Reversible Non-Blind Video Watermarking Based on Interlacing using 3-level DWT & Alpha Blending Technique

Mandeep Singh^{#1} Reecha Sharma^{*2}

[#] Department of Electronics and Communication Engineering Punjabi University, Patiala. ^{*}Assistant Professor in Department of Electronics and Communication Engineering Punjabi University, Patiala

Abstract: The growth of the Internet has frequently increased the availability of digital data such as text, audio, images and videos to the public. Digital watermarking is one of the important techniques to secure digital data in the field of authentication, copyright protection and security. The non-blind watermarking systems have a main problem that for extracting the watermark image from the watermarked image, the original image is required. Due to this it required more memory in both sender and receiver and double bandwidth in communications channel. In this paper a solution and more effective non-blind video watermarking depends on using image interlacing as a new way in the watermarking systems. In this paper DWT based watermarking technique, the frames selected from a video is get decomposed through the DWT in 3-levels and watermark is embedded into the low frequency sub-band of a original frame by using alpha blending technique and the Arnold transform is one of the popular symmetric key as an encryption and decryption method. The results obtained by these techniques are further compared and analyzed.

Keyword: Reversible watermarking, interlacing and de-interlacing, non-blind, Arnold transform 3-level DWT and alpha blending.

I. Introduction

The rapid growth of computer technology and internet network technologies, digital multimedia are become more popular and it is very easy to transmit from one place to other and distribute across the world. So, there is a demand for techniques to protect the data and to stop unauthorized duplication. Digital watermarking protects the illegal steeling or copying of multimedia. A watermark is secret information about origin, proof of ownership, copy control, and so many. This information is embedded in multimedia content such as audio, image or video, taking care of robustness, imperceptibly and security. The watermark is embedded and decomposes as per requirement to represent the proof of ownership and identity of multimedia [1]. Digital watermarking is categorizes such as; text watermarking, image watermarking, audio watermarking, video watermarking.

Video watermarking is different from image watermarking, because additional data are available here that allows information to be more secure, imperceptible and reliably embedded. Digital video watermarking is a combination of consecutive still images. So video watermarking can be growth of collection of image watermarking. The amount of information that can be embedded in the video watermarking is called payload. Video watermarking has more capacity as compare to image watermarking. In video watermarking techniques need to face other challenges than that in image watermarking technique such as large volume of the existing repeated sequence of data between frames.

Digital watermarking process is also classified in the watermark decomposing process into two types: blind and non-blind watermarking techniques [2]. In the non blind watermarking technique, in watermark recovery process the original data is required in addition to the watermarked data and in blind watermarking technique the original data is not required [3] as shown in Figure 1. The two advantages in non blind watermarking techniques over the blind watermarking technique are, as first is less complex and second more robustness and secure against attacks or distortions because the recovery watermark is very similar to the original one. But also the main disadvantage of the non blind watermarking systems is double overhead over system resources like memory/ storage in both sender and receiver and bandwidth on the communications channel between them.

This paper shows the key technologies of digital watermarking and explores the application in the digital image copyright protection and a brief review of video watermarked techniques is introduced.

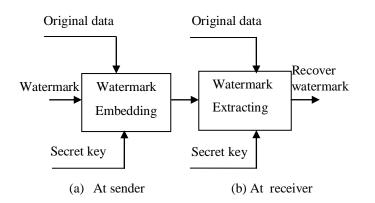


FIGURE 1: Non-blind watermark system

II. Aspects Of Video Watermarking

Video watermarking is a combination of sequential and equally spaced images. Evidently any image watermarking technique can be extend to make watermark videos, but in video watermarking techniques needs to face other challenges. Video watermarked sequences are very much susceptible to pirate attacks such noise addition, pixel removal, rotation, rescaling, shearing and more compression standard [4].

Digital watermarking systems can be classified by a number of defining properties including embedding quality, faithfulness, data payload, blind or non-blind detection, copy right protection, capacity, robustness, perceptual transparency, security, and watermark keys, modification and multiple watermark, tamper resistance, sensitivity, and scalability. Some of them are more practical and common application. In this section, some general properties will be listed and briefly discussed and focus will make a video watermarking. These properties are playing important role in watermarking application.

A. Perceptual Transparency

Invisibility is the extent at which an embedded watermark remains unperceived when the user views the watermarked data. However this need effort with other needs such as tamper resistance and robustness, specific against lossy compression techniques. To outlive the next generation of compression techniques, it will likely be compulsory for a watermark to be observed to a trained observer which is enquired to compare the original and the watermarked data of the video

B. Robustness

Robustness is the quickly power of recovery of an composed watermark against removal by signal processing. The use of audio, images and video signals in digital form, commonly occur many types of distortions, such as lossy compression. For watermarking to be utility, the watermark should be recoverable even after such distortions involved. Robustness against signal distortion is better executed if the watermark is placed in very important parts of the data.

Due to existing redundancy between frames and large amount of data, video data are highly vulnerable to attacks, such as frame averaging, frame dropping, rotation, sharpening [4].

C. Capacity

Capacity is the amount of information that can be expressed by an embedded watermark. Depending on the watermark application, the watermarking algorithm should approve a predefined number of bits to be embedded.

III. Video Watermarking Technique

Digital video is a combination of still and equally space images called frames and these frames are loaded by a constant rate called frame rate. So, by viewing the each frame from the video data step-by-step and dealing with each frame as a color image. Video watermarking technique can be extended version of image watermarking techniques [5].

As in image watermarking, the watermark embedding and decomposing process can be in form of spatial domain or frequency domain. In the spatial domain, the watermark is embedded by modifying the pixel values of the original image or video directly. In the frequency or transform domain, the watermark is composed by modifying the frequency components of the original image and video directly. This is done by transforming the original signal to the frequency domain before composing the watermark and after that retransforming to spatial domain. As a result, spatial domain watermarking techniques are less complex than frequency domain

techniques. The characteristics of the human visual system (HVS) are better captured by the frequency components than spatial components [1]; thus, frequency domain watermarking techniques has better imperceptibility, more robustness against attacks such as noise addition, pixel removal, rescaling, rotation, and shearing, and more compatibility with compression standards.

Unlike image watermarking, there is a third type of watermarking techniques called compresseddomain video watermarking techniques [3]. There are no. of digital videos are typically stored and distributed in compressed form (e.g., MPEG). Due to the real-time needs of video broadcasting, there is no time for decompression and recompression, so watermark is directly embed in these compressed video techniques. The watermarked video is highly susceptible to be recompressed with different parameters or converted to formats other than MPEG. This is main disadvantage of these techniques.

C. Spatial Domain Watermarking

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the original image or video directly. This technique has the main strength of pixel domain method due to low complexities and simplicities than other in real time these techniques are more useful.

Least Significant Bit Modification

In this technique, the each pixel of the original image has Least Significant Bit is used to embed the watermark or the other information. In this watermark is stored in the cover image, in which we can embed a smaller object multiple times. The image pixels are identified and embedding will be done using a pseudo-random number generator based on a given key.

Least Significant Bit modification is powerful tool for stenography as it is a simple and useful for it. But it cannot better robustness which is required in video watermarking applications.

Correlation-Based Techniques

This is also simple technique. In this the watermark is directly add in the image or video in spatial domain by pseudo random noise pattern to the important values of its pixels. A Pseudo-random Noise (PN) pattern P (x, y) is added to the cover image I (x, y), according to the given equation:

$$I w (x, y) = I (x, y) + z^* P (x, y)$$
(1)

Where z denotes a gain factor and Iw the watermarked image. By increasing the value of z the robustness is also increases at the spending of the quality of the watermarked image. The same key is used as an input to embed the data and to extract the data as well, to the same pseudo-random noise generator technique, and the correlation between the noise pattern and possibly watermarked data is computed. If the correlation exceeds a certain threshold value, the watermark is recovered, and a single bit is set [6]. This method can easily be extended to a multiple-bit watermark by dividing the image into blocks and applying the same procedure independently on each block.

B. Frequency Domain Watermarking

This watermarking techniques is mostly used in digital watermarking [7-8], in this the watermark is embedded into the frequency domain as compare to the spatial domain for the robustness of the watermarking technique. The frequency domain watermarking mainly of three types: Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) is used for data transformation in this domain. The main power proposed by transforming domain techniques is that they can take advantage of special properties of different domains to guide the disadvantage of pixel-based methods or to support additional features. Generally, in this transform domain method, higher computational time is required.

Discrete Fourier Transform

Discrete Fourier Transform is the technique which firstly extracts the brightness of the watermarked frame, computing its full-frame DFT and then taking the magnitude of the components. The watermark is embedded of two alphanumerical slender ropes. The DFT coefficient is different, then IDFT. Only the first frame of each GOP is watermarked, which was embedded of twelve frames, leaving the other ones undestroyed. It is better robustness to the usual image processing as linear and non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping.

Discrete Cosine Transform

DCT like a Discrete Fourier Transform, it denotes data in form of frequency space rather than an amplitude space. This is useful because it is more similar to the way humans understood light, so that the part

that are not understood can be identified and thrown away. DCT based watermarking techniques are more robust as compared to spatial domain techniques. Such techniques are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. but is more complex than other frequency domain and they are difficult to implement and more expensive. DCT are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be divided into Global and Block based DCT watermarking. Embedding in the most significant portion of the image has its own advantages because most compression schemes remove the most insignificant portion of the image.

IV. 3-Level Dwt Based Watermarking

When spreading this technique to the video watermarking system, three-level discrete wavelet transform (DWT) is used which example of the frequency domain watermarking. For more security, a symmetric key is used i.e. Arnold Transform which is more popular image frame encryption methods for encrypt the data before embedding them in the original data. This technique will discuss following.

Three-Level DWT- DWT as compare to the other frequency domain transform i.e. discrete Fourier transform (DFT), discrete cosine transform (DCT), are the most popular reversible transforms used in frequency domain watermarking. DWT as a multiresolution multilevel transform is much better in watermarking than DCT and DFT, because it better understands the human visual system (HVS) closer than them [7].

At the first level of DWT extracting process, the image is pass through low (L) and high (H) pass filters in horizontal and vertical manner to produce four frequency sub bands [5].i.e. LL1 is the low frequency sub band and HL1, LH1, and HH1 are the high frequency sub bands. In low frequency components contain the most important portions of the image in which any modifications like watermarking can damage it [8], as shown in Figure 2(a). The high frequency components contain the least important portions of the image/video frame which can be eliminated by compression. So, the mid frequency components are the best part for watermarking. These mid frequency components appeared strongly at the next levels of DWT decomposition in which the LL (m) sub band is decomposed into LL (m+1), LH (m+1), HL (m+1), and HH (m+1), where "m" is the level number, LL (m + 1) is the lower frequency sub band, and LH (m + 1), HL (m + 1), and HH (m + 1) are the mid frequency sub bands [10]. 3-level DWT technique shown in figure 2(b). This number of extracting levels is enough to present the mid frequency components strongly such as the HL3 sub band which is considered as the best part for watermarking operations according to the HVS properties [9]. So, in our case, more than three levels of extracting are unnecessary, as well as it will be more computational complexity.

LL1	HL1	LL3	HL3	HL2	
		LH3 HH1	HH3	HH2	HL1
LH1	HH1	LH1			HH1

(a) Single-level decomposition (b) Three-level decomposition FIGURE 2: One and three level DWT decomposition of image.

According to use of keys: There are two type of keys are used

- Asymmetric watermarking: This is technique where different keys are used for embedding and extracting the watermark.
- Symmetric watermarking: Here same keys are used for embedding and extracting the watermark.

Arnold Transform

The Arnold Transform is one of the popular symmetric key [13] as an encryption method for any image of size N x N is the changing of the location of each pixel according to the following equation:

$$\binom{x}{y}' = \binom{1}{1} \binom{1}{2} \binom{x}{y} \pmod{N}$$

Where (x, y) is the current location and (x', y') is the new location, after a certain number of iterations called Arnold Period the image is returned to its original state, this period is changing according to the image size, bigger image size bigger Arnold Period (for image of size 64 x 64 the Arnold Period = 96, for image of

(2)

size 128 x 128 the Arnold Period = 192 and so on). To use Arnold Transform as an encryption method, a number of iterations less than the Arnold period is required, this number of iterations is used as a key of type symmetric which means that the same number of iterations is used in decryption operation but using the inverse of the encryption formula.

·b

Watermark image of size 64*64Watermark image after scrambling by arnold transforr

FIGURE 3: Watermark and after Scrambling

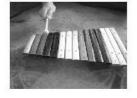
• Image Interlacing

Image interlacing (also known as interleaving) is an operation in which the original image is divided into sub images. Each sub-image has the same number of unrepeated pixels. The interlacing algorithm indicates the contents of each sub-image. The reverse operation called de-interlacing, in which these sub-images are combined together to generate back the original image [10-11]. The first use of the image interlacing is how to solve the problem of communicating the internet over a slow communications link. Before image interlacing, the image pixels are loaded in order left-to-right and top-to-bottom which means that the complete loading of the image will take a long time. By image interlacing, the original image is divided into a number of sub-images and these sub-images are loaded in sequence. As a result, the viewer can partially see a degraded copy of the image until it will be a perfectly clear copy. This operation helps the viewer to decide more quickly whether to abort or continue the transmission.

Another way to use the image interlacing is present, where the original image is interlaced by rows (One level interlacing) into two sub-images (even rows and odd rows), and two different watermark images are embedded, one in each sub-image (Multiple Watermarking System). It is noticed that the two sub-images are very similar.

Even rows even columns (EE) interlaced inplateframoe/s odd columns (EO) interlaced input frame





Odd rows Even columns (OE) (EE) interlaced ம்ddtrb்வனலிdd columns (EE) interlaced input frame





Figure 4: Two Level Interlacing

V. Video Watermarking In Wavelet Domain

The video watermarking process in wavelet domain includes embedding of watermark by modifying wavelet coefficients of sub-video's image, extraction and detection of watermark from watermarked video [6].

A. Embedding Watermark

In the non-blind watermarking the original video is divided into four sub-videos by using interlacing technique. Out of four, two sub-videos can play the same role of the two identical copies of the original video and two are rest in place. There are two identical copies, in which one for embedding purpose and other for

recovery operation. In the end, there is no need to another copy of original video in the watermark image recovery operation.

In this process firstly the host video is taken and interlace into four sub video. The one of the sub-video divided into no. of frames and 3-level DWT (Discrete Wavelet Transform) is applied to the no. of frames of video which decomposes images into four components: low frequency approximation, high frequency diagonal, and low frequency horizontal, low frequency vertical components. In the same manner 3-level DWT is also applied to the watermark image which is to be embedded in the one sub-video and Arnold transform key is also applied to the each of the watermarked images. The technique used here for inserting the watermark is alpha blending [9]. In this technique the decomposed components of the host images and the watermark image which are obtained by applying 3-level DWT to host images and the watermark image are multiplied by a scaling factor and are added. During the embedding process the size of the watermark should be smaller than the host images. After embedding, the all four sub-video combine by de-interlacing technique and make a watermarked video.

• Alpha blending

According to the formula of the alpha blending the watermarked image is given by

 $WI=q^{*}(LL1)+k^{*}(WM)$

WI=Watermarked image

LL1=low frequency approximation of the original image

WM=Watermark.

q, k-Scaling factors for the original image and watermark respectively.

Figure: 5 shows embedding watermark in wavelet domain.

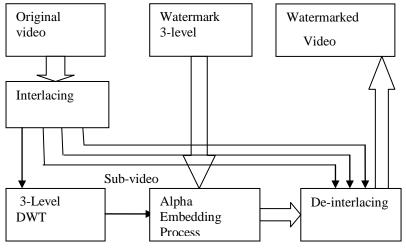


Figure 5: Embedding of Watermark at sender

B. Extraction and Detection of Watermark

In this process the watermarked video again divided into four sub-videos by interlacing technique and selects one watermarked video. The Inverse discrete wavelet transform and inverse Arnold transform is also applied is to the watermarked sub-video's frames or images. Now the result obtained is subtracted from the watermarked image and in this way the host video also recovered. The watermark is recovered from the watermarked sub-video by using the formula of the alpha blending.

• Alpha blending

RW= (WI - k*LL1) RW=Recovered watermark, LL1=Low frequency approximation of the original image, WI=Watermarked image (3)

(2)

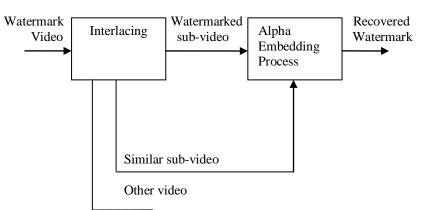


Figure 6: Extraction of Watermark at receiver

In involves comparison of both the images or comparison with the threshold. The correlation between the extracted watermark and the embedded watermark signal is then calculated. Detection process allows the owner to be identified and provides information to the intended recipient depending on threshold value. Watermark detection at lower resolutions is computationally effective because at each successive resolution level, smaller frequency bands are involved.

VI. Results And Discussion

To implement this technique we have used a video which is divided into sub-video by interlacing and divide144 frames or images from a sub-video as original images and the 'k.jpg' image as watermark. Fig. 7(a) & 7(b) shows the original video and the watermark video. For embedding of watermark in the original image the Value of scaling factor k is varied from 0.57 to 1.6 by keeping k constant and best result is obtained for k=0.99 & q=0.009. As the value of q is decreased further to 0.57 the watermarked image becomes darker and finally become invisible and when the value of q is further increase above 1.6 the value of PSNR are decreases & the value of MSE is increases. We can see the watermarked image using discrete wavelet transform for different value of k & q, and the value of MSE & PSNR in Table 1 and Table 2 respectively.

Table 1 MSE for watermarked image.									
Frame no.	1	2	3	4	5	6	7	8	9
Salt & pepper	14.36	13.41	13.07	14.38	13.45	13.01	14.83	13.30	13.03
Median filter	48.65	47.73	56.14	48.59	49.28	54.18	47.83	49.55	56.06
Histogram attack	53.55	62.30	49.02	52.98	63.23	48.28	54.66	62.97	50.51
Sharpening attack	29.63	29.85	33.14	20.62	31.09	32.85	30.16	30.25	32.63
Gamma correction	06.55	05.38	06.02	05.97	05.49	06.04	06.24	05.35	06.23
Flipping attack	21.09	03.40	04.73	20.64	03.48	04.76	21.27	03.38	04.78
Scaling attack	16.22	15.02	19.13	16.36	15.49	18.85	16.12	15.02	18.97
Gaussian noise	37.75	39.42	40.35	38.25	39.88	39.88	39.25	39.53	39.84
addition									

Table 1 MSE for watermarked image.

Table 2 PSNR for watermarked image.

Frame no.	1	2	3	4	5	6	7	8	9		
Salt & pepper	36.59	36.88	37.00	36.58	36.87	37.01	36.45	36.92	37.01		
Median filter	31.29	31.37	30.67	31.29	31.23	30.82	31.36	31.21	30.67		
Histogram attack	30.87	30.21	31.26	30.98	30.15	31.32	30.78	30.17	31.13		
Sharpening attack	33.44	33.41	32.96	33.44	33.23	32.99	36.36	33.35	33.02		
Gamma correction	40.00	40.85	40.41	35.01	42.74	41.38	34.88	42.86	41.36		
Flipping attack	34.92	42.84	41.41	35.01	42.74	41.38	34.88	42.86	41.36		
Scaling attack	36.06	36.39	35.34	36.02	36.26	35.41	36.09	36.39	35.38		
Gaussian noise addition	32.39	32.20	32.10	32.33	33.15	32.15	39.22	32.19	32.16		

For the process of recovering of the watermark shown in fig. 7(b) from the watermarked video the value of k and q are same as for embedding. In this Method we consider that the original image & value of k are known for extraction. Recovered image using 1, 2 and 3 level discrete wavelet transform are independent of scaling factor. Best result for watermarked image & recovered image is obtained at k = 0.99 & q = 0.009.

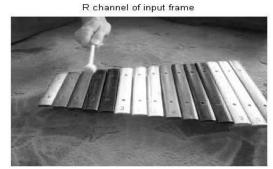
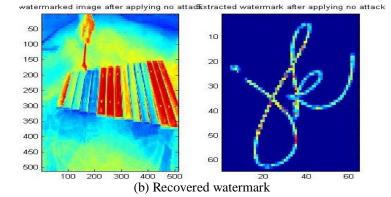


Figure 7: (a) Original video



VII. Conclusion

This paper shows a technique for non-blind video watermarking. The main aim of this paper is to achieve non-blind watermarking without need of original video at the receiver to save memory and bandwidth. This technique depends on image interlacing. A 3 level DWT based video watermarking technique has been enforced. This technique can embed the watermark into the video by using alpha blending technique which can be recovered by extraction technique. The quality of the image is depending upon the scaling factors and the recovered watermarks are independent of the scaling factor. The recovered images and the watermark are better for 3-level DWT then 1 & 2 levels. We have compared the performance of the proposed method with other non-blind watermarking methods, all the results obtained for the recovered images and the watermark are identical to the original images, and the robustness of this technique was tested by applying different types of attacks.

References

- Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, "A Survey on Digital Watermarking Techniques," International Journal of Computer Science and Information Technologies, Vol. 4 (3), 451-456, 2013
- [2] B. Pushpa Devi and Kh. Manglem Singh, "Dual Image Watermarking Scheme based on Singular Value Decomposition and Visual Cryptography in Discrete Wavelet Transform," International Journal of Computer Applications (0975 – 8887) Volume 50 – No.12, July 2012.
- [3] Nirbhay Kashyap, Shailendra Narayan Singh, "Analysis of Multimedia Watermarking Techniques" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 6, June 2014
- [4] S.Elango, Dr.G.Thirugnanam, R.Shankari, "A Survey of Digital Video Watermarking Techniques for Copyright Protection and Authentication," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 4, Issue 4, April 2015
- [5] Rini T Paul, "Review of Robust Video Watermarking Techniques," IJCA Special Issue on "Computational Science New Dimensions & Perspectives" NCCSE, 2011.
- [6] K. Su, D. Kundur and D. Hatzinakos, "A novel approach to collusion-resistant video watermarking", Proceedings of the SPIE, vol. 4675, pp. 491-502.
- [7] M. Kaur, S. Jindal, and S. Behal, "A study of digital image watermarking," International Journal of Research in Engineering & Applied Sciences, vol. 2, no. 2, pp. 126–136, 2012.
- [8] B. L. Gunjal and S.N.Mali, "Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces," International Journal of Computer Theory and Engineering, vol. 3, no. 6, 2011.
- [9] Bo Shen, Iihwar K. Sethi and Vasudev Bhaskaran, DCT Domain Alpha Blending, IEEE, 2008
- [10] Mohamed M. Ibrahim1, Neamat S. Abdel Kader 2, M. Zorkany3, "A Robust Image Watermarking Technique Based On Image Interlacing 31st National Radio Science Conference, Faculty of Engineering, Ain Shams University, Egypt April 28 – 30, 2014.
- [11] http://en.wikipedia.org/wiki/Image Interlacing.