Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Video Data Hiding Using Encryption Algorithms with Embedding Methods

P.Meena, J. Anitha Joseph MCA
Gonzaga College of Arts and Science for Women, Kathampallam, Elathagiri, India.
*Corresponding author Email: meena@gonzagacollege.edu.in,

Abstract. Due to the increased digital media on the Internet, data security and privacy protection issue have attracted the attention of data communication. Data hiding has become a topic of considerable importance. Nowadays, a new challenge consists of reversible data hiding in the encrypted image because of the correlations of local pixels that are destroyed in an encrypted image; it is difficult to embed secret messages in encrypted images using the difference of neighboring pixels. Video data hiding is a very important research topic due to the design complexities involved. In general, due to the wide presence and the tolerance of human perceptual systems involved visual and aural media are preferred. The methods vary depending on the nature of such media and the general structure of data hiding process does not depend on the host media type. However, most of the video data hiding methods utilize uncompressed video data. Recent video data hiding techniques are focused on the characteristics generated by video compressing standards. The main objective of this research work is to propose a new video data hiding method that makes use of correction capability of repeat accumulate codes and superiority of forbidden zone data hiding (FZDH). FZDH is used for no alteration is allowed while data hiding process. The framework is tested by all kinds of videos such as .mp4, .3gp, .avi etc., and gets successful output for all video data hiding process. The proposed scheme is hiding the video data to provide security by encryption and decryption process. The simulation results show thatthe process of hiding the video data enforce security in higher level.
Keywords— FZDH, data hiding, encrypt process, decrypt process, superiority

1. Introduction

As ITC (Information Technology and Communication) grows rapidly, multimedia is used widely in order to have flexibility in expression and also communication. This led to security problems over Internet. This facilitated the need for new data hiding technologies for having secret communication. Cryptography is one such technique that scrambles messages or converts message into misunderstand able format while another technology by name steganography hides data in such a way that it can't be viewed by adversaries. Intellectual property such as digital media like video, audio, images are distributed, manipulated and reproduced over IT systems. Copyright protection in this scenario is a challenging issue. Towards this end watermarking technology came into existence. This technology is meant for identifying the owner of the media. This is achieved by encoding some sort of hidden information for copyright protection. It is in contrast with encryption as it can be part of media permanently and protects copyrights while encryption merely restricts data access illegally. As an alternative to encryption, data hiding within cover media came into existence. The cover media includes video, image and audio. This kind of data hiding can also be called as steganography where data is hidden in unused and undetectable bytes of the select host media. It gives superior security when compared with cryptography. The process of data hiding in various cover media has significant similarities. However, the data hiding process in video demands more complex designs [1], [2]. There are two main ways in which data hiding in video takes place. They are data-level and bit stream-level. The bit stream – level data hiding exploits redundancy in compression standards. Its encoders have freedom to choose various options for the purpose of data hiding based on the structure of the bit stream. This makes the technique fragile and it can't withstand any kind of format conversion though perceptual quality can be preserved. Therefore it is not suitable to all applications except some fragile applications like authentication. On the other hand, data-level approach to data hiding is more robust to security attacks. This makes it suitable for wide range of applications. In spite of their fragility, the bit stream-level data hiding techniques are still attractive solutions for data hiding as described in [3], [4], and [5]. In [3] redundancy in block size selection is used while in [5] DCT coefficients are modified in the bit-stream level. In [4] QIM (Quantization Index Modulation) technique is used to low frequency DCT coefficients based on the parameters of videos of type MPEG-2. They changed embed rate based on the type of video frame resulting in de- synchronization of erasures and insertions that take place at the decoder. They processed each frame separately since the parameters are used based on the type of frame.

In this paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) [8] and RA codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical data hiding method, which is shown to be superior to the conventional Quantization Index Modulation (QIM) [9]. RA codes are already used in image [3] and video [2] data hiding due to their robustness against erasures. This robustness allows handling desynchronization between embedded and decoder that occurs as a result of the differences in the selected coefficients. In order to incorporate frame synchronization markers, we partition the blocks into two groups. One group is used for frame marker embedding and the other is used for message bits. By means of simple rules

applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks. We utilize systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. Random interleaving is performed spatio-temporally; hence, dependency to local characteristics is reduced. Host signal coefficients used for data hiding are selected at four stages. First, frame selection is performed. Frames with sufficient number of blocks are selected. Next, only some predetermined low frequency DCT coefficients are permitted to hide data. Then the average energy of the block is expected to be greater than a predetermined threshold. In the final stage, the energy of each coefficient is compared against another threshold. The unselected blocks are labeled as erasures and they are not processed. For each selected block, there exists variable number of coefficients. These coefficients are used to embed and decode single message bit by employing multi-dimensional form of FZDH that uses cubic lattice as its basequantizer. However, most of the video data hiding methods utilize uncompressed video data. Sarkar et al. Proposed a high volume transform domain data hiding in MPEG-2 videos. They applied quantization index modulation (QIM) to low frequency DCT coefficients and adapted the quantization parameter based on MPEG-2 parameters. Furthermore, they varied the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes de-synchronization. They utilized repeat accumulate (RA) codes in order to withstand erasures. Since they adapted the parameters according to type of frame, each frame is processed separately[6].

Problem Domain: The major drawback of host activity based methods is that the host activity collected from each stepping stone is generally not trustworthy. Since the attacker is assumed to have full control over each stepping stone, it can easily modify, delete or forge user login in formation. This defeat the ability to correlate based on host activity.

Existing scheme: In special domain, the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods; hide datain another domain such as wavelet domain.

- Least significant bit (LSB) is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.
- LSB method has intense affects on the statistical information of image like histogram. Attackers could be aware of a hidden communication by just checking the Histogram of an image. A good solution to eliminate this defect was LSB matching. LSB-Matching was a great step forward in Steganography methods and many others get ideas fromit.

Proposed scheme:

- Data hiding in video sequences is performed in two major ways: bit stream-level and data-level.
- In this paper, we propose a new block-based selective embedding type data hiding frame work that encapsulates Forbidden Zone Data Hiding(FZDH)
- By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks.

Advantages

- User cannot find the originaldata.
- It is not easilycracked.
- To increase theSecurity.
- To increase the size of storeddata

Block Diagram

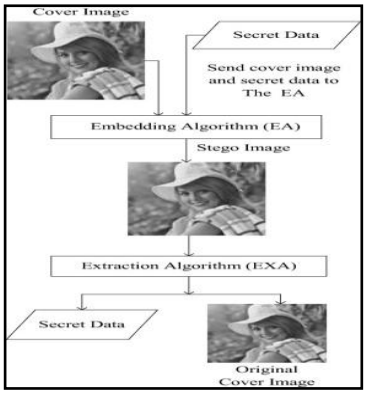


FIGURE 1.1 Block Diagram of the new Block Based data hiding technique

2. Forbidden Zone Data hiding

Forbidden zone data hiding (FZDH) is introduced in [8].The method depends on the for bidden zone(FZ)concept, which is defined as the host signal range where no alteration is allowed during data hiding process. FZDH makes use of FZ to adjust the robustness-invisibility trade off.

Proposed video data hiding frame work: A block based adaptive video data hiding method that incorporates FZDH, which is shown to be superior to QIM and competitive with DC-QIM [8], and erasure handling through RA Codes. We utilize selective embedding to determine which host signal coefficients will be used in data hiding as in [3]. Unlike the method in [3], we employ block selection (entropy selection scheme [3]) and coefficient selection (selectively embedding in coefficients scheme [3]) together. The de-synchronization due to block selection is handled via RA Codes as in [2] and [3]. The de- synchronization due to coefficient selection is handled by using multi-dimensional form of FZDH in varying dimensions. In [2], the frames are processed independently. It is observed that [10] intra and inter frames do not yield significant differences. Therefore, in order to overcome local bursts of error, we utilize 3-D interleaving similar to [5], which does not utilize selective embedding, but uses the whole LL sub band of discrete wavelet transform. Furthermore, as in [5], we equip the method with frame synchronization markers in order to handle frame drop, insert, or repeat attacks. Hence, it can be stated the original contribution of this paper is to devise a complete video data hiding method that is resistant to de-synchronization due to selective embedding and robust to temporal attacks, while making use of the superiority of FZDH

Framework: The embedding operation for a single frame is shown in Fig. 2.1.Y-channelisutilized for data embedding. In the first step, frame selection is performed and the selected frames are processed block wise. For each block, only a single bit is hidden. After obtaining 8 × 8 DCT of the block, energy check is performe don the coefficients that are predefine dinamask. Selected coefficients of variable length are used to hide data bit m. m is a member of message bits or frame synchronization markers. Message sequence of each group is obtained by using RA codes for T consecutive frames. Each block is assigned to one of these groups at the beginning. After the inverse transform host frame is obtained.

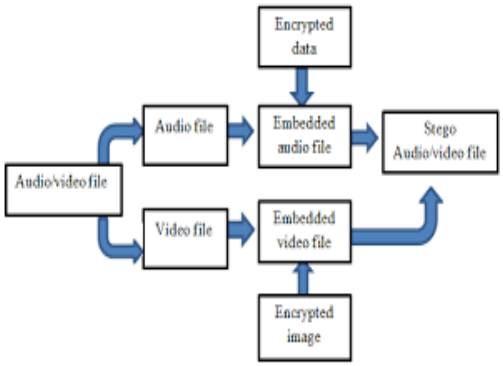


FIGURE.2.1 Embedder flowchart of the proposed video data hiding frame work for a single frame.

Decoder is the dual of the embedded, with the exception that frame selection is not performed. Fig. 2.2 shows the flowchart for a single frame. Marked frames are detected by using frame synchronization markers. Decoder employs the same system parameters and determines the marked signal values that will be fed to data extraction step. Non-selected blocks are handled as erasures. Erasures and decoded message data probabilities (om) are passed to RA decoder for T consecutive frames as a whole and then the hidden data is decoded.

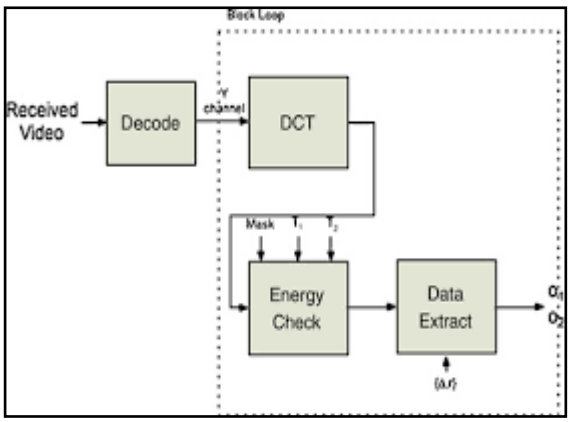


FIGURE.2.2 Decoder Flowchart of the Proposed Video Data Hiding Framework for a Single Frame

Selective Embedding: Host signal samples, which will be used in data hiding, are determined adaptively. The selection is performed at four stages: frame selection, frequency band determination, block selection, and coefficient selection.

- Frame selection: selected number of blocks in the whole frame is counted. If the ratio of selected block stoall blocks is above a certain value (T0) the frame is processed. Otherwise, this frame is skipped.
- Frequency band: only certain DCT coefficients are utilized. Middle frequency band of DCT coefficientsshowninFig.2.3 is utilized similar to[2].
- Block selection: energy of the coefficients in the mask is computed. If the energy of the block is above a certain value (T1) then the block is processed. Otherwise, itisskipped.
- Coefficient selection: energy of each coefficient is compared to another threshold T2. If the energy is above T2, then it is used during data embedding together with other selected coefficients in the sameblock.

3. Modules

In this paper, we divided into four modules. They are

- -INPUT MODULE
- -ENCRYPTIONMODULE
- -DECRYPTIONMODULE
- -SECURITY MODULE
- -UMARAM
- -UR5
- -RSA

Input Module: The Input Module is designed as such a way that the proposed system must be capable of handling any type of data formats, such as if the user wishes to hide any image format then it must be compatible with all usual image formats such as jpg, gif, bmp, it must be also compatible with video formats such as .avi,.flv, .wmf etc.. And also it must be compatible with various document formats, so that the user can be able to user any formats to hide the secret data.
Encryption Module: In Encryption module, it consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is c licked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image or video file through another open file dialog box which is opened when the cover file button is clicked. Where the user can select the cover file and then the Hide button is clicked so that the secret data or message is hidden in cover file using Forbidden Zone Data Hiding Technique.
Decryption Module: This module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted cover file and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.
Security Module: UMARAM: The UMARAM was designed by Ramesh G and R.Umarani in the year 2010. This algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of 16X 16 X 16. The S-Box consists of 16-slides, and each slide having 2-D of 16 x16. The numbers from 0 to 255 are arranged in random positions in each slide[20]. UR5:This algorithm was designed by G.Ramesh and Dr. R. Umarani in the end of the year 2010. A block encryption algorithm is proposed in this approach. In this Algorithm, a series of transformations have been used depending on S- BOX, XOR Gate, and AND Gate. The UR5 algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits.It uses eight rounds for encryption or decryption process. It over comes some drawback soft he other algorithms. It is more efficient and useable for the Wireless Local Area Network because it avoids the using of the same key with other packets within a message. The algorithm is simple and helpful in avoiding the hackers. S-BOX generation is the backbone of this algorithm. It has eight columns and 256 rows; each element consists of 8-bits. It replaces the input by another code to the output.[21].
RSA: RSA is an algorithm for public-key crypto graphy that is based on the presumed difficulty of fact oaring argeint eggers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in1978.AuserofRSAcreatesandthenpublishestheproduct of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, butwith currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.[1] Whether breaking RSA encryption is as hard as factoring is an open question known as the RSAproblem.

4. Implementation and experimental Results

Implementation**:** Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. For more security provides by 4.1.1 RSA Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key")cannot understand the content of the text. Encryption has long been the domain of spies and diplomats, but recently it has moved into the public eye with the concern of the protection of electronic transmissions and digitally stored data. Standard encryption methods usually have two basic flaws:

- A secure channel must be established at some point so that the sender may exchange the decoding key with the receiver; and
- There is no guarantee who sent a given message. Public key encryption has rapidly grown in popularity (and controversy, see, for example, discussions of the Clipper chip on the archives given below) because it offers a very secure encryption method that addresses the seconcerns.

In a classic cryptosystem in order to make sure that nobody, except the intended recipient, deciphers the message, the people involved had to strive to keep the key secret in a public-key cryptosystem. The public key cryptography solves one of the most vexing problems of all prior cryptography: the necessity of establishing a secure channel for the exchange of the key. The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is currently one of the favorite public key encryption methods. Here is the algorithm:

UMARAM: The UMARAM was designed by Ramesh G and R.Umarani in the year 2010. This algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of 16X 16 X 16. The S-Box consists of 16-slides, and each slide having 2-D of 16 x16. The numbers from 0 to 255 are arranged in random positions in each slide[20].

UR5:This algorithm was designed by G.Ramesh and Dr. R. Umarani in the end of the year 2010. A block encryption algorithm is proposed in this approach. In this Algorithm, a series of transformations have been used depending on S- BOX, XOR Gate, and AND Gate. The UR5 algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It uses eight rounds for encryption or decryption process. It over comes some drawback soft he other algorithms. It is more efficient and useable for the Wireless Local Area Network because it avoids the using of the same key with other packets within a message. The algorithm is simple and helpful in avoiding the hackers. S-BOX generation is the backbone of this algorithm. It has eight columns and 256 rows; each element consists of 8-bits. It replaces the input by another code to the output.[21].

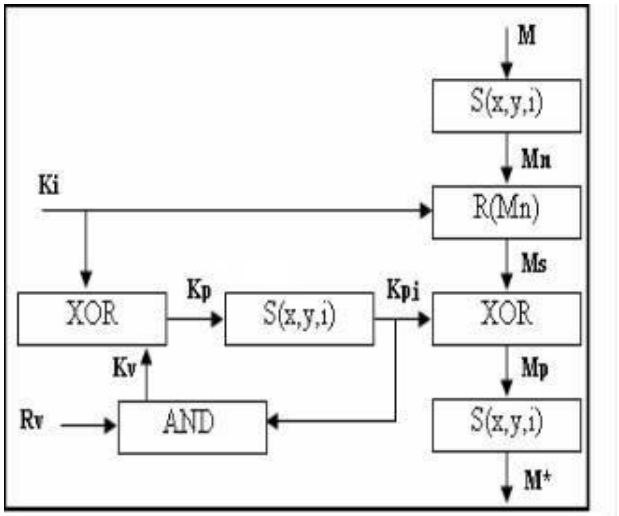


FIGURE. 4.1 Encryption process in each round

Fundamentally UMARAM performs only two operations on its input, bit shifting, and bit substitution. The key controls exactly how this process works. By doing these operations repeatedly and in a non-linear manner you end up with a result which cannot be used to retrieve the original without the key. Those familiar with chaos theory should see a great deal of similarity to what UMARAM does. By applying relatively simple operations repeatedly as stemcanachievea state of near total randomness. Consult one of the references in the bibliography for details. UR5: UR5 is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute- force attacks feasible. UR5provides a relatively simple method of increasing the key size of UMARAM to protect against such attacks, without the need to design a completely new block cipher algorithm.

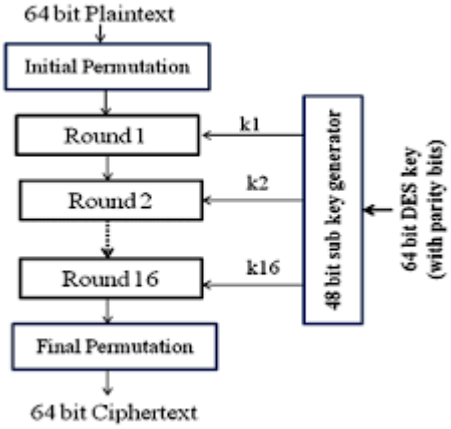
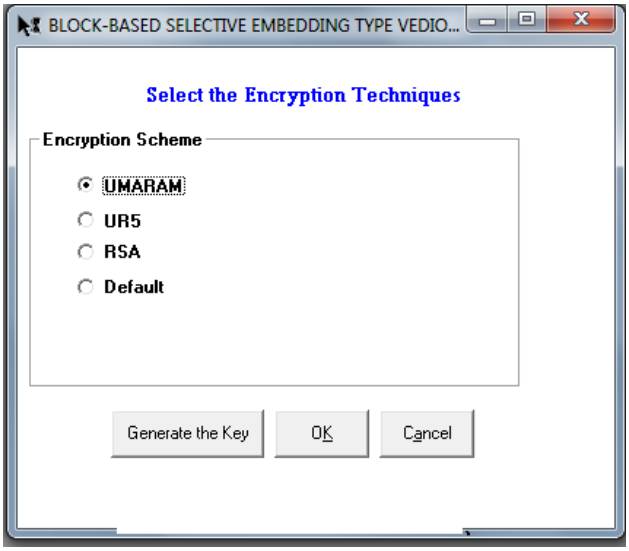


FIGURE 4.2. UR5 Working Model

Experimental Results: In Secret file, we can upload our video file with any format then to select which file used to hide in this by using cover file.



Finally to select the destination path to store our hidden file with password. When we retrieve the original file that time to provide same password. In this initial stage, while hiding the video data by choose any one of the encryption techniques.

5. Conclusion

A new video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH. The method is also robust to frame manipulation attacks via frame synchronization markers. First, we compared FZDH and QIM as the data hiding method of the proposed framework. We observed that FZDH is superior to QIM, especially for low embedding distortion levels. The frame work was tested with MPEG-2, H.264 compression, scaling and frame-rate conversion attacks. Typical system parameters are reported for error-free decoding. The results indicate that the framework can be successfully utilized in video data hiding applications.

Reference

[1]. M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: I. Fundamental issues and solutions," IEEE Trans. ImageProcess.,vol.12,no.6,pp.685–695,Jun.2003.

[2]. M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: II. Designs and applications," IEEE Trans. Image Process., vol. 12, no. 6, pp. 696–705, Jun.2003.

[3]. S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data hiding in H-264 encoded video sequences," in Proc. IEEE9th Workshop Multimedia Signal Process., pp. 373–376,Oct. 2007,.A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath,"Adaptive MPEG-2 video data hiding scheme,"in Proc. 9th SPIE Security Steganography Watermarking Multimedia Contents, pp.373–376.2007,

[4]. K.Wong,K.Tanaka,K.Takagi,andY.Nakajima, "Complete video quality-preserving data hiding," IEEE

[5]. A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, ―Adaptive MPEG-2 Video Data Hiding Scheme,‖ in Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX, 2007.

[6]. M. Wu, H. Yu, and B. Liu, "Data hiding in image and video I. Fundamental issues and solutions, "IEEE Transactions on Image Processing, vol. 12, pp. 685—695, June 2003.
[7]. E. Esen and A. A. Alatan, "Forbidden zone data hiding," in EEE International Conference on Image Processing, 2006, pp. 1393—1396.
[8]. B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods fordigital watermarking and information embedding," IEEE Transactions on Information Theory, vol. 47,May 2001, pp. 1423-1443, May2001,.
[9]. E. Esen, Z. Doğan, T. K. Ates, and A. A. Alatan, "Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding,"in IEEE 17th Signal Processing and Communications Applications Conference SIU,2009.
[10]. D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for turbo like codes," in Proc. 36thAllerton Conf. Communications, Control, and Computing, 1998, pp. 201— 210.
[11]. M. M. Mansour, "A Turbo-Decoding Message-Passing Algorithm for Sparse Parity-Check Matrix Codes," IEEE Transactions on Signal Processing, vol. 54, pp. 4376—4392, Nov.2006.
[12]. Z. Wei, K. N. Ngan, "Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Videoin DCT Domain," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, pp.337—346, Mar.2009.
[13]. M. Maes, T. Kalker, J. Haitsma, and G. Depovere, "Exploiting Shift Invariance to Obtain a High Payload in Digital Image Watermarking," in IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), vol. 1,1999.
[14]. T. Kalker, G. Depovere, J. Haitsma, and M. J. Maes, "Video watermarking system for broad castmonitoring," in Security and watermarking of multimedia contents Conference, SPIE Proceedings vol.3657 , 1999, pp. 103— 112.
[15]. M. Maes, T. Kalker, J. -P. M. G., J. Talstra, F. G. Depovere,andJ.Haitsma,"DigitalwatermarkingforDVD video copy protection," IEEE Signal Processing Magazine, vol. 17, pp. 47—57, Sep. 2000.
[16]. K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, pp. 1499—1512,Oct.2009.
[17]. G. Tardos, "Optimal probabilistic fingerprint codes," in Proceedings of the thirty fifth annual ACM symposium on Theory of computing (STOC '03), New York, NY, USA, 116—125.
[18]. B.Skoric,T.U.Vladimirova,M.Celik,andJ.C.Talstra, "Tardos fingerprinting is better than we thought," IEEE Transactions on Information Theory, vol. 54, no. 8, pp. 3663—3676,2008.
[19]. Ramesh, G. Umarani, R. ,UMARAM: A novel fast encryption algorithm for data security in local area network http://ieeexplore.ieee.org /xpl/ freeabs_all.jsp? arnumber=5670740
[20]. Ramesh, G. Umarani, R," UR5: A Novel Symmetrical Encryption Algorithm with Fast Flexible and High Security Based on Key Updation", European Journal of Scientific ResearchISSN1450-216XVol.77No.2(2012),pp.275-292.

