International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

Various Techniques for Multimedia content distribution: A Survey

Kanchan S. Tule, C. N. Deshmukh
PG Student, Associate Professor
Department of Electronics & Telecomm. Engineering
P.R.M.I.T. & R, Badnera
S.G.B.A.U. Amravati
Badnera-Amravati, India
kanchan.tule@gmail.com, cndeshmukh@mitra.ac.in

Abstract— Now a day due to vast usage of internet for exchanging data has frequently increased the availability of digital data such as audio, images and videos to the public. Techniques are being developed to ensure and facilitate data authentication, security and copyright protection of digital media. There are so many different methods like Cryptography, Steganography, Digital watermarking, Digital Fingerprinting that are available to protect confidential multimedia data from unauthorized access. In this paper, we introduce the survey of various techniques that are available for multimedia content distribution.

Keywords— Steganography, Stego Key, Cryptography, Digital watermarking, Digital Fingerprinting, LSB, DCT, DFT, DWT, SVD, PCA.

INTRODUCTION

The recent growth of networked multimedia systems has increased the need for the protection of digital media. This is particularly important for the protection and enforcement of intellectual property rights. Techniques are needed to prevent the copying, forgery and unauthorized distribution of multimedia content. Without such methods, placing data on a public network puts them at risk of theft and alteration. Thus, security is an important issue in communication. In order to achieve it, many image encryption methods have been proposed like Cryptography which scrambles messages so they cannot be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message in the first place. Watermarking ads information, embedded it within a multimedia content. Fingerprinting technology used for copyright protection of digital media. Fingerprinting has attracted the attention of Researchers during the early to mid. One of the primary motivations for applying Fingerprinting is to avoid video piracy by improving copy-right protection of multimedia data.

This Survey report has reviewed different method for Cryptography, Steganography, Watermarking, Fingerprinting..

I. REVIEW OF CRYPTOGRAPHY TECHNIQUES

Cryptography technique is used when secret message are transferred from one party to another over a communication line. There are two main types of cryptography

- Secret key cryptography
- Public key cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. Cryptography technique needs some algorithm for encryption of data. There are so many algorithms available to protect image from unauthorized access.

In Advanced Encryption Standard (AES) method, key stream generator is added in image as encryption technique to ensure improving the encryption performance. [1]

Block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. [2]

In image encryption technique using the Hill cipher, self-invertible key matrix is generated for Hill Cipher algorithm. Using this key

matrix they encrypted gray scale as well as color images. Their algorithm works well for all types of gray scale as well as color images except for the images with background of same gray level or same color. [3]

A new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved. [4]

An advanced Hill (AdvHill) cipher algorithm uses an involuntary key matrix for encryption. It is observed that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. Thus in that case advanced Hill (AdvHill) cipher algorithm is superior for any images with different gray scale as well as color images. [5]

In algorithm based on Chaotic encryption and DES encryption method, uses logistic chaos sequencer to make the pseudo-random sequence and after that they used DES method for further encryption. These method have high security and the encryption speed. [6]

A Novel Image Encryption Algorithm Based on SHA-512 hash function consists of two sections: The first does preprocessing operation shuffle one half of image. The second uses function to generate a random number mask. The mask is then XOR with the other part of the image which is going to be encrypted. [7]

A modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption.This algorithm is superior than original AES encryption algorithm. [8]

Algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provides confidentiality to color image with less computations Permutation process is much quick and effective. The key generation process is unique and is a different process. [9]

II.REVIEW OF STEGANOGRAPHY TECHNIQUES

Steganography is another technique for multimedia content distributions by hiding data in cover media so that others will not be able to notice it. In the current situation digital images are the most popular carrier/cover files that can be used to transmit secret information. There are many types of steganography methods. In this paper, we are going to take a short look at different steganography methods.

A) Substitution Methods (Spatial-Domain)

Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).3D geometric algorithm re-triangulates a part of a triangular mesh and embedded the secret information into newly added position of triangular meshes. This algorithm also resists against uniform affine transformations such as cropping, rotation and scaling. The stego key is generated from the message to be embedded. The vertices of the triangle are used for embedding. [10]

In this novel and secured algorithm , data is embedded into the red plane of the an image and the pixel is selected using a random number generator. It is almost impossible to notice the changes in the image. A stego key is used to seed the PRNG (Pseudo Random Number Generator) to select pixel locations. [11]

Algorithm which works on color images (JPEG). The edges are chosen for data hiding to improve robustness. The regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. It is also more difficult to observe changes at the sharper edges than in smooth regions. In the embedding procedure, the RGB components are separated, and based on a shared key, one/more components are selected. The cover image is divided into non-overlapping blocks. Each block is rotated by a random degree determined by a secret key. The resulting image is rearranged as a row vector V by raster scanning. The secret message is encrypted and by using LSBMR, 2 secret bits can be embedded into each embedding unit. The message is embedded after calculating the capacity estimation using a threshold. [12]

The Pixel Value Differencing (PVD) method segments the cover image into no overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. While embedding secret data, each pixel is split into two equal parts. The number of 1's in the most significant part is counted and the secret message is embedded in the least part according to the number of corresponding bits. [13]

In histogram-based reversible data hiding approach, two interleaving predictive stages are used. Most pixels are predicted by their two neighborhood pixels and four neighboring pixels in the column-based and chess-board based approach. The difference value of each

pixel between the original image and the stego-image remains within ± 1. In interleaving predictions, pixels in odd columns will be predicted by pixels in even columns or vice versa. In the embedding process predictive error values of odd columns are used to generate a histogram to embed secret data. The predictive error values are converted to get the stego-image. [14]

B) Transform Domain Methods

Transform domain techniques embed secret information in a transform space of the signal (frequency domain) .Integer Wavelet Transform (IWT) is used to hide secret images in the color cover image. The PSNR values and image quality are compared when embedding is done in the RGB and YC_bC_r domains. [15]

In Enhanced JPEG steganography and symmetric key cryptographic algorithm, The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking. [16]

C) Statistical Methods

Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.

Syndrome-Trellis Codes (STC) algorithm is used to improve the security of the system. STC divides the samples into different bins (binning) which is a common tool used for solving many information-theoretic and also data-hiding problems. [17]

A reversible embedding algorithm, based on Vector Quantization technique, is a compression technique which uses side matching and relocation method for encoding and decoding procedures .This method is used when a tiny distortion of the original content is not applicable in some sensitive applications such as military, medical / fine art data [18].

III. REVIEW OF DIGITAL WATERMARKING TECHNIQUES

Digital Watermarking is another technique for multimedia content distribution by embedding data called watermark or signature or label or tag into a multimedia file (image or audio or video) so that the watermark can be extracted for ownership verification or authentication. This technology is becoming important due to the popularity of usages of images on web. The digital watermarks can be divided into three different types as follows:

- Visible watermark.
- Invisible watermark.

In Visible watermarking watermark appears visible to a casual viewer on a careful inspection. The invisible watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. In this paper, we have survey different invisible watermarking algorithm. Those algorithms come into two domains, Spatial and Frequency domain.

A) Spatial Domain :

Spatial domain digital watermarking algorithms directly load the raw data into the original image. Techniques are based on direct manipulation of pixels in an image. Some of its main algorithms are as discussed below:

- **Additive Watermarking :**

The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low. [31]

- **Least Significant Bit :**

Old popular technique embeds the watermark in the LSB of pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. But these primitive techniques are vulnerable to attacks and the watermark can be easily destroyed. Such an approach is very sensitive to noise and common signal processing and cannot be used in practical applications.

- **SSM Modulation Based Technique :**

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

- **Texture Mapping Coding Technique :**

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [19], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

- **Patchwork Algorithm** :

Patchwork is a data hiding technique based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution.

- **Correlation-Based Technique :**

In this technique, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image I(x, y).

$Iw(x, y) = I(x, y) + k*W(x, y)$ ----------1)

Where K represent the gain factor, Iw represent watermarked image ant position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

B) Frequency Domain

Compared to spatial-domain methods, frequency domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [20]. Some of its main algorithms are discussed below:

- **Discrete Cosine Transforms (DCT) :**

DCT based watermarking algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking.

- **Discrete Fourier Transform :**

This is a multi-bit Fingerprinting technique. The DFT method select the good area where watermark information is embed and give more perceptibility and robustness.

- **Discrete Wavelet Transforms (DWT) :**

Wavelet Transform is a modern technique frequently used in digital image processing. The transforms are based on small waves called wavelet of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition than for other bands (HH, LH, and HL).The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [21]. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [22]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [23].

- **Singular Value Decomposition (SVD) :**

Singular Value Decomposition (SVD) is mathematical technique for diagonal matrices in that the transformed domain consists of basis states that are optimal. The singular value decomposition (SVD) is a method of representing a image in a matrix for with many application in image processing. The singular value decomposition of a *complex* matrix *X* is given by

$X=U\ S\ V^*$ ----------2)

Where *U* is an $m \times m$ real or complex unitary matrix, D is an $m \times n$ rectangular diagonal matrix with nonnegative real numbers on the diagonal, and V^* is an $n \times n$ real or complex unitary matrix. The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order the columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. Singular value of the matrix shows the luminance of an video frame layer while the corresponding pair of singular vectors specifies the geometry of the video frame layer. In the SVD-based Fingerprinting , an video frame is treated as a matrix, which further broke by SVD base method into the three matrices such as U, S and V. the small changes in the elements of matrix S does not affect visual perception of the quality of the cover video frame, SVD based Fingerprinting algorithms add the watermark information to the singular values of the diagonal matrix S in such a way to meet the imperceptibility and robustness requirements of effective digital image Fingerprinting algorithms.

In SVD based Fingerprinting proposed two effective, robust and imperceptible Fingerprinting algorithms. The two algorithms are based on the algebraic transform of Singular Value Decomposition (SVD). In the first algorithm, watermark bit information are embedded in the SVD-transformed in a diagonal-wise fashion and in the second algorithm bits are embedded in a blocks-wise fashion. The concert of the two proposed algorithms evaluated on the verge of imperceptibility, robustness and data payload. Both algorithms showed similar but high level of imperceptibility, however their performance varied with respect to robustness and payload. The diagonal-wise based algorithm achieved better robustness results, while the block-wise algorithm gave higher data payload rate. Each algorithm embeds the watermark in the transform-domain YCbCr space thus spreading the watermark in multimedia data. The first algorithm suggests hiding watermark information in a diagonal wise manner in one of three SVD matrices: U, S and V. On the other hand, the second algorithm hides the watermark information in a block-wise manner in either the U or V matrices [30].

IV. REVIEW OF DIGITAL FINGERPRINTING TECHNIQUES

Many digital Fingerprinting schemes have been survey in this paper. We propose new fingerprinting technique which is secure, robust and have negligible impact on quality of multimedia data. A classification of the existing video Fingerprinting techniques is divided in two main categories.

- Fingerprinting in Spatial Domain
- Fingerprinting in Frequency Domain

A) Fingerprinting in Spatial Domain

The following characteristics of spatial domain methods are as follows

- The watermark is applied to the pixel or coordinate domain.
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal

B) Fingerprinting in Frequency Domain

The Frequency domain base method are Discrete cosine Transform (DCT), Discrete Fourier Transform(DFT), Singular value decomposition (SVD), Principal Component Analysis(PCA) and Discrete wavelet transform(DWT) which used as the methods of data transformation. The frequency domain methods are comparatively more robust than the spatial domain fingerprinting schemes.

Spatial domain methods are based on direct modification of the values of the image pixels so the watermark has to be embedded in this way. Such methods are simple and computationally efficient [24].

Frequency domain methods are based on the using of some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) etc. to the host image [25] [26]. Embedding of a watermark is made by modifications of the transform coefficients accordingly to the watermark or its spectrum. Finally, the inverse transform is applied to obtain the marked image. This approach distributes the watermark irregularly over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult. The watermark signal is usually applied to the middle frequencies of the image [27], keeping visually the most important parts of the image (low frequencies) and avoiding the parts (presented by high frequencies), which are easily destructible by compression or scaling operations. The techniques which are used for digital fingerprinting are as follows.

- **Discrete Cosine Transform Features of DCT :**

DCT is highly used method in image Fingerprinting. Using The Discrete cosine transform image get decompose into different frequency bands. In this frequency band, watermark information is easily embedded into the middle frequency band. This is important method for video processing. DCT gives accurate result in video Fingerprinting it is not robust method. [28]

- **Discrete Fourier Transform :**

The frequency of the host signal is controlled by the discrete Fourier transformation. This is a multi-bit Fingerprinting technique for video sequences. An N-bit message is embedded in one unit of video fragment, in which a scene is employed as a Fingerprinting unit. In order to generate a watermark with optimum weighting factors, the perceptual properties for all the three-dimensional DFT coefficients should be computed, but this strategy seems to be undesirable due to the high computational complexity. [29]

- **Singular value decomposition (SVD) :**

In algorithm based on singular value decomposition (SVD), the host image is originally presented as USV^{-1} where the matrix S contains the singular values and U, V are the singular vectors. The algorithm adds the watermark to the singular values S thus, the modified singular value S is presented by USV^{-1}. Then the newly generated singular value S_w will replace the original S to generate the watermarked image. The singular vectors U_w and V_w are kept by the owner just for watermark detection. Since S_w is approximately equal to S, the visual quality of the image is preserved. To extract the watermark, the watermarked image will be decomposed again using SVD. The corrupted singular values S_w and the singular vectors U_w, V_w will recover the watermark. The main issue of this method is that the attacker can also claim his/her watermark easily by providing another set of singular vectors such as U_a, V_a. In other words, the recovered watermark depends more on the selected singular vectors. It proves that embedding a watermark (or fingerprint) only on singular values is unreliable.

- **Principal Component analysis :**

In PCA method watermark is embed into the Eigen vectors. First, the PCA process decomposes the image into eigenvectors and Eigen values. Then the image is projected onto each eigenvector and becomes a coefficient matrix. The watermark is embedded into the coefficient matrix based on the selected components. Finally, the watermarked image is obtained by applying the inverse PCA process. The robustness becomes the issue of this method. Because the eigenvectors are normalized and the numerical value of each component of the eigenvector is very small and can be easily corrupted by distortion methods.

- **Discrete Wavelet Transform :**

Discrete wavelet transform (DWT) is a tool for continuously decomposing an image. DWT is the multi-resolution description of an image. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. As the human eyes are less sensitive to the changes in the edges the high frequency components are used for Fingerprinting. There is various level of decomposition, after the first level of decomposition; there are 4 sub- bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands: LL3, LH3, HL3, HH3.if we increase the level of decomposition for embedding the watermark then proposed video Fingerprinting scheme made much robust.

CONCLUSION

In this paper, we take an introductory look at techniques available for multimedia content distribution. We have categorized different methodology implemented for multimedia content distribution like Steganography, Cryptography, Digital watermarking and Digital fingerprinting. While studying the various techniques for Steganography, Cryptography, Digital watermarking , One can observe that they have depicted shortcoming such as less encryption speed, decreased correlation between transmitted, reconstructed multimedia data and high computational complexity. If one tries to increase the robustness it has moderate impact on the quality of image in case of Digital watermarking. Techniques such as digital fingerprinting provide better security and have higher correlation between transmitted and reconstructed image. Also in order to achieve more robustness, scalability, we can combine two fingerprinting techniques Wavelet and PCA (Principal Component Analysis).

REFERENCES:

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, "A Modified AES Based Algorithm for Image Encryption" , World Academy of Science, Engineering and Technology,Vol.2, 2007.

[2] Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm", International Journal of Computer Science, Vol.5, 2008.

[3] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm",1st International Conference on Advances in Computing, Chikhli, India,21-22 February 2008.

[4] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption",IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[5] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,"Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[6] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan ,Dai Wei-di,"Digital image encryption algorithm based on chaos and improved DES" , IEEE International Conference on Systems, 2009.

[7] Seyed Mohammad Seyedzade, Reza Ebrahi mi Atani and Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[8] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, "A new modified version of Advance Encryption Standard based algorithm for image encryption" , International Conference Electronics and Information Engineering (ICEIE), 2010.

[9] Sesha Pallavi Indrakanti , P.S.Avadhani,"Permutation based Image Encryption Technique" , International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[10] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha,"Pattern Based 3D Image Steganography", 3D Research center, Kwangwoon University and Springer, 3DR Express., pp.1-8, 2013

[11] Shamim Ahmed Laskar and Kattamanchi "Steganography Based Data Hiding Random Pixel Selection For Efficient", International Journal of Computer Technology, Vol.4, Issue 2, pp.31, 2013.

[12] B.Sharmila and R.Shanthakumari,"Efficient Adaptive Steganography For Color Images Based on LSBMR Algorithm", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392, 2012.

[13] M.B.Ould MEDENI and El Mamoun SOUIDI,"A Generalization of the PVD Steganographic Method",International Journal of Computer Science and Information Security, Vol.8.No.8, pp156-159,2010.

[14] C.-H. Yang and M.-H. Tsai, "Improving Histogram-based Reversible Data Hiding by Interleaving Predictions", IET Image Processing, Vol.4. Iss. 4 pp.223-234,2010.

[15] Hemalatha.S, U.Dinesh Acharya and Renuka.A,"Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains",International Journal of Vol.4, No.1, pp.83-89,2013

[16] Prosanta Gope, Anil Kumar and Gaurav Luthra , "An Enhanced JPEG Steganography Scheme with Encryption Technique", International Journal of Computer and Electrical Engineering , Vol.2.No.5, pp924-930,2010.

[17] Tomas Filler, Student Member, IEEE, Jan Judas and Jessica Fridrich, Member, IEEE,"Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article, pp.1-17,2010.

[18] Jessica Fridrich, Miroslav Goljan, David Soukal,"Wet Paper Codes With Improved Embedding Efficiency ",IEEE Transactions on Information Forensics and Security,Vol 1. No.1, pp 102-110,2006.

[19] Jiang Xuehua, —"Digital Watermarking and Its Application in Image Copyright Protection",International Conference on Intelligent Computation Technology and Automation.,2010.

[20] Manpreet kaur, Sonia Jindal, Sunny behal, "A Study of Digital image watermarking", Volume2, Issue 2, Feb 2012.

[21] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University,"Watermarking with Wavelets: Simplicity Leads to Robustness", Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.

[22] G.Bouridane. A, M. K. Ibrahim,"Digital Image Watermarking Using Balanced Multi wavelets", IEEE Transaction on Signal Processing , pp. 1519-1536,2010.

[23] Cox, I.J.; Miller, M.L.; Bloom, J.A.,"Digital Watermarking",‖ Morgan Kaufmann,2001.

[24] Arularasi C. ,Meenakshi M. , Veena R.,Jayapriya J.,and Ramakrishnan,"Robust Digital Image Fingerprinting Using Middle Frequency Sub Bands of Discrete Wavelet Transformation", Proceedings of National Conference on Computing, Communication and Information Systems, pp.61-67, 11-12, Sri Krishna College of Engineering and Technology,Coimbatore,2011.

[25] Ramakrishnan S., Arularasi C. ,Meenakshi M. , Veena R. and Jayapriya J,"SVD Based Digital Image Fingerprinting Using DWT', Proceedings of the National Conference on Intelligent Computing and Control Engineering Applications", pp. 83-86, Anna University of Technology, Coimbatore,2001.

[26] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Q. Shi,and Z. Ni.' Lossless data hiding using histogram shifting method based on integer wavelets'. Proc. Int. Workshop on Digital Fingerprinting , Vol. 4283, pp.323–332,2006.

[27] Sadik Ali M. Al-Taweel, Putra Sumari, and Saleh Ali K.Alomar."Digital Video Fingerprinting in the Discrete Cosine Transform Domain" Journal of Computer Science 5 (8): 536-543, 2009.

[28] Lama Rajab Tahani Al-Khatib and Ali Al-Haj "Video Fingerprinting Algorithms Using the SVD Transform "European Journal of Scientific Research ISSN 1450- 216X Vol.30 No.3, pp.389-401,2009.

[29] D. Tsolis, S. Sioutas, and T. Papatheodorou, "Digital watermarking in Peer to Peer networks," in *16th Int. Conf.Digital Signal Processing*, Greece, pp. 1–5,2009 [30] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," in *Proc. Int. Conf. Image Processing, 1998 (ICIP 98)*, vol. 2, pp. 419–423,1998.

[31] A. Kaarna and P. Toivanen, "Digital watermarking of spectral images in PCA/wavelet-transform domain," in Proc. IEEE Int. Geoscience and Remote Sensing Symp.,2003 (IGARSS '03), vol. 6, pp. 3564–3567,2003.

[32] CHAPTER 2: LITERATURE REVIEW, Source: Internet

[33] http://ippr-practical.blogspot.in