Selective Video Encryption using Bit XOR Technique

Mrinal Paliwal
Assistant Professor
Department of Computer Science and Engineering
P.K. Group of Institutions Mathura, India

Saddam Hussain
Assistant Professor
Department of Computer Science and Engineering
P.K. Group of Institutions Mathura, India

Abstract

Selective video encryption has advanced in recent years on the grounds that they require less time and guarantees security of video substance as well. There has been numerous selective Video Encryption Techniques, which are mind boggling and reliant on different elements like key sharing and bury and intra frame contrast and so on. In this paper we propose a selective video encryption calculation, which is quick, more minimal and free of key sharing component. Here we propose another plan for computerized video encryption. In this strategy we produce an encoded video by scrambled Video-frame. In light of a safe video conspire, a successful and summed up plan of video encryption. We have proposed another plan for video encryption which taking into account encryption of I-frame (video frame).Here we have taken a thought from grid estimation for creating the encoded I-frame. In this strategy, we gather the all video frame then take frame one by one structure it and select a key Image as key frame for encryption and unscrambling procedure, so this key picture is send through secure channel.

Keywords: encryption, video frame, I-frame, grid estimation, key, XOR

I. INTRODUCTION

In the late years with the advancement of web advances, video innovations have been extensively utilized as a part of TV, correspondence and interactive media, so security is needed on video information. In every segment of the business, extensive measure of information, pictures and videos with some secret data are created and put away and transmitted over the system. Furthermore, medicinal pictures with a tolerant's record may be shared among the specialists of diverse division of healing facility for distinctive clinical purposes. These picture and video may contain private data. So assurance of, such kind of sight and sound information in life time, is an issue. The information amount is expansive for the computerized video and the memory of the stockpiling gadgets and the transfer speed of the transmission channel are not unbounded, so it is not reasonable for us to store the full advanced video without preparing. Albeit much video encryption system has been grow yet they don't give such a great amount of effectiveness as far as encryption and decryption process. On the other hand, they are more mind boggling to actualize as a framework and are hard to be connected in a broad way.

Here we propose another plan for computerized video encryption. In this system we produce an encoded video by scrambled Video-frame. In light of a protected video plot, a successful and summed up plan of video encryption. We have proposed another plan for video encryption which in light of encryption of I-frame (video frame).Here we have taken a thought from grid count for producing the scrambled I-frame. In this technique, we gather the all video frame then take frame one by one structure it and select a key Image as key frame for encryption and decryption process, so this key picture is send through secure channel. Other frame scrambled by taking after calculation. Subsequent to applying the encryption calculation we join all frame, make video which is in encoded structure, send it from basic channel. It is a lattice calculation plan which utilizes an idea of Video-frame and XOR operation. This proposed plan has the capacity completely encode the video frame and have a superior execution that can be measured by distinctive Parameters.

II. REVIEW OF THE PREVIOUS WORK

A. Partial Encryption Schemes for Video

1) *Meyer and Gadegast, 1995*

This system is proposed for MPEG videos. This strategy utilizes customary encryption routines RSA or DES in CBC mode to encode MPEG video stream. It executes 4 level of security. (i) Encrypting all stream headers. (ii) Encrypting all stream headers and all DC and lower AC coefficients of intracoded pieces. (iii) Encrypting I-frames and all I-hinders in P- and B frames.(iv) Encrypting all the bit streams. The quantity of I pieces in P or B frames can be of the same request as the quantity of I squares in I frames. This diminishes extensively the productivity of the selective encryption plan. Encryption proportion may fluctuate in view of which parameters are encoded. Encoding just headers have less encryption proportion. However, scrambling all the bit streams have 100% encryption proportion. Velocity of this technique again changes in view of customary calculation being used,

for example, DES or RSA and number of parameters that are encoded. Numerous security levels can be acquired. The encoder proposed is not MPEG agreeable [6].

2) *Shi and Bhargava, 1998*

The creators [8] proposed video encryption calculation (VEA) which utilizes a mystery key to haphazardly change the indications of all DCT coefficients in a MPEG stream. It is quick as it works on a little partition of unique video. It is more effective than DES calculation on the grounds that it just specifically encodes a little number of bits of the MPEG packed video and chose bit is just XORed one time with the comparing bit of the mystery key. VEA does not shield from plaintext assault gave the assailant knows the first video image (plaintext and figure content). The creators introduce another form of VEA decreasing computational unpredictability; it scrambles the sign bits of differential estimations of DC coefficients of I-casings and sign bits of differential estimations of movement vectors of Band P-outlines. The encryption of the image got will permit us to get the key length and even process the mystery key by picked plaintext assault.

3) *Shi, Wang and Bhargava, 1999*

Another variant of the adjusted VEA introduced is proposed, called ongoing video encryption calculation (RVEA) [9]. It scrambles chose sign bits of the DC coefficients and/or sign bits of movement vectors utilizing DES or IDEA. It chooses at most 64 sign bits from every full scale piece. RVEA accomplishes the objective of diminishing and bouncing its reckoning time by constraining the most extreme number of bits chose. The differential encoding of DC coefficients and movement vectors in MPEG pressure builds trouble of breaking RVEA encoded videos. On the off chance that the beginning speculation of a DC coefficient wrong, it is exceptionally hard to figure the accompanying DC values effectively.

4) *Wu and Kuo, 2001*

It [10] is in view of a situated of perceptions, the creators call attention to that vitality fixation does not mean clarity focus. Undoubtedly, they talked about the system proposed by Tang. They demonstrate that by altering DC values at an altered esteem and recuperating AC coefficients (by known or picked plaintext assaults), a semantically decent reproduction of the image is gotten. Notwithstanding utilizing a little portion of the AC coefficients does not completely annihilate the image semantic substance. They propose two plans for the most well known entropy coders: numerous Huffman tables (MHTs) for the Huffman coder and different state file (MSI) for the QM math coder.

5) *Wen, Severa, Zeng,Luttrel, and Jin, 2002*

A general specific encryption approach for altered and variable length codes (FLC and VLC) is proposed in [11].FLC and VLC codewords comparing to critical data conveying fields are chosen. At that point, each codeword in the VLC and FLC (if the FLC code space is not full) table is allocated a settled length code list, when we need to encode the linking of some VLC (or FLC) codewords, just the records are encoded (utilizing DES). At that point the encoded connected files are mapped back to an alternate yet existing VLC. The encryption procedure bargains the pressure proficiency. Undoubtedly, some short VLC codewords (which are the most likely/continuous) can be supplanted by more ones. This is adversarial with the entropy coding thought. The proposed plan is completely consistent to any pressure calculation that uses VLC or FLC entropy coder[1-4].

6) *Bergeron and Lamy-Bergot, 2005*

A punctuation agreeable encryption calculation is proposed for H.264/AVC [13]. Encryption is embedded inside of the encoder. Utilizing the proposed strategy permits to embed the encryption component inside the video encoder, giving a safe transmission which does not modify the transmission process. The bits "chose for encryption" are picked regarding the considered video standard as indicated by the accompanying govern: each of their scrambled arrangements gives a non-desynchronized and completely standard consistent bit stream. This should specifically be possible by scrambling just parts of the bit stream which have no or an irrelevant effect in advancement of the unraveling procedure, and whose effect is subsequently absolutely a visual one. Around 25% of I-cuts and 10–15% of P-cuts are encoded. Since intracoded cuts can speak to 30–60%, the encryption proportion is relied upon to be moderately high. The fundamental downside of this plan is the absence of cryptographic security. Without a doubt, the security of the scrambled bit stream does not depend all the more on the AES figure. It relies on upon the span of the agreeable codewords. Thus, the dispersion of the AES figure is lessened to the plaintext space size. Likewise, a predisposition is presented in the figure content. This predisposition relies on upon the key size and the plaintext spaces[6].

7) *Lian, Liu, Ren and Wang, 2006*

This plan is proposed for AVC [14]. Amid AVC encoding, such delicate information as intra forecast mode, buildup information and movement vector are scrambled incompletely. The encryption plan is of high key affectability, which implies that slight distinction in the key reasons awesome contrasts in figure video and that makes measurable or differential assault troublesome. It is hard to apply known plaintext assault. In this encryption conspire, every cut is scrambled under the control of a 128 bit sub-key. Along these lines, for every cut, the savage power space is 2^128; for the entire video, the animal power space is 2^256 (the client key is of 256 bit). This savage power space is too expansive for assailants to break the cryptosystem. As per the encryption plan proposed here, both the surface data and the movement data are scrambled, which make it hard to perceive the composition and movement data in the video outlines[7].

III. METHODOLOGY OF THE RESEARCH WORK

This section briefly discusses various types of videos exists and encryption algorithms used for the video encryption. The encryption and decryption of a plain text or a video stream can be done in following ways:

A. Selective Encryption

It is also called as partial encryption & is a subcategory of variable encryption. The algorithms in this will selectively encrypt the bytes within video frames. As these algorithms are not encrypting each and every byte of video data, it reduces computational complexity. To save computational complexity only particular video bytes maybe encrypted[3-6].

1) *Classification OF Selective Video ENCRYPTION*

Selective Video encryption algorithms can be classified into four basic categories:

1) Completely Layered Encryption

In this method, the entire video is first compressed and is then encrypted using traditional algorithms like RSA, DES, and AES. This technique is not applicable in real time video applications due to heavy computation and very low speed.

2) Encryption Using Permutation

Here, the video content is scrambled using a permutation algorithm. The entire video content may be scrambled or only particular bytes. A permutation list may be used as a secret key for encryption.

3) Perceptual Encryption

After encryption using this technique the video will still be perceptible. The audio/video quality can be controlled continuously.

B. MPEG – 1 Video Encoding

In MPEG-1 video coding model [Gall], a video is made out of a succession of gathering of pictures (GOPs). Each GOP is a progression of I, P and B pictures. I pictures are intra edge coded with no reference to different pictures. P pictures are predicatively coded utilizing a past I or P picture. B pictures are bidirectional introduced from the past and tailing I and/or P pictures. The relative recurrence of event of I, P and B pictures can be controlled by the applications. Every photo is isolated into full scale squares. A large scale square is a 16×16 pixel cluster. Large scale pieces fitting in with I pictures are spatially encoded. Those fitting in with B and P pictures are transiently inserted from the relating reference picture(s), and the blunder between the real and reference qualities is figured[8-12].

IV. PROPOSED WORK

We have proposed another plan for video encryption which in view of encryption of I-casing (video frame).Here we have taken a thought from grid computation for creating the encoded I-outline. In this strategy, we gather the all video outline then take outline one by one structure it and select a key Image for encryption and decryption process, so this key image is send through secure channel. Other edge scrambled by taking after calculation. In the wake of applying the encryption calculation we consolidate all casings, make video which is in scrambled frame, and send it from straightforward channel.

Let V be a video grouping comprising of n casings meant by I1, I2, . . . Im. We will execute the calculation in two pass utilizing Keys K1 and K2. In the first pass key K1 is utilized to encode the odd casings by performing Bit XOR with first key1. In the second pass key K2 is utilized to scramble the even edges by performing the Bit XOR operation with second key 2. Presently this is the last encoded image. At that point make the advanced video through these encoded images and send this video through basic channel. However, key image transmitted through secure channel. At the recipient side opposite procedure is connected.

A. Proposed Algorithm:

1) *Encryption algorithm:*
   1) Input a video.
   2) Convert the video into frames.
   3) Separate the three frames(I,B,P)
   4) Perform encryption on I-frames (To reduce computation)
   5) B and P frames remain unencrypted.
   6) Apply lossless compression to compress the frames(Reduces size of video)
   7) Transmit the video (Cipher video) into the channel.
2) *Decryption Procedure:*
   1) Input a cipher video.
   2) Break the video into frames.
   3) Decompress the frames.
   4) Apply the key and decrypt the encrypted R channel.
   5) Combine the entire channel.
   6) Convert the frames into video.
   7) Output will be a video.
3) *Algorithm for Encryption*

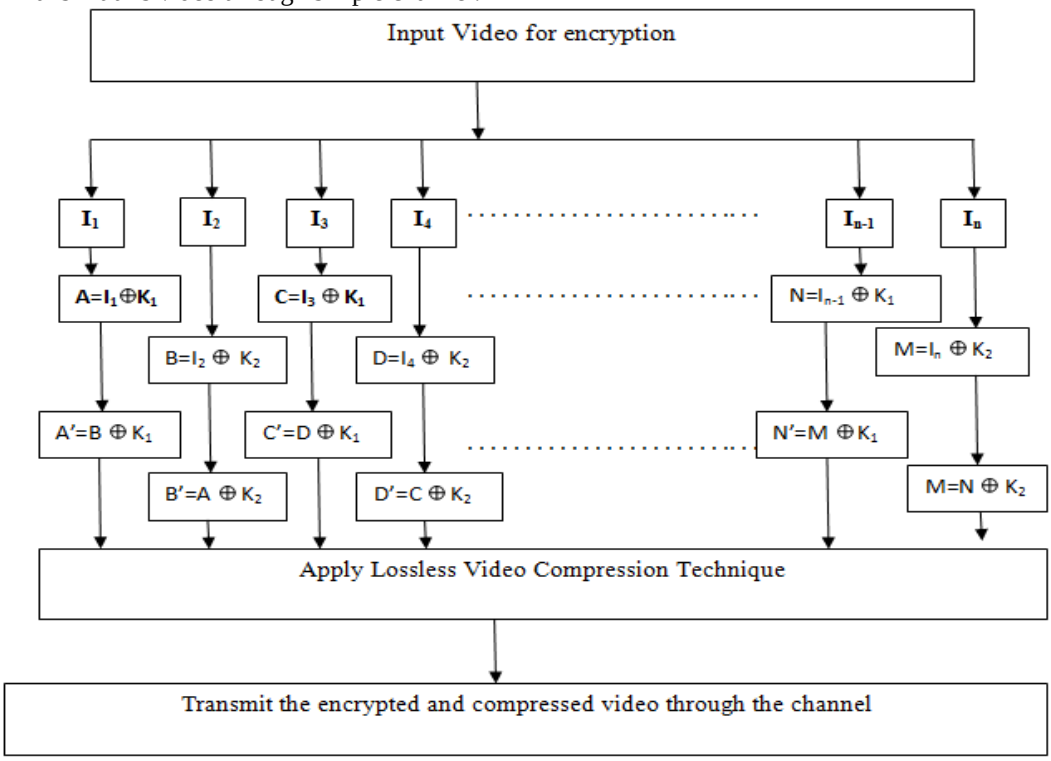
The following is a proposed algorithm for encryption.

Definition:

Vn: Video stream, In: Video Frames

n= {0,1,2……}
K1, K2: Key Image
α: Sorting function

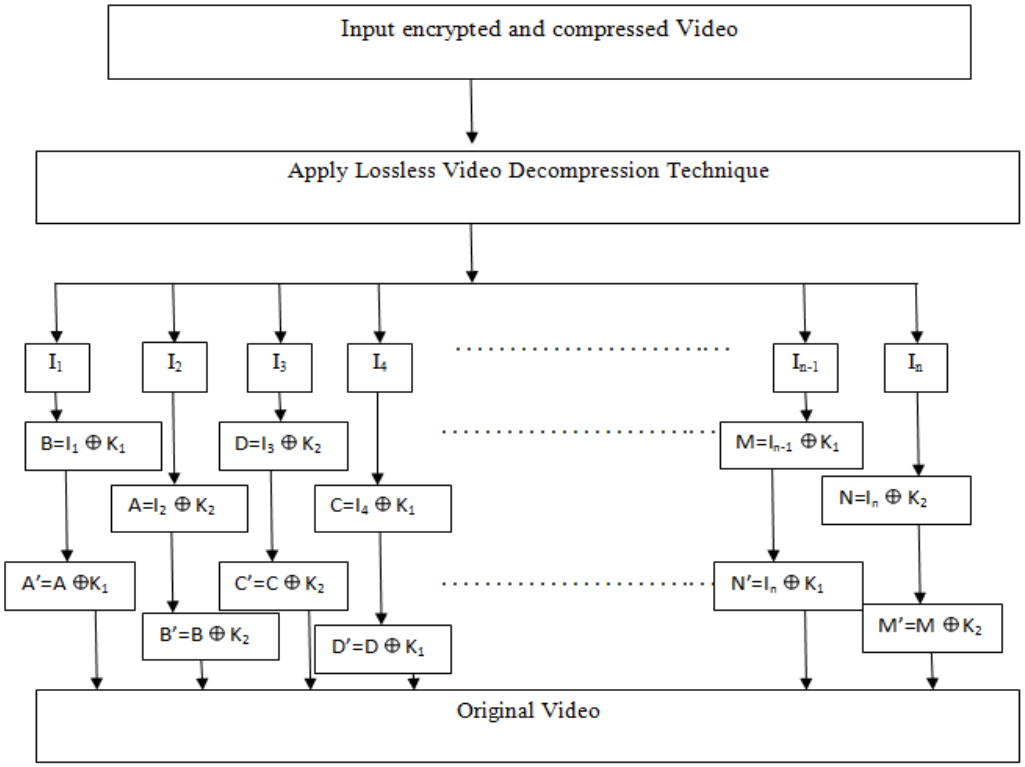
1) Step1 Choose any video stream V.
2) Step2 Compute all frame of video stream V (I1, I2, I3…..In).
3) Step3 An= In , Where n= 2, 3 …n.
4) Step4 A=I1 BitXOR K1(Encrypt odd frame with K1)
5) Step5 B=I2 BitXOR K2 (Encrypt even frame with K2)
6) Step6 Repeat step 3 & step 4 for all frames.
7) Step7 A'=B BitXOR K1
8) Step8 B'=A BitXOR K2
9) Step9 Repeat step 7 & step 8 for all frames.
10) Step10 Apply Lossless Compression Technique.
11) Step11 Construct video from Encrypted frame.
12) Step12 Transmit this video through simple channel.



4) *Algorithm for Decryption*

The following is a proposed algorithm for decryption.
Definition:
Vn: Video stream, In: Video Frames
n= {0,1,2……}
K1, K2: Key Image

1) Step1 Receive Video Stream data and first frame, Random sequence no and Key image.
2) Step2 Apply Lossless Decompression Technique.
3) Step3Compute all frame of video stream V (I1, I2, I3…..In).
4) Step4 An= In , Where n= 2, 3 …n.
5) Step5 B=I_1 BitXOR K1(Encrypt odd frame with K1)
6) Step6 A=I_2 BitXOR K2 (Encrypt even frame with K2)
7) Step7 Repeat step 3 & step 4 for all frames.
8) Step8 A'=A BitXOR K1
9) Step9 B'=B BitXOR K2
10) Step10 Repeat step 7 & step 8 for all frames.
11) Step11 Construct original video through I-frame.



B. Analysis of Proposed Model

We analyse the performance of encryption and decryption of two different video formats and frame sizes and find out the quality and speed of encryption and decryption of the same. We analyse them on below given two formulas:

Encryption Rate=no.of FrameX size/time (2)

Bitwise encryption rate=size of video/time (3)

1) *AVI Video Input*

In this case we input uncompressed AVI video of 352 frames of 480X640 pixels of 2.39 MB

Fig. 1: Original Video Frames

Fig. 2: Encrypted Video Frames

Fig. 3: Decrypted Video Frames

Table 1:
Comparison of Performance of both the videos in terms of speed AVI Video

No. Of Frames	*352*	*313*
Size of Frames	*480*640*	*240*320*
Encryption Time (sec)	*88.128099*	*26.00576*
Decryption Time (sec)	*75.670624*	*24.72528*
Pixels Encryption Rate (Pixels/Sec)	*1227013.872*	*924349.1*
Pixels Decryption Rate (Pixels/Sec)	*1429014.245*	*972219.6*
Bitwise encryption rate (KB/Sec)	*27.7705*	*132.303*
Bitwise decryption rate (KB/Sec)	*80.2467*	*50.9457*

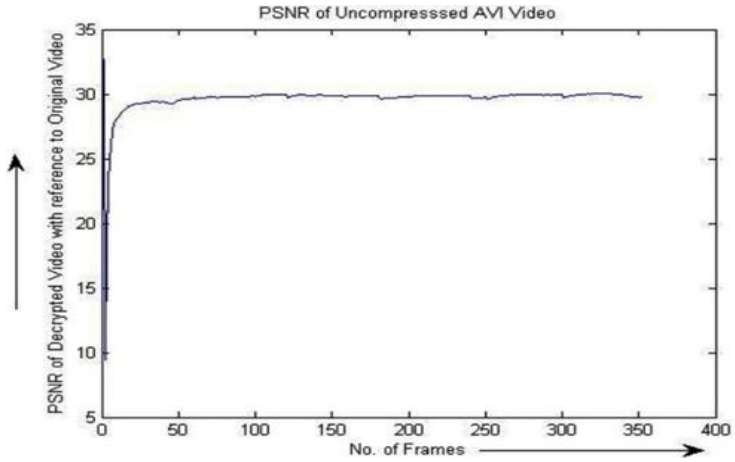


Fig. 4: PSNR values of AVI decrypted video with reference to Original Video

V. CONCLUSION

In the above work we have proposed a method of specific video encryption which is altogether key autonomous and quick. The investigation of above is performed on two distinct sorts of video organizations one is compacted one and other one is uncompressed of diverse casing sizes and practically comparable no. of video casings. By this investigation it can be demonstrated that the encryption performed, by utilizing I outline as key decreases the obligation of key sharing. The encryption and decryption time of packed video is less, whilst the same for the uncompressed video is all the more however the edge size of uncompressed video size is high yet the encryption rate of compacted video is very nearly 6 seasons of uncompressed video.

As far as nature of video quality after decryption for both of the video configurations is verging on comparative however it is differing all the more in the event of H.264 organization due to pressure of video as well yet the PSNR are just about of 30 db, in this way demonstrating that nature of video is likewise kept up in both the cases. Next we contrasted the execution of proposed method and a standout amongst the most prominent particular video encryption strategy called MVEA and as the outcome (tables and charts) demonstrates the rate of encryption for proposed procedure is much speedier than that of MVEA Algorithm both for AVI and H.264 Video.

A. Future Work

In future using key sharing, independent video encryption technique can further be more enhanced with complex encryption techniques, also the researchers may attempt to use zig-zag and selective encryption to ensure fast and secure video encryption.

REFERENCES

[1] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Video," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.
[2] M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.
[3] M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption ofUncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, September 9-11, 2002.
[4] M. Podesser, H.-P. Schmidt and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments," 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7, 2002.
[5] A. Pommer and A. Uhl, "Selective Encryption of Waveletpacket Encoded Image Data: Efficiency and Security,"Multimedia Systems, Vol. 9, No. 3, 2003, pp. 279–287, DOI: 10.1007/s00530-003-0099-y.
[6] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin, 1995.
[7] G.A. Spanos and T.B.Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked Real Time Video," in Proceedings of the International Conference on Computer Communications and Networks,1995, pp. 2-10.
[8] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," in Proceedings of the 6th ACM International Conference on Multimedia, 1998, pp. 81–88.
[9] C. Shi, S. Y.Wang, and B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography," in Proceedings of the International Conference on Parallel and Distributed Processing Algorithms and Applications, 1999,pp. 191–201.
[10] C.-P. Wu and C.-C. J. Kuo, "Fast Encryption Methods for Audiovisual Data Confidentiality," in Proceedings of SPIE, 2001, Vol. 4209, pp. 284–295.
[11] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A Format-Compliant Configurable Encryption Framework for Access Control of Video," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 6, 2002, pp. 545–557.
[12] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Transactions on Multimedia, Vol. 5, No. 1, 2003, pp. 118–129.