Communication in Network using Wavelet Transform

C. Parthasarathy
Assistant Professor, IT Dept
Sri Chandrashekarendra Saraswathi Viswa Mahavidyalaya University,
Enathur, Kanchipuram – 631 561

C.S. Ramanathan
Head, Dept. of Computer Science
Sri Sankara Arts & Science College
Enathur,
Kanchipuram – 631 561

Dr.S.K.Srivatsa
Senior Professor
St. Joseph's College of Engg,
Jeppiaar Nagar,
Chennai-600 064

ABSTRACT
Huge amounts of digital visual data are stored on different media and exchanged over various sorts of networks nowadays. We propose new measures and techniques for encryption of image. We show that both statistical and pattern classification techniques using our proposed measures provide reasonable discrimination schemes for detecting embedding of different levels. We propose the use of wavelet transforms for steganalysis. As a consequence, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for these data types. A relatively new field, denoted "Multimedia Security", is aimed towards these emerging technologies and applications. Several dedicated international meetings have emerged as a forum to present and discuss recent developments in this field, among them "Security, Steganography, and Watermarking of Multimedia Contents" as the most important one. Further meetings are "Communications and Multimedia Security (CMS)" and the "ACM Multimedia Security Workshop". Besides watermarking, steganography, and techniques for assessing data integrity and authenticity, providing confidentiality and privacy for visual data is among the most important topics in the area of multimedia security, applications range from digital copy rights management to secured personal communications.

Keyword Video Encryption, Permutation, steganalysis, Wavelet filters.

1. INTRODUCTION
Many digital services, such as pay-TV, confidential video conferencing, medical and military imaging systems, require reliable security in storage and transmission of digital images/videos. As the rapid progress of Internet in the digital world today, the security of digital images/videos has become more and more important [9]. In recent years, more consumer electronic services and devices, such as mobile phones and PDA (personal digital assistant), have also started to provide additional functions of saving and exchanging multimedia messages [11]. The prevalence of multimedia technology in our society has promoted digital images and videos to play a more significant role than the traditional dull texts, which demands a serious protection of users' privacy. To fulfill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel [12]. Wavelets are mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale.

2. IMAGE AND VIDEO ENCRYPTION
There are two basic ways to encrypt digital images: in spatial domain or in transform domain. Because digital videos are generally compressed in DCT (discrete cosine transform) domain, almost all video encryption algorithms work in DCT domain. Due to the recent prevalence of wavelet compression technique and the adoption of wavelet transform in JPEG2000 standard, in recent years image/video encryption algorithms working in wavelet domain also attract some attention. Some novel image/video compression algorithms have also been proposed to realize joint compression-encryption schemes[7]. Although many efforts have been devoted for better solutions for image and video encryption, the current security analyses of many schemes are not sufficient, especially on the security against known/chosen-plaintext attack. What's worse, many selective encryption schemes are indeed insecure against cipher text-only attack, due to the visible information leaking from unencrypted data[8]. In this section, we provide a comprehensive survey on image and video encryption schemes without using chaos theory, as a background of chaos-based encryption schemes. Before that, a widely-used idea in the image/video encryption community, called selective (or partial) encryption, is firstly introduced so as to facilitate the security evaluations of selective image/video encryption.

3. VIDEO IDEO ENCRYPTION SCHEMES (MPEG ENCRYPTION SCHEMES)
The most frequently used idea of MPEG encryption is to encrypt selective frames, macro blocks, DCT coefficients and/or motion vectors. The following is a list of selective data for encryption in different schemes (from light to heavy encryptions):

- All header information (and partial blocks).
- Selective AC coefficients of Y/V blocks in all I-frames.
- Selective leading DCT coefficients of each block.
- Selective DCT coefficients of each block and motion vectors.
- All or selective motion vectors.
- All I-frames and the header of the MPEG video sequence.
- All I and P frames, or all I-frames and I-macro blocks in B and P frames.
- All or selective I-macro blocks and the headers of all predicted macro blocks.

Another frequently used idea is to secretly permute all or selective macro blocks, DCT coefficients and/or motion vectors.

- In DCT, coefficients are secretly permuted within each block, and the DC coefficient is split into two halves and AC coefficient is set to be the higher half of the DC coefficient.
- In the following, three operations are combined to encrypt images: secret permutations of DCT coefficients, selective encryption of DCT coefficients, and motion vector scrambling. In this scheme, several blocks compose a segment, and DCT coefficients in different blocks at the same frequency are secretly permuted.
- In the secret permutations of DCT coefficients and the encryption of sign bits of DC coefficients are combined to realize a selective encryption scheme.
- In different basic units are secretly permuted: macro blocks, 8×8 blocks, and run-level code words.

The first three schemes above are all insecure against cipher text-only attack and known/chosen plaintext attacks. Another disadvantage of secret permutation of DCT coefficients is the

expansion of the video size. In three encryption schemes were proposed that encrypt selective sign bits of DCT coefficients and motion vectors, which are respectively called VEA (video encryption algorithm), MVEA (modified VEA) and RVEA (real-time VEA).

- VEA is a simple cipher XOR-ing all sign bits with a repeated m-bit key. It is too simple to resist cipher text-only attack and known/chosen plaintext attacks.
- MVEA is a simple modification of VEA, in which only sign bits of DC coefficients in I-frames and sign bits of motion vectors in B and P frames are XOR-ed with the secret key. In fact, MVEA is weaker than VEA.
- RVEA is a combined version of VEA and MVEA, where the XOR operations are replaced by a traditional cipher. For each macro block, at most 64 sign bits are encrypted with the order from low frequency to high frequency. Although RVEA is the strongest VEA cipher, the attempt of using unencrypted AC coefficients to reconstruct some visible information is still possible.

4. GENERIC VIDEO ENCRYPTION SCHEMES

VEA was proposed to encrypt video stream: divide each 128-byte piece of the plain-video into two 64-byte lists: an Odd List and an Even List, and the Even list is XOR-ed by the Odd list and then encrypted. This VEA can reduce the encryption load by 50%. An extended VEA with lighter encryption cost was proposed into support the error-tolerability property. A simple video encryption scheme was proposed, which applies a secret linear transformation on each pixel value[1]. All pixels in the same macro block are encrypted with the same secret parameters set. A similar encryption scheme was proposed. Both schemes are insecure against known/chosen-plaintext attacks. In combining a fast (stream) cipher and a secure (block) cipher was suggested to achieve overall fast encryption of digital videos. The encryption procedure can be described as follows. Assume that C, M respectively means the cipher text and the plaintext, and that SE, FE respectively mean the secure cipher and the fast cipher,

C = {SE (K, Mik+1), FE (Ki+1, Mik+2Mik+2 · · ·M (i+1) k)} ti =0,

Where Ki+1 = SE (K, SE (K, Mik+1)). Two ciphers with high encryption speeds were designed. Since partial plaintexts are selected to be encrypted with a securer cipher but others are selected to be encrypted by a faster cipher, such a mechanism can be regarded as a generalized version of selective encryption.

5. CHAOS – VIDEO ENCRYPTION

SCAN-based encryption for lossless compressed videos: The new generations of SCAN-based image encryption schemes were also extended to encrypt videos[2]. The plain-video is compressed with a frame-difference-based light lossless compression algorithm, and then encrypted with the new SCAN-based encryption algorithm.

5.1 CVES (Chaotic Video Encryption Scheme)

A chaos-based encryption scheme called CVES using multiple chaotic systems was proposed. CVES is actually a fast chaotic cipher that encrypts bulky plaintext frame by frame[3]. The basic idea is to combine a simple chaotic stream cipher and a simple chaotic block cipher to construct a fast and secure product cipher. It was pointed out that the original CVES is not sufficiently secure against the chosen-plaintext attack, and an enhanced version of CVES was proposed by adding cipher text feedback. Diagrammatic view of the enhanced CVES, where CCS, ECS(1), ECS(2n) are all piecewise linear chaotic maps, and m-LFSR1, m-LFSR2 are the perturbing PRNG of CCS, ECS respectively. The encryption procedure of CVES can be described as follows. Each plain-block is first XOR-ed by a chaotic signal pseudo-randomly selected from chaotic orbits of the 2n ECS (encryption chaotic systems), and then substituted by a pseudo-random S-box generated from all chaotic orbits of the 2n ECS. Initial tests have shown that the encryption speed of CVES is competitive with most traditional ciphers, and is only a little slower than the AES reference code.

6. VLC TABLE CODEWORD PERMUTATION

The coefficients in a transformed 8*8 DCT block are scanned in zigzag order; each non-zero value is encoded using a predefined entry in a VLC (variable length code) table. The actual value does not only depend on this nonzero value, but also on the number of coefficients with 0 values immediately before this value. The entries in this table can be as long as 16 bits, and to be decodable any codeword must not be the prefix of another codeword (this requirement is also called "Fano condition").

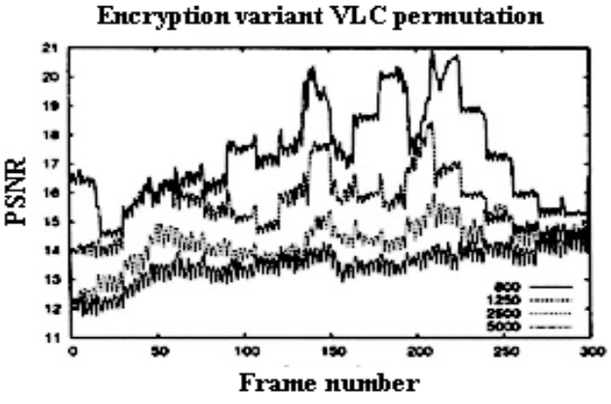

Fig 1. (a) Resulting quality for 4 different bitrates

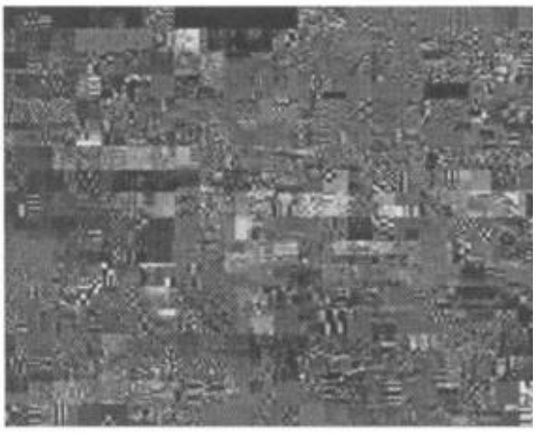

Fig 1. (b) frame #180,bit rate 5000 kb/s

7. MACRO BLOCKS PERMUTATION

Each frame within a video consists of the same number of macro blocks; each macro block contains such data as quantized coefficients from the Y, U and V bands, or motion vectors. A variant to encrypt videos is to exchange the macro blocks within a frame. The key for this encryption method is used as a seed value for a PRNG which generates a permutation. This is an encryption variant which is annoying but not very secure. The reason is that based on the correlation of border pixels the originally neighboring macro blocks can be regained. This effect becomes even easier when there are more frames available which are permuted using the same order[6]. So to keep this approach reasonably secure it is necessary to change the key as often as possible, at best with every frame.

8. DCT BLOCK PERMUTATION

Similar to the approach where complete macro blocks are exchanged it is possible to exchange the individual 8*8 DCT coefficient blocks. By permuting the smaller blocks the confusion being created is bigger, and reconstruction becomes more difficult but it is possible. Additionally the algorithm does not discriminate between DCT blocks from the Y plane and DCT blocks from the U and V planes.

9. MOTION VECTOR PERMUTATION

Similar to the macro block permutation and the DCT block permutation it is possible to permute the motion vectors which are assigned to distinctive macro blocks. Within a predicted frame each macro block can be either I block or a predictive block, motion vectors are just assigned to the latter. These vectors can be permuted according to an order provided by a PRNG, where the seed is the key. The distortion which results from this encryption method is very light, since it affects no I-frames and no I-blocks, and since in many cases many motion vectors within a frame share the same overall direction. However the effects increase with the number of successive P- or B- frames, as they vanish with the next I-frame (obviously). This variant is related to the MVEA and RVEA methods.

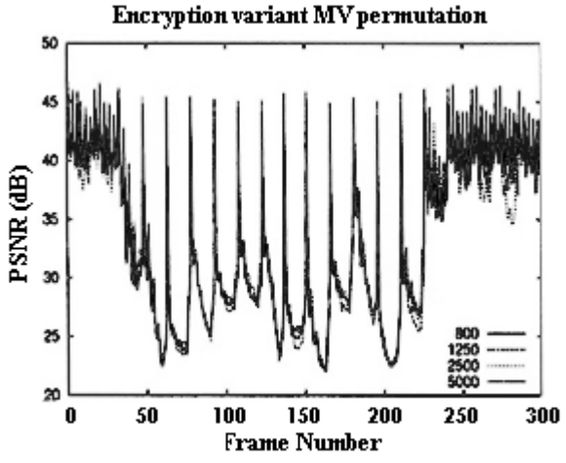

Fig 2. (a) Resulting quality for 4 different bitrates

Fig 2. (b) frame#100, bit rates 5000(kb/s)

10. SOME SPECIAL FEATURES OF IMAGE / VIDEO ENCRYPTION SCHEMES

In image/video encryption systems, some features are required to support special functions of diverse multimedia services in different environments. These features are generally realized with a combination of compression and encryption, and impose some limits on the design of the image/video encryption algorithms[5].

10.1 Format-compliance

This feature means that the encrypted image/video is still decodable at the receiver end without the knowledge about the decryption key. For online stream multimedia services, especially those running in wireless environments, the transparency property is desirable to eliminate the problems caused by loss or uncorrected data. Transparency property is also useful to ease concatenating other post processing devices (such as digital watermarking) to the whole compression/encryption system errors. To achieve transparency, the encryption procedure should not destroy the syntax structure of the encrypted file/stream; that is, the descriptive information of the file/stream should be left unencrypted.

- Scalability: Scalability means multi-level security for different applications with flexible parameter settings. The embedded multi-layer structure, i.e., the fine granularity scalability (FGS), of JPEG2000 images and MPEG-2/4 videos makes scalable encryption easy and natural. The basic idea to realize scalability is to encrypt partial layers and/or partial data in selected layers. Scalability can be considered as a control mechanism for the visual quality of the encrypted image/video.
- Perceptibility: Perceptibility means partial encryption of visible information of the plain-image/video, which is useful for pay-after-trial services of digital multimedia, such as pay-TV and VOD services. It is a generalization of scalable (multi-layered) encryption, and does not depend on the embedded multi-layered structure of the encrypted image/video. Two typical perceptual encryption schemes for JPEG images and MP3 music were proposed in and respectively.
- Error-tolerability: The concept of error-tolerating (or error-resilient) encryption was investigated. It is undesirable if an encrypted stream cannot be decoded when some bit errors are introduced, which frequently occurs in multimedia applications particularly in wireless environments. However, the avalanche property of good ciphers means high sensitivity to errors, which may lead decryption to fail in some cases. .

11. WAVELET BASED TECHNIQUES

The most wavelet-based compression schemes use arithmetic coding as their entropy coding stage which does not provide a one-to-one correspondence among symbols and code words like Huffman coding as used in DCT-based systems does[4]. Therefore, techniques manipulating single coefficients cannot be employed in the transform domain.

11.1 Secret wavelet filters: Parameterization approach

The Discrete Cosine Transform and Discrete Wavelet Transform are the most widely used transforms for frequency domain encryption of images. However the computational complexity of the transforms that involve floating point operations is quite high. Motivated by the fact that integer transforms lower the computational complexity, we propose the use of orthogonal polynomials based transformation for image encryption in this section by analyzing the image formation system. Here, a linear 2-d image formation system is considered around a Cartesian coordinate separable, blurring, point spread operator in which the image *I* results in the superposition of the point source of impulse weighted by the value of the object *f*. Expressing the object function *f* in terms of derivatives of the image function I relative to its Cartesian coordinates is very useful for de-correlating the image. The point spread function M(x, y) can be considered to be real valued function defined for (x, y) ε X x Y, where X and Y are ordered subsets of real values. In case of gray level image of size (n*n) where X (rows) consists of a finite set, which for convenience can be labeled as {0, 1, …. n-1}, the function M(x, y) reduces to a sequence of functions.

$M(i,t) = u_i(t), I=0, 1,. . . . . , n-1 \quad \ldots (1)$

The linear two dimensional transformation can be defined by the point spread operator $M(x, y)(M(i, t) = ui(t))$ as shown in Eq. (2).

$$\beta'(\varsigma,\eta) = \int_{x \in X} \int_{x \in Y} M(\varsigma, x)\, M(\eta,y)\, I(x,y)\, dxdy \ldots (2)$$

Considering both X and Y to be a finite set of values {0, 1, and 2 … n 1}, Eq. (2) can be written in matrix notation as follows

$$|\beta'_{tf}| = (|M| \otimes |M|)^{t} |I| \quad \ldots (3)$$

Where ⊗ is the outer product, $|\beta'_{ij}|$ are n2 matrices arranged in the dictionary sequence, $|I|$ is the image, $|\beta'_{ij}|$ are the coefficients of transformation and |M| is

$$|M| = \begin{vmatrix} u_0(t_1)\, u_1(t_1) \ldots u_n\text{-}1(t_1) \\ u_0(t_2)\, u_1(t_2) \ldots u_n\text{-}1(t_2) \\ \vdots \\ u_0(t_n)\, u_1(t_n) \ldots u_n\text{-}1(t_n) \end{vmatrix} \quad \ldots (4)$$

we consider the set of orthogonal polynomial $u_0(t)$, $u_1(t)$,…., $u_{n-1}(t)$ of degrees 0,1,2,…., n-1, respectively to construct the polynomial operators of different sizes from Eq.(4) for n≥2 and ti =i.

In order to construct the orthogonal polynomial basis, we first propose set of orthogonal polynomials in Eq.(4)

$$u_{i+1}(t) = (t - \mu)\, u_i(t) - b_i(n)\, u_{i-1}(t) \text{ for } i \geq 1 \quad \ldots (5)$$
$$u_1(t) = t - \mu, \text{ and } u_0(t) = 1,$$

Where

$$b1(n) = \frac{\langle u_t, u_t \rangle}{\langle u_{t-1}, u_{t-1} \rangle} \frac{\sum_{t=1}^{n} u^2(t)}{\sum_{I-1}^{n} u^2}$$

And

$$\mu = (1/n) \sum_{t=1}^{n} t$$

considering the range of values of t to be $t_{1=I,I=1,2,3,\ldots}n$, we get

$$b_t(n) = \frac{i^2 (n^2 - i^2),}{4 (4 i^2 - 1)}$$

$$\mu = \frac{1}{n} \sum_{t=1}^{n} t = \frac{n+1}{2}$$

12. THE PROPOSED ENCRYPTION ALGORITHM

The steps involved in the proposed encryption process are given below.

Input: Cover image of size H x W, secret key
Output: Encrypted image

Step 1: Divide the input cover image of size H x W pixels into non-overlapping blocks of size N x N where N<H, W. Let each block be denoted as $[I_{ij}]$ $(0 \leq i < H/N, 0 \leq j < W/N)$.
Step 2: Apply the proposed Orthogonal Polynomials based transform and compute the block of OPT coefficients [β'ij] as described in Eq. (4).
Step 3: Perform the steps 4 thro' 9 for all the OPT coefficient blocks, {[β'ij]|≤I<H/N,0≤j<W/N}.
Step 4: Arrange the elements of [β'ij] in a 1-D zigzag sequence to form the feature vector fv.
Step 5: Choose the first n low frequency OPT coefficients from fv to form lfv, where n is calculated using the block size and the secret key k.
Step 6: Select coefficients from lfv using the pseudorandom sequence S_1 generated using the sub-key k_1 and encrypt their sign-bits.
Step 7: Scale the magnitude of the DC coefficient using the scaling factor S generated from the secret key k.
Step 8: Using the pseudo-random sequence S_2 generated using the sub-key k_2, select the coefficients to whose bits are rotated in the direction dr for np number of positions to get the bit permuted feature vector $[lfv_{bi}]$. Here,
dr = left : $k_2(0) = 0$
right: $k_2(0) = 1$
Where $k_2(0)$ is the first bit of k_2

$$np = \sum_{i=0}^{2} k_2 (i + 1) \times 2^{i}$$

Step 9: Shuffle the elements $Elfv_{bi}$ of $[lfv_{bi}]$ to get $[lfv_{co}]$ using M_{S3} $(Elfv_{bi})$ where M_{S3} $(Elfv_{bi})$ is a mapping defined by S_3 generated from the sub-key k_3
Step 10: Select the blocks $[lfv_{co}]$ to be shuffled using S_{41} and Perform permutation using M_{S42} $([lfv_{co}])$ where M_{S42} (lfv_{co}) is a mapping defined by S_{42}
Step 11: Reconstruct the image using the basis function described in Section 3 to get the encrypted image.
Step 12: End.

13. KEY GENERATION PROCEDURE

Since the security of the proposed encryption Algorithm lies in the secret key, we propose a new key generation technique in which a 256 bit user pass phrase *k* is split into four sub-keys k_1, k_2, k_3 and k_4 of 32 bits each. The scaling factor *S* for the DC coefficients is derived from *k*. The value *n*, which is calculated from the block size and the sub-key k_1, are used to select the low frequency coefficients from the transformed block. A cryptographically secure pseudo-random number generator (PRNG) is used to generate the sequences S_1, S_2 and S_3 with k_1, k_2 and k_3 as seed values respectively. The sequence S_1 is used for sign-bit encryption while S_2 *is* used for pixel permutation and S_3 is used for coefficient permutation. The sequence S_4 generated using k_4 as the seed value is split into two subsequences S_{41} and S_{42} and are employed in block selection and block permutation.

14. IMPLEMENTATION DETAILS

This paper consists of implementing the Electronic Copyright Management System. In ECMS there are four modules.

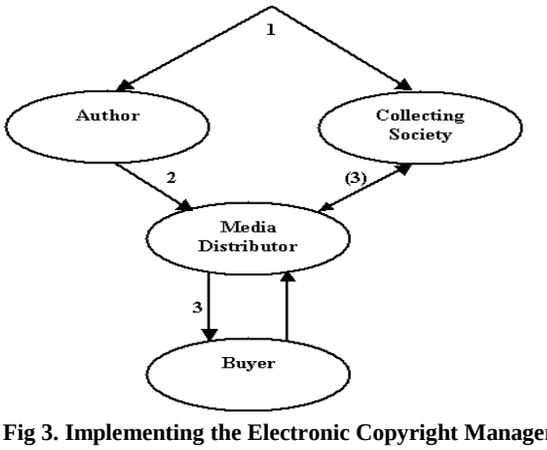

Fig 3. Implementing the Electronic Copyright Management System.

In Author Module Creation Unique Number is embedded into the Image using author private key. In the embedding of CUN it uses asymmetric watermarking algorithm. Distributor PIN is also embedded into the image using private key Asymmetric encryption algorithm.

Collection Society is the trusted third party that will ensure that the protected document traded correctly. It involves transaction between buyer & media distributor.

In collection Society module, Buyer PIN is embedded into the image using CS private key in Asymmetric encryption. It also computes Hash value of the image which should be sending to buyer. It is used as authentication purpose. This hash value is also appended into the image and the encrypted image is transferred to the buyer using LAN or Email networks.

In Buyer module, Buyer decrypts the encrypted digest using CS public key and the digest value is computed. Hash value is recomputed from the decrypted digest and the hash value is compared. If these values are same then it ensures no transmission loss. From third encrypted watermark buyer decrypt the Buyer PIN from it and ensures it legal ownership.

Control Authority is used for Illegal usage detection phase. It compares CUN with buyer watermark, distributor watermark and detect the legal or illegal ownership

15. CONCLUSION

Image and video encryption is neither in its infancy nor may it be considered a mature technique. It plays a more and more important role in today's multimedia world. Although many encryption schemes have been proposed to provide security for digital images and videos, some of them are too weak to resist various attacks designed by cryptanalysts. Basically, many efforts have been devoted to study the security issue, but for multimedia the security is still not strong from a serious cryptographic point of view. To design a truly secure image/video encryption scheme, the classical cryptology must be employed. The simplicity of many discrete chaotic maps and the well-established chaos theory make it possible to approach practically good solutions to image and video encryption. The success and failure of chaos-based encryption schemes have led to some valuable experiences and lessons, which can be used as the fundamentals of future research on the chaos-based multimedia encryption technology. At this point, chaos theory for image/video encryption appears to be promising but not yet mature. More efforts are needed for its further development.

16. REFERENCES

[1] H. Abut, editor. Vector Quantization. New York: IEEE Press, 1990.

[2] A. Alattar G. AI-Regib. Evaluation of selective encryption techniques for secure transmission of MPEG-compressed bit-streams. In proceedings of the IEEE international Symposium on Circuits and System.

[3] A. M. Alattar, G. I. AI-Regib, and S. A. AI-Semari. Improved selective encryption techniques for secure transmission of MPEG video bit-streams. In Proceedings of the IEEE International Conference on image Processing(ICIP'99) volume 4, pages 256-260, Kobe, Japan, October 1999. IEEE Signal Processing Society.

[4] M. Antonini, M. Goel, N.R. Shanbhag, D. L. Jones, and I. Daubechies. Image coding using wavelet transform. IEEE Transactions on image processing.

[5] H. Cheng and X. Li. Partial encryption of compressed image and videos. IEEE Transactions on signal processing.

[6] Ahmet M. Eskicioglu and Edward J. Delp. An overview of multimedia content protection in consumer electronics devices.

[7] Thomas Kunkelmann. Applying encryption to video communication. In Proceedings of the Multimedia and Security Workshop at ACM Multimedia.

[8] J. Meyer and F. Gadegast. Security mechanisms for multimedia-data. Unpublished, available at http://www.gadegast.de/frank/doc/secmeng.pdf.

[9] Proceeding of National Conference on Network Security, Nagercoil , September 2008.

[10] Alessandro Piva and Franco Bartolini *University of Florence* Mauro Barni *University of Siena* "Copyright protection in Open networks" IEEE Internet Computing June,2002.

[11] An Introduction to Wavelets, http://www.amara.com/IEEEwave/IEEEwavelet.html.

[12] WHITFIELD DIFFIE and MARTINE E.HELLMAN "New directions in Cryptography" submitted to IEEE Transactions on information theory, Vol IT-22, no 6, November 2010.