomes much more scrambled after encryption than that of slow-motion videos with a static background. The reason is that there are less residual coefficients and MVDs in low-motion videos that are available for encryption. Scrambling performance of the encryption system is more than sufficient.

- Intra-Prediction Mode (IPM) Encryption

In data hiding H.264/AVC standard there are four types of intra coding are useful and which are denoted by Intra_4 × 4, Intra_16×16, Intra_chroma, and I_PCM . Intra_4×4 and Intra_16 × 16 blocks are used to encrypt data. In Intra_16 × 16 four intra prediction are available. Intra_16 × 16 block is specified in the mb_type (macroblock type) as well as it specified in the from of coded block pattern (CBP). To keep unchanged codeword length, the encrypted codeword the same size as original codeword. The combination of CBP is the same in every four lines, and the codewords have the same length in every two consecutive lines.

- Motion Vector Difference (MVD) Encryption

Not only the IPMs encrypted to protect both information texture and motion, but also the motion vector should also be encrypted. In H.264/AVC standard Exp-Golomb entropy coding is very useful to encode MVD. The Exp-Golomb codeword constructed as[*M zeros*] [*I NFO*], where *I NFO* is an *M*-bit field carrying information. The last bit of the codeword is encrypted by the bitwise XOR operation with stream cipher, which is an encrypted by an encryption *E_Key*. The last bit encryption may change the sign of MVD, but the length of the codeword does not affect and filled with satisfaction and the compliance format. In that way, the resulting cipher texts are still valid Exp-Golomb codes.

6. CONCLUSION

Data hiding in encrypted media is one of the important concept for privacy-preserving requirements from cloud data management. This paper focus on an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, which furtherly divided into video encryption, data embedding and data extraction phases. The algorithm maintain the bit-rate after encryption and data embedding. The algorithm is also useful to implement to performed in the compressed and encrypted domain. It means that ,it does not require partial decompression of the video stream. Thus algorithm is ideal for video applications. The data can be hide which is embed additionally data into the encrypted bit stream using codeword substituting. Data hiding is done totally in the encrypted domain, the method which is given in this paper can preserve the confidentiality of the content completely. When encrypted video contain hidden data, data extraction can be carried out either in encrypted or decrypted domain, which having two different practical applications.

One of the important benefit as it is fully compliant with the H.264/AVC syntax. The experiment shows that the proposed encryption and data embedding scheme can maintain &preserve file-size, where the degradation in video quality caused by data hiding is quite small.

7. REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, "Secure video processing:Problems andchallenges," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing*,Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme inthe encrypted domain for buyer-seller watermarking protocol," *Inf. Sci.*,vol. 180, no. 23, pp. 4672–4684, 2010.

[3] P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphicencrypted domain and its application in image watermarking,"in*Proc. 14th Inf. Hiding Conf.*, Berkeley, CA, USA, 2012, pp. 1–15.

[4] W. Puech, M. Chaumont, and O. Strauss, "A reversible datahiding method for encrypted images," *Proc. SPIE*, vol. 6819,pp. 68191E-1–68191E-9, Jan. 2008.

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

[6] W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible datahiding in encrypted images using side match," *IEEE Signal Process.Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[7] X. P. Zhang, "Separable reversible data hiding in encryptedimage," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2,pp. 826–832, Apr. 2012.

[8] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible datahiding in encrypted images by reserving room before encryption," *IEEETrans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[9] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robustwatermarking of compressed and encrypted JPEG2000 images," *IEEETrans. Multimedia*, vol. 14, no. 3, pp. 703–716, Jun. 2012.

[10] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption andwatermarking in video compression," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[11] S. W. Park and S. U. Shin, "Combined scheme of encryption andwatermarking in H.264/scalable video coding (SVC)," *New DirectionsIntell. Interact. Multimedia*, vol. 142, no. 1, pp. 351–361, 2008.

[12] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overviewof the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 13, no. 7, pp. 560–576, Jul. 2003.

[13] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advancedvideo coding based on selective encryption algorithms," *IEEE Trans.Consumer Electron.*, vol. 52, no. 2, pp. 621–629, May 2006.

[14] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVCby selective encryption of CAVLC and CABAC for I and P frames,"*IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565–576,May 2011.

[15] M. N. Asghar and M. Ghanbari, "An efficient security system forCABAC bin-strings of H.264/SVC," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 23, no. 3, pp. 425–437, Mar. 2013.

8. AUTHOR PROFILE

Nikita Ramdas Bodke she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of computer Security.

Jayashri Shantaram Khule she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of computer networking.

Premlata Uttam Shinde she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of cloud computing and image processing.

Sandip Nathu Kapse he is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. His interest is in the field of cloud computing.

K. S. Kumavat, ME, BE Computer Engg. Was educated at Pune University. Presently she is working as Head Information Technology Department of Brahma Valley College of Engineering and Research Institute, Nasik, Maharashtra, India. She has presented papers at National and International conferences and also published papers in National and International Journals on various aspects of Computer Engineering and Networks. Her areas of interest include Computer Networks Security and Advance Database.