International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

A Survey on Various Techniques Used to Add Watermark to Multimedia Data for Digital Copyrights Protection

A.R.Zade, Sanjana Konde, Purva Patil, Pratik Navasare, Riah Dhanani.

A.R.Zade: Professor, Dept. of I.T. Engineering, Rajarshi Shahu College of Engineering, Maharashtra, India.
Sanjana Konde: Dept. of I.T. Engineering, Rajarshi Shahu College of Engineering, Maharashtra, India.
Purva Patil: Dept. of I.T. Engineering, Rajarshi Shahu College of Engineering, Maharashtra, India.
Pratik Navasare: Dept. of I.T. Engineering, Rajarshi Shahu College of Engineering, Maharashtra, India.
Riya Dhanani: Dept. of I.T. Engineering, Rajarshi Shahu College of Engineering, Maharashtra, India.

Abstract - *Now-a-days more people are using photos/audio/video to record their special activities and also share them on the social media. But these may be used without permission after they are uploaded on the internet, and this is a difficult problem to overcome. An watermark needs to be added to the data. The goal of this paper is to understand various techniques proposed recently to protect the multimedia data from being illegally used. The next step in this path would be to come up with a better solution to solve this problem. The following discussed techniques are very good. A collaborative approach using few of them can be a better solution.*

Key Words: **Watermark, Multimedia Data, Copyright Protection,**

1.INTRODUCTION *(Size 11 , cambria font)*

As there is growing interest in developing techniques for discouraging the unauthorized duplication and misuse of digital data, the process of digital watermarking is used to prove the ownership of the data.

1.1 Watermarking

"Watermarking" is the process of hiding digital information in a carrier signal; It is prominently used for tracing copyright infringements and for banknote authentication. Requirements and design of watermarking techniques are impacted by the different types of content in two major ways.

This technique leaves the original data unchanged and imposes modification which can be detected using appropriate extraction algorithm. We are designing the internet portal which will help us to protect photographs, audios and videos which are used by users to prevent copyright of owner. User has to register and then login to our system for accessing copyright protection has to upload Image, Video or Audio file on server, go to Add Watermark link to add watermark into multimedia file, select Image as Digital Watermark to embed into Video/Image/Audio file along with Secret Key required for embedding watermark into Multimedia.

1.2 Classification of Digital Watermarking

There are many algorithms which are being used to hide the secret in-formation. These algorithms can be categorized into two domains called:
A. Spatial domain and
B. Frequency domain.
Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. On the other side, in frequency domain techniques the image is first transformed to the frequency domain by the use of any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT). Now the information is added to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image.

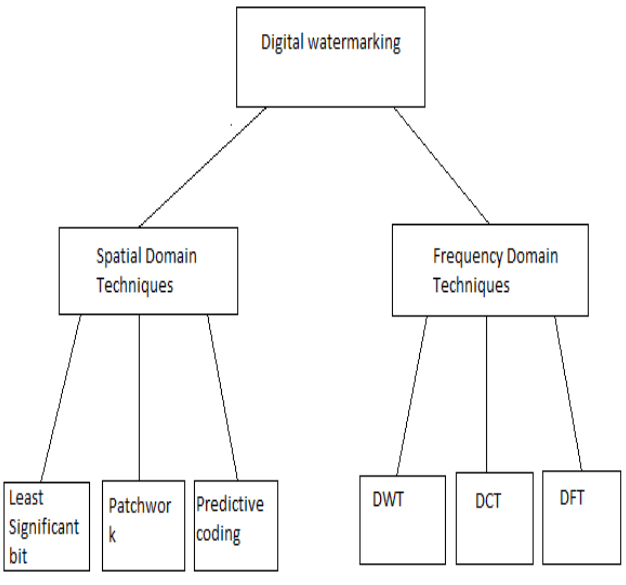

Fig 1 – Classification of Digital watermarking

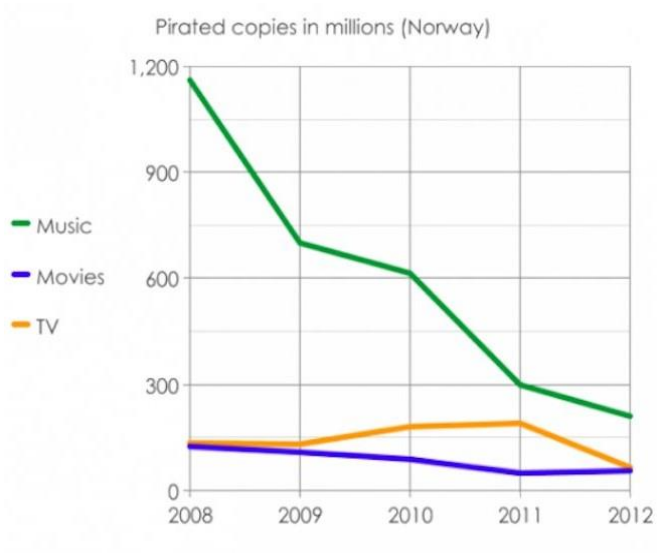

Fig 2 – Piracy rate graph

The above graph illustrates the piracy reports of Norway from the year 2008 to 2012. It shows the piracy rates for multimedia data like the audio and video. The rate of making pirated copies of the authors/writers/directors/copyright holder's original work is growing day by day and year after year. Different attacks are done on the copyrighted data with the motive to steal the original copy and make n- number of duplicate copies. Such duplicate copies are sold illegally.

1.3 Applications of Digital Watermarking

1. Owner Identification: It establishes ownership of the content.
2. Copy Protection: It prevents people from making illegal copies of copyright content.
3. Authentication of Content: To detect modifications of the content as a sign of invalid authentication.
4. Fingerprinting: Trace back illegal duplication and duplication of the content.
5. Broadcast Monitoring: Especially for advertisements and in entertainment industries, to monitor content that is broadcast as contracted and by the authorized source.
6. Medical Applications: Used to provide both authentication and confidentiality without affecting the medical image in any way.

2. PROJECT SURVEY

[2.1] ***Copyright protection for e-learning videos using digital watermarking*** **[1] -** In this paper, the authors have described that one of the major strategies to be implemented to reduce risks associated with E-Learning assets is digital right management. Digital watermarking is one of the methods to protect the multimedia data. It is a concept of hiding some data or details about the ownership. The decoding is based on the side information which is produced at the time of watermarking. The information embedded in the multimedia content is called a watermark. They have also proposed methods for data insertion which uses frequency domain transforms (Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT).
One of the major strategies to be implemented to reduce risks associated with E Learning assets is digital right management. The watermark method explained in this paper is for e learning lecture videos. It can also be used for general purpose. The result shows that the DWT method is more efficient when an attack is done on the watermarked videos.

[2.2] ***Watermarking of compressed images using SWT technique and Fragile approach*** **[2] -**In this paper, the authors have discussed about the two different categories if watermark namely, robust and fragile. To check the ownership of the image Identity Number is used and Hash function for integrity. Discrete Cosine transform (DCT) and the discrete wavelet transform (DWT) are used to do watermark the images. Digital image watermarking is data hiding technique that insert watermark signal into the host image signal for authorization or integrity check. The authors have explained the purpose of robust watermarking, which is to check the ownership data (images) and fragile watermarking checks integrity. The authors have also explained that the Stationary Wavelet Transform (SWT), which overcomes the problems of the DWT, can be used to insert the robust watermark.

[2.3]*Digital watermarking in audio for copyright protection* **[3] -** Digital watermarking technologies have been acting as appropriate tools to verify the owner, of a document or an image. Watermarking of multimedia content is important to authenticate, copy-control and ownership detection. The scheme used in this paper an efficient robust audio watermarking algorithm based on double transforms is introduced. In this paper an efficient robust audio watermarking algorithm based on double transforms is introduced. In a first step, the original signal is decomposed by discrete wavelet transform (DWT). Then the prominent approximation coefficients are segmented in non-overlapping 2D blocks. Singular value decomposition (SVD) is applied on each one. The watermark is embedded in the singular values (SVs) for each block. Watermark extraction is non-blind and it's done by performing inverse operation of embedding process. Experimental results show that this scheme provides high robustness against common signal processing attacks such as noise addition, resampling, MP3 compression and maintains good perceptual transparency. In addition, this method uses a double key for insertion and extraction, making it suitable for secure application such as copyright protection.

[2.4] ***Image encryption using camellia and chaotic maps*** **[4] –** In this paper, the author has used a new image encryption approach. This approach uses the camellia block cipher algorithm which is combined with logistic chaotic map. Also he has used a key-scheduling algorithm for round key generation. This approach which was proposed by the authors was tested for both grey scaled and colour images. After many efforts, they were able to reduce the rounds used in AES and DES algorithms and combined them with chaotic maps so that these algorithms would become suitable for image encryption and could also face different attacks like the Brute Force attack. The authors also used the 128-bit block cipher algorithm called as the Camellia which was developed by NTT and Mitsubishi. This algorithm had high resistance against various attacks. In this work, the authors aim to use the Camellia algorithm for encryption of images. The results of the algorithms proposed by the authors confirm that it has excellent properties such as: large key space, they are resistant to attacks, and they are very sensitive to small changes in the key.

[2.5]*Image encryption techniques based on Chaotic System Hash Function* **[5] –** In this paper, the authors have written about the encryption techniques which can be used for encrypting an image over an unreliable network. Their proposed method encrypts the image using chaotic system, Wavelet transform along with that the fingerprint of the image is created using hash function which is then transmitted over an unreliable network to the receiver. This method maintains the privacy of the image. The Wavelet transform is multi-frequency channel decomposition method. It breaks the image into sub images which provide the frequency of the image. To access the information the fingerprint functions are used as high frequency hash function. The results of the authors work, show that their methods maintain the privacy over the networks which are not reliable but it fails to maintain the integrity.

[2.6]*Image Security Using Quantum Rivest-Shamir-Adleman Cryptosystem Algorithm and Digital Watermarking* **[6] -** In this paper, to achieve the CIA triangle for security, the authors have proposed to use the RSA algorithm in combination with the Digital watermarking algorithm. Also the hybrid discrete wavelet transform and singular value decomposition algorithms for embedding and extracting process of digital watermarking is used. The results showed that the histogram for the sender and receiver are same. The proposed model maintains a very good image quality.

To secure the secrecy of communication cryptography technique is used. The authors have used the benefits of quantum mechanics to accelerate the RSA algorithm's encryption process. They have compared DES and blowfish algorithms and the results showed that that time taken using mathematical relations in RSA make steps faster implemented than DES and blowfish algorithms and with more secured data than symmetric systems. They also have presented a new proposal that merges between the merits of classical cryptography and quantum cryptography. It took advantage of LSB Algorithm to hide the cipher text process. This process completes the authentication of the picture in very less time. RGB image was used for the process and sent to the Recipient. The authors also have used the same image and created a watermark on those images using DWT and SVD to embed and extract of the watermark. The authors have worked on the same image but the format is of grey scale.

Results showed accelerate the encryption process using RSA with quantum ideas compared with RSA only. This model maintains the image quality is good.

[2.7]*Copyright for Images with Chaotic Sequence* **[7] -** People use multimedia (images, video and audio) to record their special moments and also share them on the social media. But sometimes these are used without the permission of the owner i.e. illegally. Thus to resolve this problem, invisible watermarks are added to the images, video or audio. But sometimes when the number of photos is more, then this process is lengthy. Thus the authors have proposed a watermarking process for copyrights on the android platform. Using this system the pre-specified copyright information is automatically embedded on the multimedia before uploading it on the internet. Also the images can be obtained in original form later whenever needed. Thus it is useful when uploading images from android phones to the internet. As people give preference to android phones over computers, the authors have proposed to co pyright images using android and thus avoid piracy. This application creates images with some copyright information.

Chaos is all about nonlinear dynamics law control of the data stream generated and is similar to random noise. The new binary sequence, which is the binarization of acquired chaotic sequence, has two main functions as follows:

A. It is used to the encryption of text data information, which can enhance the security of the steganography.

B. It is used to stimulate the binary data stream, which can facilitate the process of various experiments.

Chaos Equation –

$$Xnew = K .Xold(1 - Xold)$$

Thus the results show that changes cannot be made to original images illegally. As the original image goes through many embedding processes, editing is very difficult. And as android is used by many people, anyone can use the application for securing the images.

[2.8]*Robust Copyright Protection of Raster Images Using Wavlet Based Digital Watermarking.[*8]- In this paper , the authors depict a scheme to protect copyright of raster images using wavelet transform. Here to embed and extract the watermark from the raster image third level wavelet coefficients (LL and HH) are used. The classification of original and watermarked data is performed and it is

observed that the proposed watermarking scheme leads to less misclassification. The proposed algorithm has transparency, strong, large data hiding capacity and correct extraction of watermark, and also has strong robustness against JPEG lossy compression, filtering, and noise.
The classification of Watermarking techniques is done into spatial domain methods and transforms domain methods. Spatial domain methods are less complex, but less robust against attacks. Transform domain methods alter frequency transform of data elements to embed watermark data. Thus, the authors have proposed wavelet based watermarking scheme for raster image copyright protection. The authors have utilized both low frequency and high frequency band of wavelet at third level with 'Haar' wavelet.

[2.9]*A Secure and Robust Digital Image Watermarking Scheme using Repetition Codes for Copyright Protection* [9]- In this paper, the authors have discussed about the Digital Image Watermarking which is used to hide the copyrighted information as a watermark inside a Digital image, to identify the ownership. To ensure the security watermark is first encrypted by standard A5/1 algorithm is illustrated in this paper**.** The perceptual quality of watermarked image remains almost unchanged. For performance evaluation Normalized Correlation (NC) and Bit Error Rate (BER) are computed.
To resolve copyright ownership and verifying the originality of digital contents a strong technique may be needed. One such strong solution for copy right protection as described by the author for digital data is provided by Digital watermarking. It is a branch of information hiding, used to hide secret information inside the original image also called as cover image. The hidden information also known as the watermark may be in text, binary image or audio form.
After inserting or embedding the watermark, the original image will get modified. The Modified image is called as watermarked image. When this watermarked image is stored in a digital device or transmitted through a wireless channel it may be affected by noise which in turn affects the quality of extracted watermark. Due to this noise sometimes watermark may deteriorate and even ownership cannot be identified. Digital image watermarking scheme must satisfy three major properties such as Perceptibility, Robustness and Security. Perceptibility means embedded watermark should not visually distort the original image and must be invisible. Robustness means embedded watermark is reliably detectable against noise and signal processing attacks and not easy to detect or modify by the unauthorized person. Security means even if embedded watermark is detected by intruder it should not be decodable without knowing secret key. Applications of Digital Image Watermarking mainly include copyright protection, tamper detection, content authentication and confidentiality.

[2.10] *An Audio/Speech Watermarking Method for Copyright Protection* [10] - Protecting the copyrights of multimedia content is for discourage of unauthorized distribution or sharing of the content over Internet. Digital watermarking is the process of inserting owner related information as a watermark into a host signal such as audio or image or video without disturbing quality of the host signal. Digital watermarking helps in protecting the copyrights reducing the monetary loss to the content owner. The main characteristic of a digital watermarking is to enable accurate watermark detection even if the multimedia content undergoes some changes that may eliminate the watermark from the content. These changes include compression, rate conversion, filtering and noise addition etc. We present a watermarking that can be used for both audio and speech watermarking. Watermark embedding is done using singular values obtained by applying Singular Value Decomposition (SVD) on the structured Discrete Wavelet Transform(DWT) coefficients, correlation peak to side-lobe ratio(PSLR) metric is used to detect watermark from the correlation output, which is computed between the singular values obtained from the watermarked content and each watermark in the database. This proves the robustness of proposed method while satisfying the imperceptibility criteria.

[2.11]*Data Hiding Technique in Video Using a Secrete Key*[11] - Data hiding has increased the recent activity in digital copyright protection. The way of protect the image is to secretly embed data in content of the image. The owner can hide the message using hiding key in any cover medium. The receiver does these things in reverse way for getting back the original message the data hiding key is employed to extract the secret message and get back the original content.
We will present the overview on the use of data hiding technique using the LSB on video. One of the major disadvantage with simple LSB method is that, while inserting the secrete data into the target image it can change the least significant bit of the entire image pixel. We can destroy the hidden message by changing the quality of image. To overcome this limitations we are proposing improved LSB with 1, 4, 3 bit position techniques. Using the block size 4x4 we can hide data. We will review development in data hiding technique; specifically it is secure data hiding in the image. We mainly focus on data hiding techniques and importance of data hiding and the goal that must be achieved of data hiding technique. Data hiding provides the security to secrete data.
The existing system contains some disadvantages to remove the disadvantages such as data extraction and recovery of image are free of errors by adding reversible manner.

[2.12]*A Novel image watermarking scheme using block coefficient in DHT Domain.*[12] - In this paper, the author discusses about usage of data over the internet. Duplication and alteration is been done. In this paper, they have proposed a novel blind watermarking scheme in hadamard transform for digital image. In this they modify the DHT coefficient of two adjacent blocks in same position.

This algorithm was easy to implement with low computational cost and high resiliency under compression. Discrete hadamard transform and its variant are used to develop watermarking algorithm. In this paper we came across the fact that watermarking must have proper fidelity and high PSNR.
2D Hadamard transform is based of Hadamard transform matrix which can be conveniently use for image processing. If we have to use Hadamard transform on the image size 2^n, then we need hadamard transform matrix H to the base n. With the simple rules they easily calculated forward and inverse hadamard transform.
In this paper they have proposed an algorithm to change DNT coefficient of blocks. In this the algorithm is based on inter- block DHT coefficient correlation. In this the message selected as a watermark is changed to binary string and permuted using user selected key. Then they divided the image into 8*8 blocks and in case image is M*N then it is divided into (M*N)/64 only if M and N are multiple of 8. Two DHT coefficient of adjacent DHT block satisfy the relationship Bx,y(i,j) > Bx,y+1(i,j) or Bx,y(i,j) > Bx+1,y(i,j) they will use to embed bit 1 and if they satisfy the relation Bx,y(i,j) < Bx,y+1(i,j) or Bx,y(i,j) < Bx+1,y(i,j) they will be used to embed bit 0. In other words the two adjacent 8*8 DHT blocks, two DHT coefficients of adjacent blocks at same position are modified to satisfy the condition given above. To extract the watermark they have divide the image into 8*8 non overlap blocks and applied hadamard transformation to each adjacent blocks. Calculate the Δ for each two adjacent blocks. If Δ is placed in the sector 2 or 4 the binary bit is 1 and sector 1 or 3 the binary bit is 0 is extracted. Then they save the binary bit in array and apply inverse permutation on bit using permutation key and change bit to char to get watermark string.
In this good quality of watermark is extracted with high values of PSNR and NCC. And this technique is more reliable.

[2.13]*A new algorithm on wavelet based robust invisible digital watermarking for multimedia security* [13] - This paper has a new algorithm based on wavelet for multimedia security. This algorithm is design, implemented and verified using MATLAB R2014a for extraction and embedding of the watermark. The advantage of the wavelet based technique this method use to watermark in each of resolution levels. In this paper they have provided simultaneous spatial localisation and frequency spread of the watermark within the host image. The wavelet basis have two scaling function 0 and wavelet function +. In wavelet basis set has one scaling function and all other elements are wavelet functions.
They have took grayscale cover image to which they have applied 2D bi-orthogonal DWT and gpt coeff matrices defining approx., horizontal, vertical and diagonal details as LL4, LH4, HL$ suands. Then they took PN-sequence of equal size that of wavelet transformed coefficient matrix. Take a binary watermark of size(m*m). Finally they added PN-sequence and the watermark element by element. This algorithm has good imperceptibility and robustness.

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

3. CONCLUSIONS

This paper discusses about the use of multimedia done illegally. So, to resolve this problem of checking copyright ownership and verifying the originality of digital contents a strong technique of digital watermarking is used. This paper gives a overview of few of the techniques used for watermarking. Undoubtedly the techniques discussed above are extremely useful.
Next step in this path is to compare and evaluate the various mechanisms by creating sets of data and an experimental testbed or to come up with the collaborative approach to find more efficient solution to defend against illegal use of multimedia. In this paper, we tried our best to give the information of digital watermarking which will give benefit to new researchers to get the maximum awareness about this domain.

REFERENCES

[1] 2015 Fifth International Conference on Advances in Computing and Communications "Copyright Protection For E-Learning Videos Using Digital Watermarking. Neena.P.M Athi Narayanan.S Kamal Bijlani Amrita E-Learning Research Lab Amrita Vishwa Vidyapeetham University, Amritapuri Kollam, Kerala, India line

[2] Watermarking of Compressed Images Using SWT Technique and Fragile ApproachMohmmad Ali M. Saiyyad Dept. of Computer Engineering Nitin N. Patil Dept. of Computer Engineering R.C. Patel Institute of Technology, Shirpur Dist-Dhule, Maharashtra, India.

[3] "Digital watermarking in audio for copyright protection" Mustapha Hemis and Bachir Boudraa Speech communication and signal processing laboratory University of Sciences and

Technology Houari Boumediene (USTHB) BP 32 El Alia, Algiers, Algeria

[4] Marva S. Elpeltagy, Moataz M. Abdelwahab, Mohammed S. Sayed, "Image encryption using camellia and chaotic maps", IEEE international symposium on signal processing and information technology (ISSPIT) 2014.

[5] Manish Mishra, Shraddha Pandit, "Image encryption techniques based on Chaotic System Hash Function", IEEE international symposium on signal processing and information technology (ISSPIT) 2015.

[6] 2016 Progress In Electromagnetic Research Symposium (PIERS), Shanghai, China, 8–11 August "Image Security Using Quantum Rivest-Shamir-Adleman Cryptosystem Algorithm and Digital Watermarking" Hend A. Elsayed1, Yasir Khalid Jadaan2, and Shawkat K. Guirguis2 Alexandria University, Alexandria, Egypt

[7] International Journal of Research (IJR) Vol-1, Issue-5, June 2014 **ISSN 2348-6848** "Copyright for Images with Chaotic Sequence" Prof.P.M.Patil, Mr.Shreyas Shinde, Miss.C.V.Arekar Miss.N.M.Bhandwalkar Vidya Pratishthan's College of Engg, Baramati Pune- 413133

[8]"ROBUST COPYRIGHT PROTECTION OF RASTER IMAGES USING WAVELET BASED DIGITAL WATERMARKING" *Sangita Zope – Chaudhari, P. Venkatachalam* Centre of Studies in Resources Engineering, Indian Institute of Technology Bombay, Mumbai, India.

[9] "A Secure and Robust Digital Image Watermarking Scheme using Repetition Codes for Copyright Protection "Rohit S, K. S. Hari Bhat Department of TCE, M S Ramaiah Institute of Technology Bangalore, Karnataka, India.

[10] 2015 Third International Conference on Artificial Intelligence, Modelling and Simulation An Audio/Speech Watermarking Method for Copyright Protection Krishna Rao Kakkirala, Srinivasa Rao Chalamala, Bala Mallikarjunarao Garlapati TCS Innovation Labs, Hyderabad, India krishna.kakkirala@tcs.com, chalamala.srao@tcs.com, balamallikarjuna.g@tcs.com

[11] 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16) *Data Hiding Technique in Video Using a Secrete Key* Miss. Chaitali. D. Raut *M.Tech., Dept. of Information Technology Y.C.C.E., Hingna Road, Wanadongari Nagpur- 441110, India raut.chaitali3@gmail.com*

[12] "A Novel image watermarking scheme using block coefficient in DHT Domain."

[13]A New Algorithm On Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security Sudip Ghosh, Subhojit Chatterjee School of VLSI Technology IIEST, Shibpur Howrah, West Bengal, India