ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

LITERATURE REVIEW on TRANSFERRING VIDEO using WATERMARK

Tejaswy Rao[1], Payal Talreja[2], Udhar Suraj[3],Gandhali Gurjar[4]

BE Student, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India[1,2,3]

Professor, Department of Computer Engineering, Singhad Academy of Engineering, Pune, India[4]

Abstract: The rapid growth of network distributions of images and video, there is a need for copyright protection against piracy. For this purpose we are using video watermarking. Different digital watermarking schemes have been proposed to address this issue of ownership identification. Digital watermarking is a process by which user specified signal (Watermark) is hidden or embedded into another signal (Video Signal) by the watermark embedding process. Afterwards the recovery of the watermark is achieved with the help of the watermark extraction process. The video watermark is robust against the attack of frame dropping, averaging and statistical analysis. It leads to broad curiosity in multimedia security and multimedia copyright protection. The most important issue in video watermarking is the invisibility of the watermark and the resilience of watermarking to attacks. Watermarking techniques are classified into three categories. They are Spatial Domain Method (SDM), Transform Domain Method (TDM) and Compressed Domain Method (CDM). Here explained about to transform domain method. This method used the discrete cosine transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) for watermark embedding.DWT are more popularity due to their spatial localization, frequency spread etc.. But DCT watermarking was to human perception model to modify low coefficients of DCT blocks. It has a larger embedding capacity and robustness. This technique provides better results with high accuracy.

Keywords: Watermarking, Discrete Cosine Transform, Watermark Extraction Process, Copyright

I. INTRODUCTION

Information hiding can be mainly divided into three processes - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user.

Thus even the existence of secret information is not known to the attacker Water-marking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Every day tons of data are embedded in digital media or distributed over the internet. The data so distributed can easily be replicated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, in potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity.

Digital watermarking is an extension of the same concept. There are two types of watermarks: visible watermark and invisible watermark. In this we have concentrated on implementing watermark on image. The main consideration for any watermarking scheme is its robustness to various attacks. Watermarking dependency on the original image increases its robustness but at the same time we need to make sure that the watermark is imperceptible. In this project an invisible watermarking technique (least significant bit) is implemented. An attack is also implemented in the visible watermarked image by adding a random noise to the watermarked image. The watermarked image is then compressed and decompressed using JPEG compression. Finally noise is removed and the images are separated from the recovered watermarked image.

The purpose of this application is to design and implement Watermarking system which provides Security for video transaction. We will develop an application which will allow user to send Video without error putting the right of their owner at risk and provides copyright protection and Owner authentication that assures secure video transfer. This paper discuss about the literature review on various algorithms which will be used this application.

II. LITERATURE REVIEW

A. TECHNIQUES AND ATTACKS OF WATER MARKING HEADING [1]

The Watermarking techniques are divided into two broad categories-:

1. Spatial Domain Techniques Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression.

2. Frequency Domain techniques

A) Discrete cosine transform (DCT) based technique:

Discrete cosine transform is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps a n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforming from this class are "sinusoidal", which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum. Therefore one speaks about the transformation to the frequency domain. The most popular member of this class is the Discrete Fourier Transform (DFT). The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry DCT and DFT are equivalent. There are eight different variants of DCT. There is a very slight modification between these eight variants. In JPEG compression the input data are two-dimensional, presented in 8x8 blocks. There's a need of using two-dimensional DCT. Since each dimension can be handled separately, the two-dimensional DCT follows straightforward form the one-dimensional DCT. A one-dimensional DCT is performed along the rows and then along the columns, or vice versa. The formula used for one-dimensional DCT:

$$F(u) = C(u)\sum_{x=0}^{N-1} f(x)\cos|\pi(2x+1)u/2N|$$

Where u = 0,1,….N-1

C(u)=$\sqrt{1}/\mathrm{N}$ When u=0 C(u)=$\sqrt{2}/\mathrm{N}$ When u≠0

DCT–II The formula used for two-dimensional DCT:

f(u,v)=c(u)c(v)

$$\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\ \cos\left|\frac{\pi(2x+1)u}{2N}\right|\cos\left|\frac{\pi(2y+1)v}{2M}\right|$$

Where u = 0,1,2…N-1 ,

v = 0,1,2…M-1

C(u),C(v)=$\sqrt{1}/\mathrm{N}$ when u,v =0,

C(u),C(v)=$\sqrt{1}/\mathrm{N}$ when u,v ≠0,

Applying the formulas directly requires much computational resources the therefore an implementation in hardware can be very efficient.

B) Wavelet Transform based Watermarking:

The Fourier transform is ananalys is of global frequency content in the signal. There are applications in digital image processing wherein we need the localized frequency components. This can be done by using the Short Time Fourier Transform. This is similar to the concept of using windowing functions. The windowed transform is given as where denotes the frequency and denotes the position of the window. This equation transforms the signal f(x) in a small window around. The STFT is then performed on the signal and local information is extracted. The wavelet transform based watermarking technique divides the image into four sidebands with a low resolution approximation of the tile component and the component's 'horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform. One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the human visual system (HVS) as compared to the DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as higher resolution detail bands {LH,HL,HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. One of the most straightforward techniques is to use an embedding technique similar to that used in the DCT. In the Wavelet Domain, where *Wi* watermark to be embedded, and α scaling factor. To detect the watermark the same process as that used in DCT is implemented. Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process would be rather adaptive; storing the majority of the watermark in the larger coefficients.

C) Simple Watermarking:

A very simple yet widely used technique for watermarking images is to add a pattern on top of an existing image. Usually this pattern is an image it self-logo or something similar, which distorts the underlying image. The fig 1 below shows a simple watermark applied to an image, Lena, using Bytes count software.

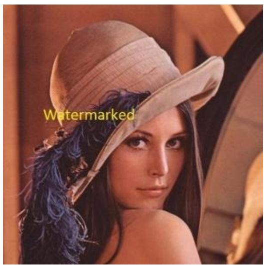

Fig 1: Simple watermarked image of Lena

D) Attacks:

Digital watermarking is not as secure as date encryption. Therefore, digital watermarking is not immune to hacker attacks. Different types of attacks are given below. *Geometrical* Instead of removing the watermark, the watermark has distorted reducing spatial or temporal alteration of stereo data. *Cryptographic* Brute-force attacks are used for exhaustive search to find the key to decipher. These are called cryptographic attacks. *Active & Passive* The attacker removes or spoils the watermark. The attacker just identifies the watermark and does not damage it. *Forgery* Attacker forges new watermark and replaces the old one with the new one. Figures.9 shows the original watermarked image, which is replaced by the attacker with Figures.10 which may look like the original image but is not the original data. There by misleading the end receiver.

B. PROPOSED WATERMARKING SCHEME [2]

This application presented an efficient video watermarking technique using discrete cosine transform (DCT) to protect the copyright protection of digital images. The efficiency of the video watermarking technique is achieved with the aid of the following two major steps. Watermark Embedding process and Watermark Extraction process.

A) WATERMARK EMBEDDING PROCESS:

Before embedding watermark pixels into the input video sequences, the following process should carry out to enhance the security of the hiding information as well as to improve the efficiency of our proposed approach. The process includes Shot segmentation of video sequences ,Bit plane slicing of a grayscale image , Pixel permutation and Decomposition of an image using DCT .

1) *Shot segmentation of video sequence :*

The fundamental task of performing the video processing application like video indexing, video summarization, video watermarking and video retrieval is video shot segmentation. The original input video sequence is first segmented into non-overlapping units, called shots that depict different actions. Each shot is characterized by no significant changes in its content which is determined by the background and the objects present in the scene. Numerous researches are available in the literature for video shot segmentation using several techniques. Here, we have used Discrete Cosine Transform and correlation measure to identify the number of frames involved in each shot. At first, the first and second frame is divided into a set of blocks of sizes and DCT is applied to every block of the frame. The two-dimensional DCT for an input image X and output image you can be defined as:

$$Y_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} X_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, 0 \le p \le M-1$$

$$0 \le q \le N-1$$

Where

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases};$$

$$\alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

$$r = \frac{\sum_{m}\sum_{n}\left(X_{mn} - \bar{X}\right)\left(Y_{mn} - \bar{Y}\right)}{\sqrt{\left(\sum_{m}\sum_{n}\left(X_{mn} - \bar{X}\right)^2\right)\left(\sum_{m}\sum_{n}\left(Y_{mn} - \bar{Y}\right)^2\right)}}$$

$$where\ \bar{X} = mean(X), \text{ and } \bar{Y} = mean(Y)$$

After finding the correlation for the first and second frame, the same procedure is repeated for the consecutive frames presented in the video. Then, the frames within a shot can be identified by maximizing the cross correlation term which gives a measure of the degree of similarity between two frames of video.

2) *Bit plane slicing of a grayscale image:*

Bit-Plane Slicing is a technique in which the image is sliced at different planes. Instead of highlighting gray level images, highlighting the contribution made to the total image appearance by specific bits might be desired. Imagine the image is composed of 8 bits, 1-bit planes ranging from bit plane1-0 (LSB) to bit plane 7 (MSB). In terms of 8-bits bytes, plane 0 contains all lowest order bits in the bytes comprising the pixels in the image and plane 7 contains all high order bits. Often by isolating particular bits of the pixel values in an image we can highlight interesting aspects of that image. The high-order bits usually contain most of the significant visual information and the lower-order bits contain subtle details. The advantage of doing this method is to get the relative importance played by each bit of the image. Figure 1 shows the Bit plane slicing concept. Significant visual information and the lower-order bits contain subtle details. The advantage of doing this method is to get the relative importance played by each bit of the image. Figure 2 shows the Bit plane slicing concept.

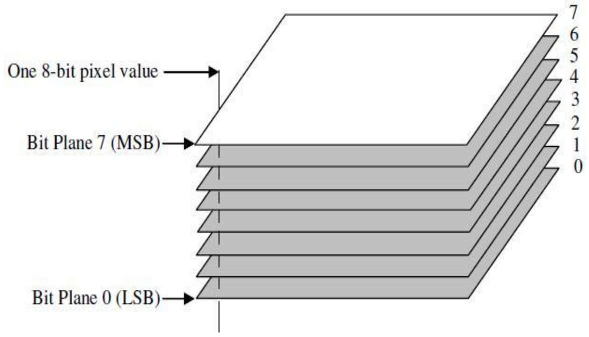

Fig 2: Bit Plane Slicing

3) Pixel permutation:

After the bit plane slicing process, the sliced images are allowed to permute each pixel value to enhance the security of the hiding information. In this scheme, each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys. The size of the pixel group is same as the length of the keys, and all the keys are of the same length. If the length of the keys is more than the size of pixel group, the perceptual information reduces. In this, the group of pixels is taken along the row without the loss of generality, i.e., the column wise procedure would yield the same kind of results .

4) Decomposition of an image using DCT:

Like other transforms, the Discrete Cosine Transform (DCT) attempts to de-correlate the image data. After de-correlation each transform coefficient can be encoded independently without losing compression efficiency.

Watermark Embedding steps:
Input: Original video sequence

$^{O}v^{[i,\ j]}$, Grayscale watermark image $^{W}I^{[i,\ j]}$
Output: watermarked video sequence $^{Wv\ [i,\ j]}$

1. Segment the original input video sequence $^{O}v^{[i,\ j]}$ into number of non-overlapping shots $S_s\ [i, j]$ using shot segmentation technique. Then, identify the number of frames $F_p\ [i, j]$ involved in each segmented shots $S_s[i,j]$ for embedding purpose.
2. Slice the grayscale watermark image
3. Permute the sliced images $^{SI\ [i,\ j]}$ using a pixel permutation technique to obtain the permuted grayscale image $^{P}I^{[i,\ j]}$.
4. Extract the blue components $B_F\ [i, j]$of all the partitioned frames for embedding the each sliced image $^{SI\ [i,\ j]}$ into the blue components of each frame.
5. Split the image into small blocks (8 x 8) and decompose the blue components $B\ [i, j]Fp$ of each partitioned frame $Fp[i, j]$ into AC and DC coefficients by DCT.
6. Choose the low frequency sub-bands from the transformed frames to embed the permuted grayscale image $^{P}I^{[i,\ j]}$.
7. Find the similarity matrix of the permuted image $^{P}I^{[i,\ j]}$ to embed into the chosen coefficient. The embedding process should repeat for all blocks of DCT. $^{W}I^{[i,\ j]}$ into 8 bit planes $^{S}I^{[i,\ j]}$ using bit plane slicing.

Case 1: for embedding the watermark pixel '1'.
The values in the embedding part $^{Ep[x,\ y]}$are compared against the maximum value $^{\max(E\ p\ )}$ and modified as follows: If the value in the chosen embedding part is greater than 1, take the absolute value and embed the same. Otherwise, if the value in the embedding part is lesser than the 1, add the corresponding pixel with the maximum value and embed the modified value.

```
if Ep(i) >1 then
Ep[x, y] <<Abs [Ep(i) ]
else
Ep[x, y] <<Ep(i) +max(Ep)
end if
```

Case 2: for embedding the watermark pixel '0'.
If the value in the embedding part $^{Ep[x,\ y]}$is lesser than the 0, take the absolute value and embed the same. Otherwise, if the value in the embedding part is greater than the 1, subtract the corresponding pixel with the maximum value $^{\max(E\ p\ )}$ and embed the modified value.

```
if Ep(i) < 0 then
Ep[x, y] <<Abs [Ep(i) ]
else
Ep[x, y] <<Ep(i) - max(Ep)
end if
```

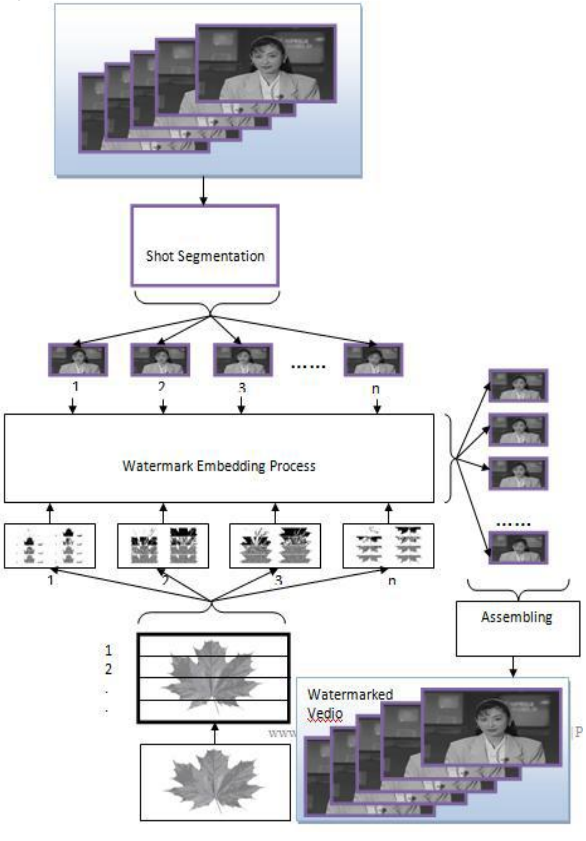

Fig 3: Watermark Embedding Process

2) WATERMARK EXTRACTION PROCESS:

After embedding the grayscale watermark image pixels into the original video sequence, we have extracted the embedded watermark image without affecting the original video.

Input: watermarked video sequence
W_v [i, j], size of the watermark image.
Output: recovered watermark image ^{W}I [i', j']

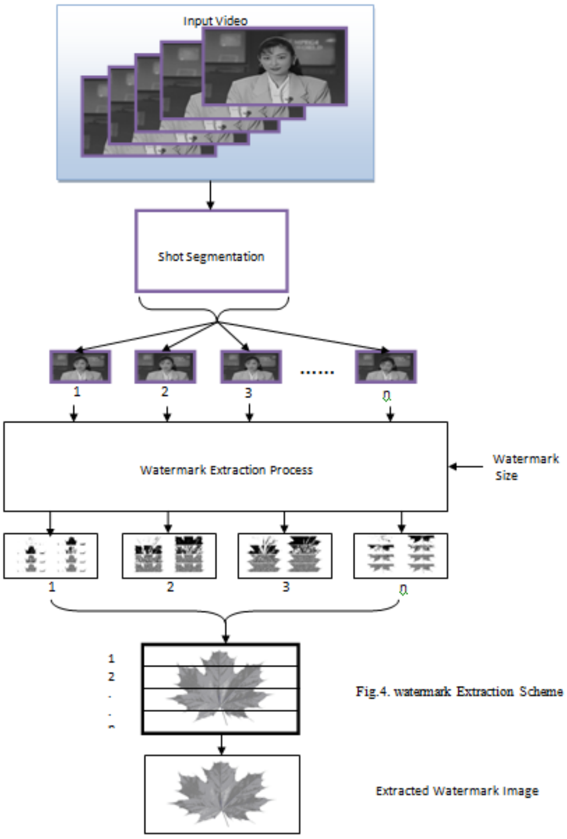
Input Video
Shot Segmentation
1
2
3
......
n
Watermark Extraction Process
Watermark Size
1
2
3
n
1
2
.
.
n
Fig.4. watermark Extraction Scheme
Extracted Watermark Image

Fig 4: Watermark Extraction Process

1) Segment the watermarked video sequence
W_v [i, j], into a number of non-overlapping shot *Ss*[*i*', *j*'] using the shot segmentation technique. Then, identify the number of frames *Fp*[*i*', *j*'] involved in each segmented shots *Ss*[*i*', *j*'] for the extraction process.

2) Extract the blue components of all the partitioned frames for extracting the embedded watermark pixels.

3) Decompose the blue components of the frames with the aid of the DCT into AC and DC coefficients.

4) Select the low frequency components from the transformed frames to extract the watermark gray scale image.

5) Extract the watermark pixels from the embedding part in a zig-zag manner from the each blocks with the aid of the following steps. If the embedded pixel

6) value is greater than the mean pixel value, then the extracted pixel value is one. If it is lesser, then the extracted pixel is zero.

7) Form the matrix with the size of the watermark image and the extracted pixels are placed in it to attain the watermark image.

8) Obtain the watermark image by applying the reverse process of permutation and bit plane slicing. The block diagram of the watermark extraction process is shown in figure 4 .

C. RSA: (Rivest, Shamir, Adleman) *[3]*

RSA is an encryption/decryption and authentication system, which is also known as public-key cryptosystems (Public Key Encryption). RSA is normally used for secure data transmission. A user of RSA creates product of two large prime numbers, along with an auxiliary value, as public key. The prime numbers given to algorithm kept as secret. The public key is used to encrypt a message, and private key is used to decrypt a message.

How RSA works?

1. Start
2. Choose two prime numbers p = 3 and q = 11
3. Compute the value for ‘n’
n = RSA.n_value (RSA_P, RSA_Q);
n = p * q = 3 * 11 = 33
4. Compute the value for? (n)? (n) = (p - 1) * (q -1) = 2 * 10 = 20
Int phi = RSA.cal_phi (RSA_P, RSA_Q);
5. Choose e such that 1 < e <? (n) and e and n are coprime. Let e = 7
6. Compute a value for d such that (d * e) % ? (n) = 1. d = 3
Public key is (e, n) => (7, 33)
Private Key is (d, n) => (3, 33)
7. Stop.

Let M, is plain text (message), M= 2.
Encryption of M is: C = Me % n.
c = "" + RSA.BigMod (ar[i], RSA_E, n);
Cipher text is, C = 27 % 33.
C = 29.
Decryption of C is: M = Cd % n.
dc = dc + (char) RSA.BigMod(Integer.parseInt(c) , d, n);
Plain text (message), M= 293 % 33.
M= 2

D. EXPERIMENTAL ANALYSIS [4]

Fig.5.Input Watermark Image

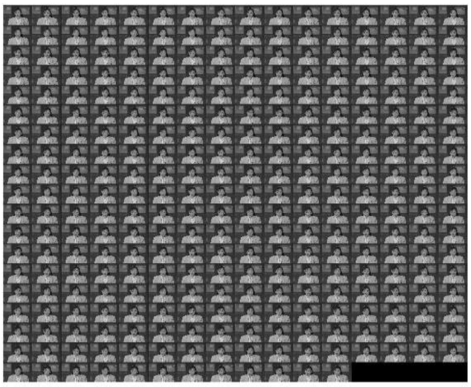

Fig 6: Input Video

Fig 7: Output of Video segmentation

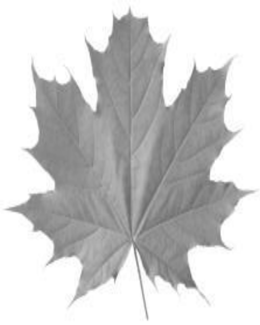

Fig 8: Extracted Watermark Image

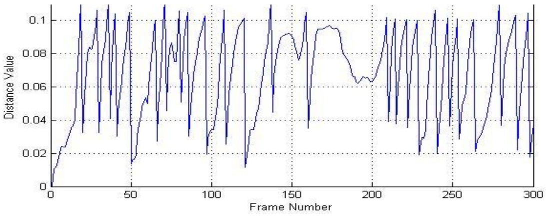

Fig 9: Distance between frames

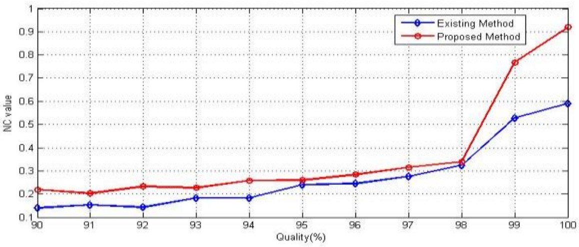

Fig 10: Performance graph(Compression Quality vs NC Values)

III. CONCLUSIONS

Watermarking can be used in following Areas: Defense Services, Corporate/commercial world, Secret Information Sharing, Education Sector Using watermarking scheme even the existence of secret information to attacker. In watermarking the hidden information usually related to cover the object hence it used for copyright protection and owner authentication. One way to discourage illegal duplication is to insert information known as watermark in potentially vulnerable data in such a way that it is impossible to separate from data.

ACKNOWLEGEMENT

We wish to thank Mrs. Gandhali Gurjar for her experienced and valuable guidance at every step of the completion of this paper of this paper and for her valuable input for the helping us in gathering the information.

REFERENCES

[1] A. Mitra, Y. V. SubbaRao and S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Electrical and Computer Engineering, Vol: 1, No: 2, pp: 127-131, 2006.18

[2] Aree A.Mohammed and Jamal A.Husssein, Efficent video watermarking using motion estimation approach,*2009,Eighth IEEE/ACIS Internation conference on Compter And Information Science*.4

[3] Chih-Chin Lai ,"A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", *Digital Signal Processing, in 2011, pp. 1128-1134.2*

[4] Gandhe S.T., Potdar U. and Talele K.T., "Dual Watermarking in Video Using Discrete Wavelet Transform", in Proceedings of Second International Conference on Machine Vision, pp. 216 - 219, 2009.7

[5] Gonzalez R.C., Woods R.E., "Digital Image Processing", Addison Wesley, 2002.16