International Journal of Electrical, Electronics and Computer Engineering **4**(2): 42-46(2015)

ISSN No. (Online): 2277-2626

Watermarking and it's Various Techniques: A Review

Khushboo Pawar and Bhawana Pillai

**Research Scholar, Department of Computer Science and Engineering, LNCT(S), (MP), INDIA*

***Associate Professor, Department of Computer Science and Engineering, LNCT(S), (MP), INDIA*

(Corresponding author: Khushboo Pawar)

(Received 03 June, 2015 Accepted 12 August, 2015)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Due to the rapid development of network technology, Multimedia such as text, image, video and audio has now been widely used. Humans can easily access or distribute any multimedia data from networks. Hence, the protection of intellectual property becomes more and more attentive and important for the society. Digital watermarking has been proposed for resolving copyright protection of multimedia. The digital water marking is a data hiding technique, where we input the message embeds into multimedia which having some application likes image or text or other digital objects. The digital watermarking system is taken as a data cancelling process which have their personal needs and that ultimately makes the digital watermark as tough as possible.

Keywords: Watermarking, Digital watermarking, steganography, Watermark Security and Keys, Robustness Imperceptibility

I. INTRODUCTION

In recent years, as digital media are achievement wider popularity, their security related issues are suitable superior concern. Digital watermark was first discovering in 1992 by Andrew Tickle and Charles Osborne [1, 2]. Watermark is derived from the germen term "Watermark". The first watermarks devolved in Italy while 13th century, but its usage apace spread across Europe. Watermarking can be measured as special techniques of steganography where one message is embedded in another and the two messages are related to each other. Digital watermarking is similar to watermarking technique which allows an individual to add exclusive rights notices or other verification messages to digital media. Image authentication's one of the applications of digital watermarking, which is used for authenticating the digital images. A digital watermark is taken as covertly embedded a noise-bearing image like audio or image data. It is mostly work to find out ownership of that copyright like image. "Watermarking" is a method of cancelling digital information as image the cancelled information must not need to relate with that image. The security and enforcement of academic property rights for digital media has become an important issue [3]. The way to understand this feature is to embed a level of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values.

There are many spatial and frequency domain techniques are available for authentication of watermarking. Watermarking techniques are judged on the basis of their performance on a small set of properties. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i.e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. Digital signature is also a verification scheme that is used for verifying the reliability and authenticity of the image content. A digital signature can be either an encrypted or a signed hash value of image contents and image characteristics.

A. Steganography

Steganography is a process that deals with secret communication by embedding or cancelling the secret information in trusted data. Steganography count on the suggestion that depends on secret communication is not familiar to third parties. Steganographic technique is non robust; the canceled information will not be leaked after data being exploit.

B. Characteristics of Digital Watermarking

There are three main Properties of digital watermarking technique.

Transparency or Fidelity: The digital watermark should not affect the quality of the original image after it is watermarked.

Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

Robustness: Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks.

Capacity or Data Payload: This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark must be capable of carrying proper information to represent the uniqueness of the image. Different application has different payload requirements [4].

C. Digital Watermarking

Requirements: The fundamental needs for digital watermarking are as below:

1) Digital watermarking able to supply as much information as possible, or the data rate should be very higher

2) Only genially parties should have the permission to operate the watermark. Its can be possible by the application of cryptography.

3) Robustness must be there in watermarking. Which will further helps in Copyright protection implementation or conditional access application.

4) A watermark is supposed to be irremovable as well as unnoticeable.

Some additional needs on the basis of media and its application are as below:

(a) The recovering process of watermark, at that time, its sometimes permit the usage of original or un watermarked host data.

(b) Watermark embedding mostly needed in real time like as, for video fingerprinting. Here we are suppose to deals with the compressed-domain embedding technique.

(c) Watermarks are supposed to supply few casual information also. As below some of the given requirements and the output design issues shown in brief".

1) Watermark Security and Keys: Safety measures that are security of the flow of information is essential, which can be possible by the application of cryptography. Cryptography is taken for embedding and taking out methods, pseudorandom signals are embedded as an example of watermark.

Here the pseudorandom number is taken as a key. In watermarking there are 2 stages of privacy, an unknown user not even read and decode the watermark information. If a certain set of data which is already being watermark is being available for the unauthorized user, then the information which is present in that data can not be read unless the user having those private keys. there are 2 watermarks which are available first one is the public key and the second one is the secrete or private key, sometimes a combination like public/private keys also taken in action as more discuss in [5].

There are some issues take place while making the copyright protection system such as key generation, key distribution management (by key distribution Center) and many more system have been consider

2) Robustness: Robustness is taken a major factor in the watermarking scheme. As the robustness oppose the distortions on the standard data process. The standard data processing involves many manipulations and changes which may be go inside in a proper distribution chain, like data editing, printing, enhancement and format conversion. Here "Attack" stand for the data manipulation and which deals with the impairing, destroying or eradicating watermarks. The robust watermark methods are being made when the watermark not get public. The watermark becomes vulnerable for attacks when watermark detector principle and key become public [6], [7]. Hence, public watermarks is taken in literature, not become robust unless every receiver start using not similar key. Practically it is tough hence it will increase collision attack.

3) Imperceptibility: Perceptual transpararecy is the major needs for watermarking process. Perceptible artifacts are not suppose to be attached with the data. With the view to achieve peak consistency the watermark amplitude must also be high. Therefore the shape the this process should have tradeoff in between imperceptibility and robustness. The watermark should be taken below the threshold of perception. but sometimes its become hard to obtain threshold in real world image and audio signals..Many operations done to find out perceived distortion and the threshold of perceived deals with the mentioned media [8].But somewhere they are still lack behind the human viewers and listeners, who observe the audio fidelity with the help of the blind test. Therefore with the shape of the watermarking methods it becomes very necessary to have some tests with volunteers. The another problem take place with the combination of post watermarking technique, which will results in the amplified embedded watermark and then make it as perceptible. Zooming of watermarked image is an example, that will make it visible or contrast enhancement, which will make it amplify with speedy frequent watermark them, if this process not take place then it become invisible.

4) Watermark Recovery With or Without the Original Data: The watermark regaining process is very robust, when the original data which is not watermark is present ,the future regaining of data set permits the searching as well as inversion of diversion , this will make its geometry different. If we provide at rotation to a watermark with the help of an attack then the original data in not present in all cases for the applications like data monitoring and data tracking. Its is not applicable to use original data for the applications like video watermarking the reason behind it is the heavy data volume, It is also possible to generate a watermarking in absence of original for the purpose of extraction. All sort of watermarking deals with the modulation process where the original data is taken as distortion, if we are familiars with the distortion or observe in the further duration it will permits us to compress it in absence of original data.

Some of the watermarking techniques does not have the need of original data for the purpose of the recovery, those kind of methods known as "blind" watermarking techniques[9, 10]

5) Watermark Extraction or Verification of Presence for a Given Watermark: Usually two sort of watermarking system are present in the literature, first one is system that gives the specific information or pattern and also find the proper existence of the known information afterwards at the time of recovery of watermark son the basis of hypothesis method. And the processor that convey the arbitrary information into the host data. In the first type which is for the known watermark is suitable for the for kind of copyright-protection application, on the other hand the next type of watermarking is mostly applicable for image tracking depended on internet with smart users .In some cases where the only source of interest is discover images and classify it, at that time we are suppose to serve them a watermark identification number , a different example where we are suppose to insert the arbitrary information for the purpose of video distribution for better understanding we are taking an example like the serial number of that receiver is suppose to be embedded.

II. LITERATURE REVIEW

In this portion we are looking for the overview of digital watermarks which deals with digital media. It explain the earlier work. Which have already done on digital watermarking by using its methods, also the analysis of several watermarking approaches and their outcomes

Giri *et al.* (2014) presented channel wise watermarking scheme for colored image based on DWT. In algorithm, level one DWT is applied on each distinguished color channel. The algorithm is robust against various attacks like Gaussian noise, JPEG compression, salt and pepper noise [11]. Khanduja *et.al* (2014) [12] proposed robust multiple watermarking technique for relational database. He not only did ownership protection but also recovered the information. In 2014, Eswaraiah *et.al* [13] presented fragile ROI based medical image watermarking

technique with tamper detection and recovery. In his algorithm Fragile watermark is stored in LSBs of ROI region and tempered information of ROI part is recovered without any loss. Run length encoding scheme is used to enhance the embedding capacity. Limitation of this algorithm is RONI part is not reversible. Joshi *et al.* (2014) [14] presented paper on secure medical image watermarking. In his paper he embed dual watermark. For the embedding, DWT and Arnold transform is used. It is used only on gray scale images. Both DWT and Arnold transform enhances the security.

Kaur *et al.* (2013) [15] reviewed paper on image watermarking Using LSB. She worked on spatial domain technique. Philip *et. al* (2013) [16] evaluated Development of a New Watermarking Algorithm for Telemedicine Applications. Embedding of watermark is done in both DCT and DWT transform and their performance is evaluated. DCT and DWT is compared by taking different value of alpha. Watermark embedding is done in different decomposition level and analyzed.

Ghosh *et.al* (2012) [17] evaluated a novel digital watermarking technique for copyright protection of video. In this paper he embedded both the invisible and visible watermarks. This increases robustness.DWT is used for embedding. This worked on gray scale and on video of uncompressed .avi format [17]. Naseem *et.al* (2012) [18] proposed robust watermarking technique for medical images which is resistant to Geometric attacks like rotation, scaling ,translation .In his work main focus is on robustness rather than imperceptibility. In the algorithm, firstly image is made invariant against by statistical moment normalization then watermarked image is crumbled.

Bamatraf *et. al.* (2011) presented a new digital watermarking algorithm using combination of Least Significant Bit and inverse bit. He inversed the watermark data and embedded in image by taking different combination of LSB bits. This improves quality of image [19]. Sridevi *et.al.* (2010) presented paper on secure watermarking based on SVD and wavelets. In this paper, after applying DWT, SVD is applied to middle frequency band and embedded watermark data by modifying singular values and robustness is improved [20].

In 2010, Sathik *et. al.* [21] presented "An modified Invisible Watermarking method for Image Authentication". Here, a binary watermark structure is build up from host image itself then make it disordered depending on Arnold Transform. It provide imperceptibility, capacity and robustness. Watermark is robust against ordinary image processing attacks like additive noises, filtering, intensity adjustment, histogram equalization, JPEG compression, Scaling and rotation. Watermark extraction scheme is blind [21]. A.M. Kothari *et al.* (2010) analyzed performance of Combined DWT–DCT over individual DWT. In this paper we reviewed an imperceptible and a robust combined DWT-DCT digital image watermarking algorithm. Their combination enhance watermarking performance while comparing with the DWT-Only watermarking approach [22].

Ping Dong *et al.* IEEE (2005) presented "Digital Watermarking Robust to Geometric Distortions. In this two watermarking approaches are described that are robust to Geometric distortions. The initial approach is depend on image normalization, which is invariant against affine transform attack is public watermarking scheme and blind. The another approach is depended on watermark resynchronization scheme invariant against random nonlinear bending attacks is private watermarking scheme and non-blind. Numerical experiments verify that watermarking schemes are robust to a wider range of geometric attacks [23].

The reversible watermarking depended on the some prediction have been introduced, the lowest square predictor is being calculated in square block center for every pixcel.This all approach is there to permit the recovery of that same predictor at the time of detection in absence of any additional information..There are four prediction context of the local pridection depended watermarking are like the rhombus context and the unit of MED,GAP and SGAP precidtors. They are 12 × 12 (rhombus), 8 × 8 (MED), 10 × 10 (SGAP), 13 × 13 (GAP).There is a specific block dimensions is assign to all the contexts. The profit collection after their optimization is very less in figure.

The outcomes occur till now reflects that the local prediction based offer their global least square and a constant prediction based counterparts. From the prediction based approaches the rhombus based prediction scheme is consider to provide finest output. The result generated depending on local prediction with not similar expansion approaches with threshold control, histogram and flag bits.

CONCLUSION

In this paper we have obtainable various aspects for digital watermarking like introduction, outline, techniques and applications. Separately from it a brief and relative analysis of watermarking techniques is presented with heir advantages and disadvantages which can help the new researchers in these areas. We also tried to classify the digital watermarking in all the known aspects like robustness, perceptivity, purpose, watermark type, domain, and detection process. In this paper we tried to give the whole information about the digital watermarking which will help the new researchers to get the maximum awareness in this domain.

REFERENCES

[1]. Prabhishek Singh, R S Chadha, "A Survey of Digital watermarking Techniques, Applications and Attacks", *Proceedings of International Journal of Engineering and Innovative Technology (IJEIT),* March 2013 Volume **2**, Issue 9.

[2]. R.G. Schyndel, A. Tirkel, and C.F Osborne, "A Digital Watermark", *Proceedings of IEEE International conference on Image Processing, ICIP- 1994*, pp. 86-90

[3]. Christine I. Podilchuk, Edward J. Delp, "Digital watermarking: Algorithms and applications", Proceedings of IEEE Signal processing Magazine, July 2001.

[4]. Akhmet M.U. and Yilmaz E.," Hopfieldtype neural networks systems with piecewise constant argument" , August 2005, *Proceedings of the Conference on Differential and Difference Equations at the Florida Institute of Technology Melbourne*.

[5]. "Fast public-key watermarking of compressed video," in *Proc. IEEE Int. Conf. on Image Processing 1997 (ICIP '97)*, vol. **1**, Santa Barbara, CA, Oct. 1997, pp. 528–531.

[6]. I. J. Cox and J.P. Linnartz, "Some general methods for tampering with watermarks," *IEEE J. Selects .Areas Communication. (Special Issue on Copyright and Privacy Protection),* vol. **16**, pp.587–593, May 1998

[7]. "Watermark estimation through detector observations," in Proc. *IEEE Benelux Signal Processing Symposium '98, Leuven, Belgium, Mar. 1998.*

[8]. M. Kutter and F. Petitcolas, "A fair benchmark for image watermarking systems," in Proc. SPIE IS & T/SPIE's *11th Annu. Symp., Electronic Imaging '99: Security and Watermarking of Multimedia Contents,* vol. **3657**, Jan. 1999.

[9]. R. J. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE J. Select. Areas Communication . (Special Issue on Copyright and Privacy Protection),* vol. **16**, pp. 474–481, May 1998.

[10]. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT domain system for robust image watermarking," Signal Processing(Special Issue on Watermarking), vol. **66**, no. 3, pp.357–372, May 1998.

[11]. K. J. Giri, M. A. Peer, and P. Nagabhushan," A Channel Wise Color Image Watermarking Scheme Based on Discrete Wavelet Transformation," in *Proceeding of IEEE International Conference on Computing For Sustainable Global Environment transaction*, pp.758-762, 2014.

[12]. V. Khanduja, O.P. Verma, and S. Goel, "A Robust Multiple Watermarking Technique for Information Recovery, "in *IEEE International Advance Computing Conference (IACC)*, pp.250-255.

[13]. R. Eswaraiah and E. Sreenivasa Reddy," A Fragile ROI depended Medical Image Watermarking method With Tamper searching and Information Recovery,"CSNT'14 *Proceeding of fourth International Conference on Communication Systems and Network Technologies* pp. 896-899, 2014.

[14]. I. Joshi, Dr. V.N. Pawar (2014). "Secure Medical Image Watermarking", *International Journal of Research in Advent Technology*, vol. **2**, No. 42, pp. 266-271, April 2014.

[15]. G. Kaur, K. Kaur," Image watermarking Using LSB," *International Journal Of Advanced Research in Computer Science and Engineering*, vol.**3**, no. 4,pp.858-861April 2013.

[16]. R. E. Philip and Sumithra M.G, "Development Of A New Watermarking Algorithm For Telemedicine Applications," *IJERA*, vol. **3**, no. 1, pp. 962-968, 2013.

[17]. P. Ghosh, R. Ghosh, S. Sinha, U. Mukhopadhay, D. Kr. Kole and A. Chakroborty," A Novel Digital Watermarking Technique for Video Copyright Protection, "in CS & IT, pp.601-609, 2012.

[18]. M.T. Naseem, I.M. Qureshi, A.V. Raman, and M.Z Muzaffar (2012). "Robust Watermarking For Medical Images Resistant To Geometric Attacks," INMIC, ISSN: 978-4673.

[19]. A. Bamatraf, R. Ibrahim, and M.N. Salleh," A New Digital Watermarking Algorithm Using Combination OF LSB," *Journal Of Computing* Press, ISSN: 2151-9617, vol. **3**, no. 4, 2011.

[20]. T. Sridevi, Y. Ramadevi, and V. Vijaya Kumar, "Secure Watermarking based on SVD and Wavelets," *ICGST-GVIP Journal*, vol. **10**, no. 5 p. 63-69, Dec.2010.

[21]. Dr. M.M. Sathik and S.S. Sujatha, "An modified Invisible Watermarking method for Image Authentication, "in *International Journal of Advanced Science and Technology*, vol. **24**, pp.61- 77, November 2010.

[22]. A.M. Kothari, A.C. Suthar, and R.S. Gajre, "Performance observation of Digital Image Watermarking method–Combined DWT–DCT over separate DWT," printed on *International Journal of Advanced Engineering & Applications*, pp.177, Jan 2010.