AN EFFICIENCT VIDEO WATERMARKING TECHNIQUESBASED ON REVERSIBLE APPROACH FOR AUTHENTICATION

[1] K. VIJAYA LAKSHMI, [2] K. NAGU, [3] G. SUDHA

[1,2, 3] *Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510*

ABSTRACT

Everyday very huge amount of data is embedded on 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. These challenges motivated researchers to carry out intense research in the field of watermarking. In our approach wavelet based video watermarking technique in reversible image is proposed, initially original video frame is undergoing a alternative pixels share further one of the share is transposed and merged with remaining share form reversible image. Next wavelet is forced on the reversible image and marked the secret information in the medium level band of wavelet coefficients. Finally, the inverse wavelet transform is applied and rearranged the shares in the proper structure for yield the watermarked frames. An experimental result displays that the proposed approach can withstand the quality of the host image after copyright information is marked and robustness.

INTRODUCTION:

Development of wireless innovation has freely allowed to widespread the multimedia contents; it has made it possible to distribute multimedia content digitally by means of the World Wide Web to a large number of people in a cost-effective manner. While in transmission, an unapproved person may effortlessly acquire to and control the data; in this manner, the shield of information and distinguishing controls is a vital task [1-2]. Since the computerized information has no conflict between in the quality of an original and its copy [3-6]. Figure 1 shows the basic model of Information hiding tools. Copyright protection inserts authentication data such as ownership information and logo in the digital media without affecting its quality. In case of any dispute, authentication data is extracted from the media and can be used as an. authoritative proof to prove the ownership.

STEGANOGRAPHY:

Steganography is the art and science of invisible communication. This is a accomplished through hiding in formation in other information, thus hi ding the existence of the communicated in formation. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” de fining it as “covered writing”. In image steganography the information is hidden exclusively in images [4].

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques [5].

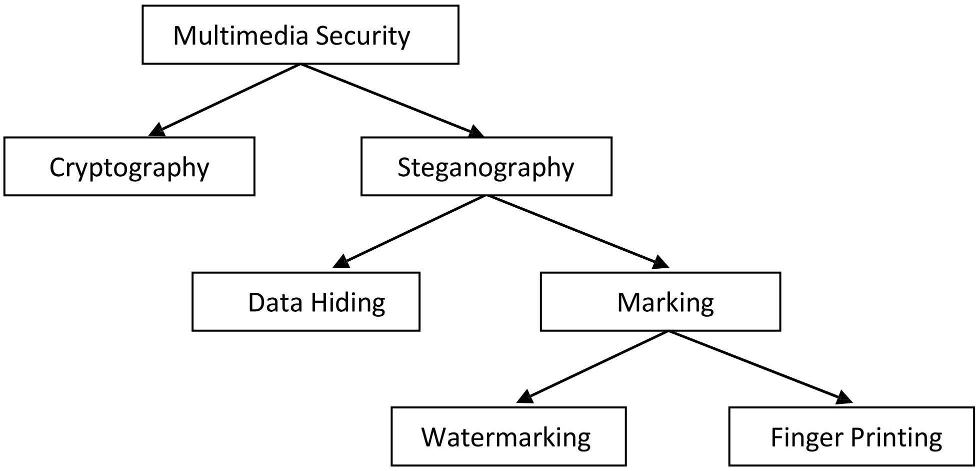

Fig 1: Information Hiding Tools

CRYPTOGRAPHY:

The word **cryptography** comes from the Greek words κ ρ υ π τ (hidden or secret) and γ ρ α φη (writing). Oddly enough, cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of un mangling [7].

The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In this book we will concentrate on the kind of cryptography that is based on representing information as number sand mathematically manipulating those numbers. This kind of cryptography can provide other ser-vices, such as •integrity checking—reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source. Authentication - verifying someone's (or something's) identity But back to the traditional use of cryptography. A message in its original form is known as Plaintext or clear text. The mangled information is known as cipher text. The process for producing cipher text from plaintext is known as encryption. The reverse of encryption is called decryption [8].

WATERMARKING:

Watermarking is defined as adding (embedding) a payload signal to the host signal. The payload can be **detected** or **extracted** later to make an assertion about the object i.e. the original data that may be an **image** or **audio** or **video**.Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object [9].

THE WATERMARKING PROCESS:

The watermarking process comprises of the following stages :

1. Embedding stage
2. Extraction phase
3. Distribution stage
4. Decision stage

CHARACTERISTICS OF WATERMARKING:

Robustness: The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, loss compression, translation, scaling, and rotation , and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting, image enhancement [10].

Imperceptibility: Imperceptibility (also known as Invisibility and Fidelity) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image.

Capacity: Capacity (also known as Payload) refers to the number of bits embedded into the image. The capacity of an image could be different according to the application that watermark is designed for. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness [11].

LITERATURE SURVEY:

Many algorithms have been put forward in the scientific review. Zhu *et al.* (1998), proposed an algorithm of embedding watermark into the static and dynamic temporal components generated from a temporal wavelet transform of the video. Using this scheme, the multi- resolution, watermark may be detected on single frames without knowledge of the location of the frames in the video scene, and is robust to the common attacks that video suffers in daily application.

Choong-Hoon *et al.*(2000), described an adaptive video watermarking scheme that used motion information for watermark embedding. Appropriate blocks for watermark embedding are selected using some criteria such as motion vectors and DBD. Selected blocks are the target of watermark embedding. For watermark embedding, blocks are transformed using wavelet transform and wavelet coefficients are changed using random signal. All selected blocks are tracked frame-by-frame and same watermark is embedded into the same block [12].

Chen and G.W.Wornell (2000), QIM techniques use different quantization code-books to represent the covered data with the selection of code-books based on the hidden information. QIM-based techniques usually have higher capacities than spread-spectrum schemes. The capacity of any QIM scheme is determined by the design of the quantization schemes [13].

Zhang *et al.*(2001), proposed a video watermarking scheme to embed watermark into larger value motion vectors. This technique has some good performance for hiding information in the MPEG video sequence. However, due to their watermarking motion vector, the modified motion vector will lead to frame dithering. In this paper, the author proposed a novel video watermarking scheme to watermark the original video based on locating motion region, using the independent.

Liu *et al.* (2001), presented a video watermark algorithm in the motion vectors. Firstly, the Y component of P frame is categorized into a high-texture area and low-texture area. The motion vectors are altered according to the texture of the area. Secondly, the prediction errors of the matched blocks are calculated again according to the changed motion vectors. Finally, the new motion vectors together with new prediction errors are encoded into compressed bit-streams. This algorithm can reduce the flaws and block the effects of watermarked video [14].

Solanki et al (2002), the authors propose to hide the large volume of information into the nonzero DCT terms after quantization. This method cannot provide sufficient embedding capacity for our application because surveillance videos have high temporal correlation with a very large fraction of DCT coefficients being zero in the inter coded frames [15].

Sun and Liu (2005), proposed another scene-based video watermarking scheme by using independent component analysis (ICA) to extract motion content from different scenes. Both of the algorithms are based on scene. In order to extract watermark, they should segment the scene accurately. However, the technique of scene segmentation is still a challenging problem in practical applications, especially the gradual changing scenes.

Koubaa *et al.*(2007), presented an efficient method for video watermarking which resists to collusion attack and MPEG compression. For this aim, the authors have used video mosaiking technique to introduce the same watermark into the same physical point along the whole sequence so as to resist collusion attack. On the other hand, creating a mark which depends on the local activity and the frequency of appearance of each pixel, make it more robust especially against MPEG compression. The main problems occur if the estimated warping parameters are not sufficiently precise [16].

J. Hussein *et al.* (2009), showed a new video watermarking scheme based on motion estimation for color video sequence in a frequency domain. This technique is tested on compressed (taken from DVD high quality film) and uncompressed (taken by digital camera) video movies. The watermark is the random Gaussian distribution which is embedded into the motion regions between frames (HL, LH bands). Experimental results show that the proposed new scheme has a higher degree of invisibility against the attack of frame dropping, adaptive quantization, and frame filtering than the previous developed scheme in spatial domain.

Mansouri *et al.* (2010), shows a new blind and readable H.264 compressed domain watermarking scheme in which the embedding/extracting is performed using the syntactic elements of the compressed bit stream. This approach is no need to fully decode a compressed video stream both in the embedding and extracting processes. Also presents an inexpensive spatiotemporal analysis that selects the appropriate submacroblocks for embedding, increasing watermark robustness while reducing its impact on visual quality. Meanwhile, the proposed method prevents bit-rate increase and restricts it within an acceptable limit by selecting appropriate quantized residuals for watermark insertion.

Maher El'Arbi, *et al.* (2011), proposed a video watermarking algorithm which embeds different parts of a single watermark into different shots of a video under the wavelet domain. Based on a Motion Activity Analysis, different regions of the original video are separated into perceptually distinct categories according to motion information and region complexity. Thus, the localizations of the watermark are adjusted adaptively in accordance with the human visual system.

Bhatnagar and Raman (2012) proposed a Wavelet Packet Transformation (WPT)- based robust video watermarking algorithm. A visible, meaningful binary image is used as the watermark. First, a sequence of frames is extracted from the video clip. Then, WPT is applied on each frame and from each orientation one sub-band is selected based on block mean intensity value called robust sub-band. A watermark is embedded in the robust sub-bands based on the relationship between wavelet packet coefficient and its 8-neighbour (D8) coefficients considering the robustness and invisibility.

Bhatnagar and Raman (2012) proposed a Wavelet Packet Transformation (WPT)- based robust video watermarking algorithm. A visible, meaningful binary image is used as the watermark. First, a sequence of frames is extracted from the video clip. Then, WPT is applied on each frame and from each orientation one sub-band is selected based on block mean intensity value called robust sub-band. A watermark is embedded in the robust sub-bands based on the relationship between wavelet packet coefficient and its 8-neighbour (D8) coefficients considering

the robustness and invisibility.

PROPOSED APPROACH:

Secret image sharing has received the considerable attention in the recent years. Secure assurance of images is taken as a primary concern in military or commercial based applications. In our proposed framework, color primary secret information is converted into YCbCr format and pick only the luminance band *(Y)* because the luminance layer has a high sampling rate.

Further this layer is grouped into alternative pixels shares and secondary watermark is concealed in one of the flipped shares. Further rearrange the concealed shares into normal form and stack the allotments into a single image. As per Equation (3.1), let us consider a luminance layer $A= (aij)mxn$, where m and n are the number of rows and columns.

```
lgorithm 1   :   Splitting of Image into two Shares
Input        :   Original Image
Output       :   Alternative pixels based shared Image

Step 1       :   For I from 1 to Rows do
Step 2       :   For J from 1 to (Columns/2) do
Step 3       :   If (I mod 2)! = 0 then  //Check rows are odd
Step 4       :   AX(I, 2*J-1)            //Read only odd rows and odd columns
Step 5       :   Else
Step 6       :   AX(I, 2*J)              //Read only even rows and even columns
Step 7       :   End If
Step 8       :   End For
Step 9       :   End For
```

EMBEDDING APPROACH:

Our proposed scheme adds the copyright information in low level band (Rll) of wavelet coefficients, because it is robust against filtering attacks, compression, Gaussian noise, scaling, and cropping. Initially the reversible image $[R]m$ x n is undergone the single level wavelet decomposition as shown in equation 3.7. Where Rll, Rlh,Rhl, Rhh are the sub bands. Scaling function (α) provides the embedding strength and it is reduce to weight of the image finally scaled watermark information is directly added to the wavelet coefficients.

Based on the equation inverse DWT is applied and obtain a watermarked image. Further the image is reconstructed in to normal form to yield the watermarked image. In order to strengthen the authentication of an image, copyright is marked in the reversible image. Hence the attackers are very difficult to prove the authentication. Figure 2 displays the overall process of the proposed system [17].

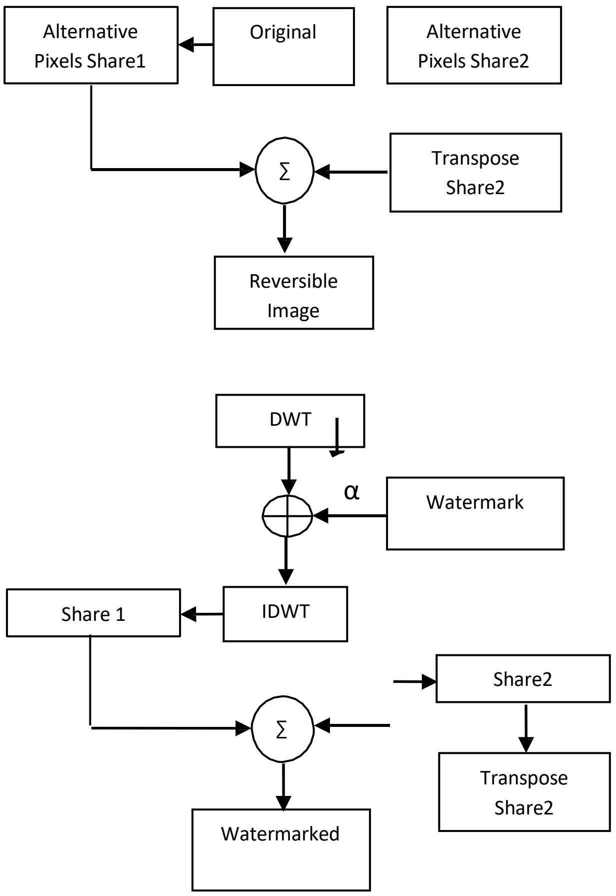

Fig 2: Proposed watermarking Scheme

EXTRACTING APPROACH:

In the extraction side again separate the watermarked image in to shares and form the reversible image, in our approach non blind technique is employed hence we required the original image for recovering the copyright information. First the reversible image undergone the wavelet and make the difference with watermarked and non-watermarked sub band yields copyright information. Above equations 3.10 and 3.11 shows the procedure of the extracting secret information [18].

CONCLUSION:

This technique can embed the invisible watermark into the image using dwt technique which can be recovered by extraction technique. Above study shows that the quality of the watermarked image is dependent only on the scaling factors and the recovered watermark are independent of scaling factor. All the results obtained for the recovered images and the watermark are identical to the original images. In this paper, the watermark is concealed into reversible image under wavelet. This reversible image is achieved by using the alternative pixels shares. The perception level of watermark is low and the watermarked image quality is high and it is hard to find the difference value between the watermarked and original image. Results achieved the low MSE values with the higher value of PSNR. Also this method gains the PSNR value around 51dB whereas SVD gains only 45dB.Our proposed approach is simple, efficient and with less complexity. In future this algorithm is implemented in video sequences.

REFERENCES:

[1] Qiao, L., and K. Nahrstedt, “Watermarking Schemes and Protocols For Protecting Rightful Ownership and

Customer's Rights", Journal of Visual Communication and Image Representation, Vol.9, 1998, pp.194–210.

[2] Arnold, M, Schumucker, M and Wolthusen, S, "Techniques and Applications of Digital Watermarking and Content Protection", Artech House,2003.

[3] Cox, IJ, Kilian, J, Leighton, FT and Shamoon, T , "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, 1997, pp. 1673-1687.

[4] Busch, C, Funk, W and Wolthusen, S, "Digital Watermarking: From Concepts to Real-Time Video Applications", IEEE Transactions on Computer Graphics and Applications, vol. 19, no. 1, 1999, pp. 25-35.

[5] C.T.Hsu and J.L.Wu, "Hidden digital watermarks in images", IEEE Transactions on Image Processing, vol.8, no.1, 1999, pp. 58–68.

[6] H. Y. Huang, C. H. Fan, and W. H. Hsu, "An effective watermark embedding algorithm for high JPEG compression", in Proc. Machine Vision Applications, 2007, pp. 256–259.

[7] L.Choong-Hoon, O.Hwang-Seok and L. Heung-Kyu, "Adaptive video watermarking using motion information", In: Proceedings of the SPIE security and watermarking of multimedia contents II, vol. 3971, 2000, pp 209–216.

[8] B. Chen and G.W.Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," in Proceedings of the IEEE International Symposium on Information Theory (ISIT "00), Sorrento, Italy, June 2000.

[9] K. Bhargavi. An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. Journal of Engineering, Computing and Architecture.2020;p.148.

[10] [21] M. Kiran Kumar , S. Jessica Saritha. AN EFFICIENT APPROACH TO QUERY REFORMULATION IN WEB SEARCH, International Journal of Research in Engineering and Technology. 2015;p.172

[11] K BALAKRISHNA,M NAGA SESHUDU,A SANDEEP. Providing Privacy for Numeric Range SQL Queries Using Two-Cloud Architecture. International Journal of Scientific Research and Review. 2018;p.39

[12] K BALA KRISHNA, M NAGASESHUDU. An Effective Way of Processing Big Data by Using Hierarchically Distributed Data Matrix. International Journal of Research.2019;p.1628

[13] P.Padma, Vadapalli Gopi,. Detection of Cyber anomaly Using Fuzzy Neural networks. Journal of Engineering Sciences.2020;p.48.

[14] Kiran Kumar, M., Kranthi Kumar, S., Kalpana, E., Srikanth, D., & Saikumar, K. (2022). A Novel Implementation of Linux Based Android Platform for Client and Server. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 151-170). Springer, Cham.

[15] Kumar, M. Kiran, and Pankaj Kawad Kar. "A Study on Privacy Preserving in Big Data Mining Using Fuzzy Logic Approach." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 11.3 (2020): 2108-2116.

[16] M. Kiran Kumar and Dr. Pankaj Kawad Kar. "Implementation of Novel Association Rule Hiding Algorithm Using FLA with Privacy Preserving in Big Data Mining". Design Engineering (2023): 15852-15862

[17] K. APARNA, G. MURALI. ANNOTATING SEARCH RESULTS FROM WEB DATABASE USING IN-TEXT PREFIX/SUFFIX ANNOTATOR, International Journal of Research in Engineering and Technology. 2015;p.16.

[18] J.Zhang, J.Li and L.Zhang , "Video watermark technique in motion vector", In: Proceedings of XIV Brazilian symposium on computer graphics and image processing, 2001, pp.179–182.