International Journal of Information Movement *Vol.2 Issue IV* *(August 2017)*

Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 217-223**

A REVIEW ON DIGITAL WATERMARKING USING AES AND GENETIC METHODS

Rahul Mahendru
Research Scholar
Galaxy Global Group of Institutions, Ambala, Haryana, India E-mail: rahulmahendru4893@gmail.com

Er. Saranjeet Singh
Faculty
Galaxy Global Group of Institutions, Ambala, Haryana, India Email:- saranjeetsinghbabra@gmail.com

Abstract: The ubiquitous nature of digital network systems means that digital documents can be copied and distributed easily to large numbers of people with no cost. People can download audio, image and video files, and they can share them with friends and they can manipulate or modify their original contents. Watermarking is defined [1-2] as the action of hiding a message, text, logo or signature into an image, audio file, video or any or other work of media. These practices have existed for quite a long time, actually for several centuries. The field of digital watermarking is relatively young and gained popularity as a research topic in the latter half of the 1990s. Watermarking can be visible, such as the images are printed on money notes, or invisible, for which the watermark is hidden inside the media. Watermarking can be applied to physical objects, examples include: fabrics, garment labels, and product packaging that can be watermarked using special invisible dyes and inks, or as electronic signals. In the research, we will be implemented the DWT for segmentation of image, Genetic for optimization for segmented image and AES will be used for providing the security to watermarked image. The proposed method of watermarking will improve the performance, security and efficiency as compared to existing methods. The results will also be analyzed on the basis of performance parameters.

Keywords: Digital watermarking; DWT;AES; Genetic; Stego image ; RGB

1.0 Introduction:

Digital Watermarking incorporates means of securing the rights of the owner of the digital data, providing authentication of the source or originality of the digital data. The hidden message (watermark) signifies information that can be detected and retrieved by authorized personnel or systems designed for that purpose. Methods of Digital Watermarking can be applied to many types of content such as text, audio, images, video, 3D meshes, software programs and network packets. In Digital Image Watermarking (DIW), the robustness transparency trade-off depends on several aspects such as: a domain chosen to embed a watermark; a technique used to modulate the coefficients in that domain; a type of attack that might occur; a measure of transparency for the watermarked image. Several domains are traditionally used for DIW. Among them there are spatial as well as basis transform domains where each domain has its advantages under different types of attacks and transparency measures [3].

Some of the most popular modulation techniques are taken from the field of digital communication and are, in fact, methods of coding. Their robustness under Additive White Gaussian Noise is usually quite high, but the other types of attacks might be more harmful. Nowadays, a great variety of image processing tools can be applied to editing of watermarked images with the aim of their enhancing or compression. For an embedded watermark, this can be qualified as an attack which might be combined with intentional/unintentional noising (additive or multiplicative in nature). Definitions of transparency and quality for watermarked images are subjective in principle and may differ depending on the application. However, one out of a number of the known objective.

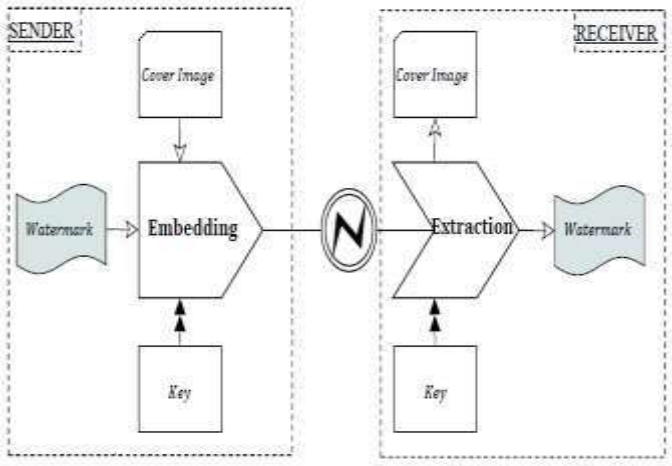

Figure 1.1: Digital Image Watermarking Scheme

2.0 Application Areas of Digital Watermarking

Watermarking techniques may be relevant in the following application areas [4]:

2.1 Copyright Protection

The primary use of watermarking is where an organization wishes to assert its ownership of copyright for digital objects. This application is of great interest to 'big media' organizations, and of some interest to other vendors of digital information, such as news and photo agencies. These applications require a minimal amount of information to be embedded, coupled with a high degree of resistance to signal modification (since they may be subjected to deliberate attack). For example, now a days, a news channel "AAJ-TAK" is showing the animal's clips (which are already shown on "Discovery" Channel) by hiding the Discovery channel's logo on the video clips. As per the law, The AAJ-TAK should show the curtsey-sign and should pay the copyright fee to the Discovery channel. In such cases, There is a strong need of watermarking as once the digital data is broadcasted, anybody else can start selling it without paying the IPR value to its owner [5].

2.2 Copy Protection

Watermarking can be used as a strong tool to prevent illegal copying. For example, if an audio CD has a watermark embedded into it, then any of the system (Hardware like DVD, or software) cannot make a copy of it, and even if it copies, the watermark data will not get copied to new duplicate audio CD. Now the duplicate CD can be easily found because it does not have watermark data.

Some schemes have attempted to satisfy more complex copy protection requirements. An early example is the Serial Copy Management System (SCMS),introduced in the 1980s, which enabled a user to make a single digital audio tape of are cording they had purchased but prevented the recording of further copies (i.e. second

generation) from that first copy. The scheme failed ultimately because not all manufacturers of consumer equipment were prepared to implement the scheme in their products [6].

2.3 Temper Detection

In this application area, it is necessary to assure that the origin of a data object is demonstrated and its integrity is proved. One example of temper detection is photo graphic forensic information which may be presented as evidence in the court. Given the ease with which digital images can be manipulated, there is a need to provide proof that an image has not been altered. Such a mechanism could be built into a digital camera [7].

For example, if a cop's camera catches an over speeding vehicle then when proving the driver guilty in front of the judge, the accused may claim that the video presented in the court is tempered and the car shown in the video does not belong to him. A watermarking system which is embedded in digital cameras may help to resolve the issue. If somebody tries to temper the data, the watermark will get destroyed indicating that the data is tempered. In our country, a well-known example is the "Tahalka-Scam".

2.4 Broadcast Monitoring

There are several types of organizations and individuals interested in monitoring the broadcast of their interest. For example, advertisers want to ensure that they receive the exact air time that they have purchased from broadcasting firms. Musicians and actors want to ensure that they receive accurate royalty payments for broadcasts of their performances and copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations. In 1997, a scandal broke out in Japan regarding television advertising. At least two stations had been routinely overbooking air time.

Advertisers were paying for thousands of commercials that were never aired [8].

The practice had remained largely undetected forever twenty years because there were no systems in place to monitor the actual broadcast of advertisements. This broadcast monitoring can be implemented by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broad casts and look for these watermarks identifying when and where each clip appears.

3.0 Digital Watermarking Technology for Authentication and Tamper Proofing

Another application of digital watermark [9, 10] is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/ Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a "sensor" to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications. The technical requirements for this application are as follows: Invisible to the ordinary users.

- Applicable to compressed image format (most digital cameras use JPEG compatible format).
- Sensitive to content manipulations, compression, and so on.

3.1 Importance of Digital Watermarking

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly with the introduction of Marc Andreessen's Mosaic web browser in November 1993, and it quickly became clear that people wanted to download pictures, music, and videos. The Internet is an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. When the only way the average customer could record a song or a movie was on analog tape, pirated copies were usually of a lower quality than the originals, and the quality of second-generation pirated copies (i.e., copies of a copy) was generally very poor. However, with digital recording devices, songs and movies can be recorded with little, if any, degradation in quality. Using these recording devices and using the Internet for distribution, would-be pirates can easily record and distribute copyright protected material without appropriate compensation being paid to the actual copyright owners. Thus, content owners are eagerly seeking technologies that promise to protect their rights. The first technology content owners turn to is cryptography. Cryptography is probably the most common method of protecting digital content. It is certainly one of the best developed as a science.

3.2 Previous work

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. **Radhika v. Totla et al. [11]** Digital watermarking is used very frequently. Hence, digital watermarking becomes very attractive research topic. Digital watermarking is a technology that creates and detects invisible markings, which can be used to trace the origin, authenticity, and legal usage of digital data. Ideally, they should be hard to notice, difficult to reproduce, and impossible to remove without destroying the medium they protect. **Shraddha S. Katariya et al.[7]**Digital watermarking technology is a frontier research field and it serves an important role in information security. According to the analysis of the definition and basic characteristics of digital watermarking technology, the system model of digital watermarking is given. The system consists of two modules which are watermark embedding module and watermark detection and extraction module. In view of the importance of digital images copyright protection, based on the analysis of the main digital watermarking algorithms, the digital watermarking technology can be applied to the image copyright protection. The two dimension discrete cosine transform is encoded on the Windows platform by using Visual C++ program language. The experiment result shows that the digital watermark is non-perceptible; the watermark information can be extracted even if it has been attacked, and the expected effect can be achieved.

V Santhi et al. [5] Due to the advancement in Computer technology and readily available tools, it is very easy for the unknown users to produce illegal copies of multimedia data which are floating across the Internet. In order to protect those multimedia data on the Internet many techniques are available including various encryption techniques, steganography techniques, watermarking techniques and information hiding techniques. Digital watermarking is a technique in which a piece of digital information is embedded into an image and extracted later for ownership verification. Secret digital data can be embedded either in spatial domain or in frequency domain of the cover data.

Christian Rey et al. [12] Digital image manipulation software is now readily available on personal computers. It is therefore very simple to tamper with any image and make it available to others. Insuring digital image integrity has therefore become a major issue.

3.3 Comparision of Recent Various Algorithms

Watermarking has become a popular technique for copyright enforcement and image authentication. The aim of this paper is to present an overview of emerging techniques for detecting whether image tampering has taken place. Compared to the techniques and protocols for security usually employed to perform this task, the majority of the proposed methods based on watermarking, place a particular emphasis on the notion of content authentication rather than strict integrity. In this paper, we introduce the notion of image content authentication and the features required to design an effective authentication scheme. We present some algorithms, and introduce frequently used key techniques(Fig. 2.1).

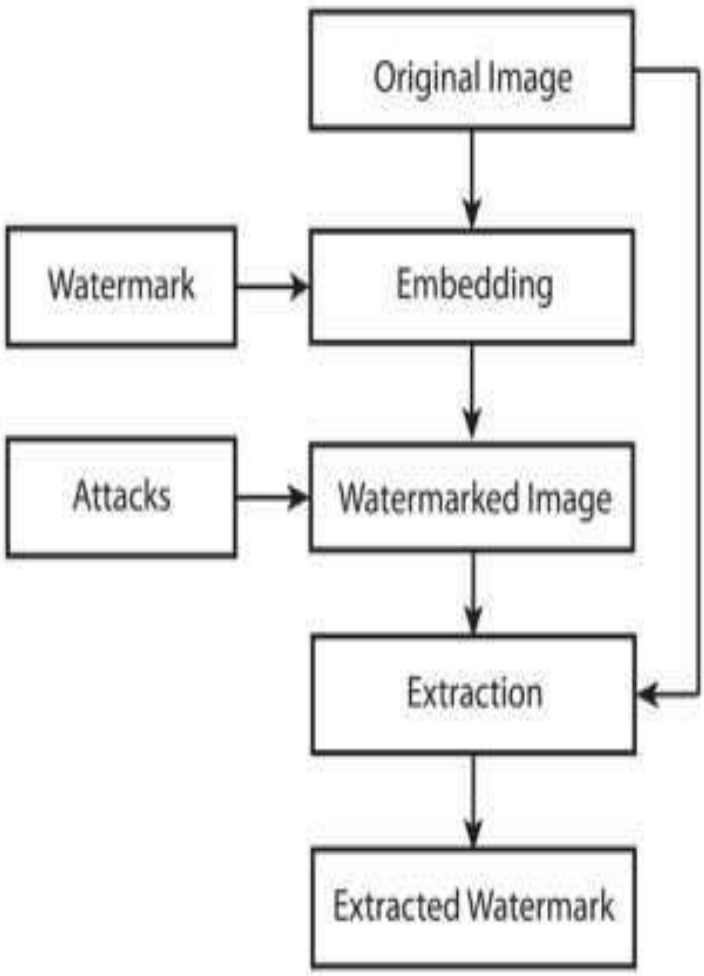

Fig2.1. Algorithm used for watermarking

The algorithm is based on combination method of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for embedding. The embedding watermarking technique employs one level of decomposition of

DWT coefficients at HL1 sub band. In the above technique, the error rate is about 1% for which we are going to use in our work to further decrease this error rate with Neural networks and AES.
In the method as shown in Fig 2.3, each part was required to be watermarked individually, but using Neural and AES scheme, **we** can decrease the computation time which was taken by the FFT and DFT method by using DWT scheme.

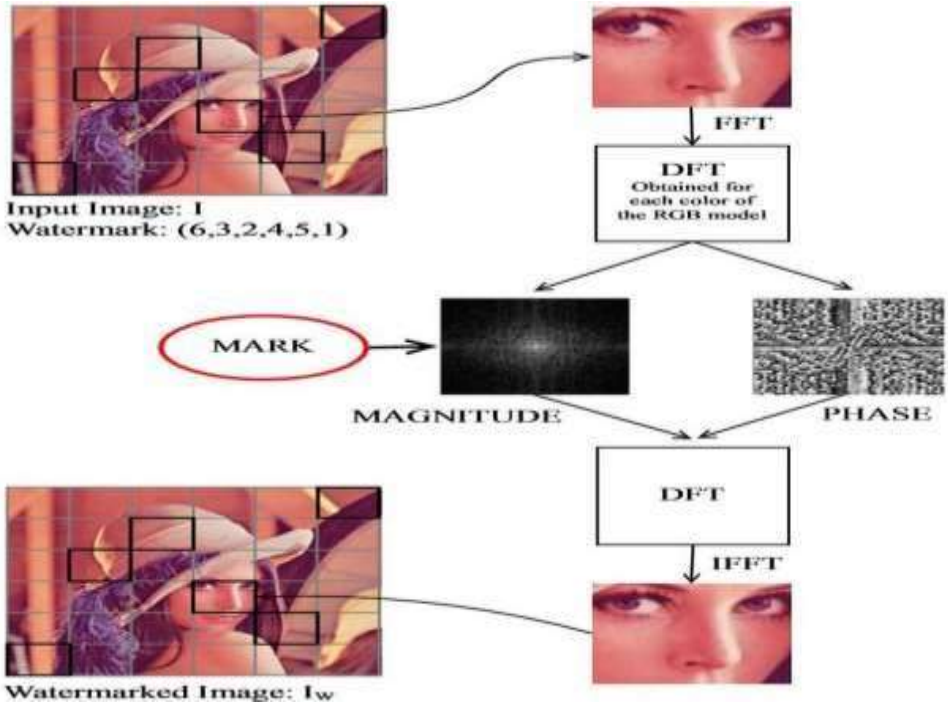

Fig2.3. Previous algorithm using FFT

4.0 Conclusion

Digital Image Watermarking can defend image from unsanctioned or unauthorized activities, various distortions, copyright etc. There are many techniques in data hiding. Digital Watermarking is more secure and easy method of data hiding. All techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency. In Watermarking we mark the information which is to be hiding. Security of data is essential today because of cyber-crime, which is highly increased day by day. In the review paper, the different aspects have been discussed of digital watermarking such as applications areas, importance and methods. The review paper have been elaborates the research problem formulation and objective for the research work. The detailed literature has also been presented in this review paper.

5.0 References

1. **[1]**Maninder Kaur and NirvairNeeru, " Digital Image Watermarking using New Combined Technique" in the International Journal of Computer Applications (0975 – 8887) Volume 145 – No.2, July 2016.
2. **[2]**SmitaPandey and Rohit Gupta, "A Comparative Analysis on Digital Watermarking with Techniques and Attacks" in the International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016.
3. **[3]**Zhu Yuefeng and Lin Li, "Digital Image Watermarking Algorithms Based on dual Transform Domain and Self-Recovery" International Journal on Smart Sensing and Intelligent Systems Vol. 8, No. 1, March 2015.

4. **[4]** SamiraLagzian, Mohsen Soryani and MahmoodFathy,"A New Robust Watermarking Scheme Based on RDWT–SVD", International Journal of Intelligent Information Processing, 2011, Vol. 2 (1).
5. **[4]**Sumedh P. Ingale 1 and Dr.C.A.Dhote, "A Survey Of Digital Watermarking Techniques" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 2 February 2015.
6. **[5]** V Santhi and Dr. ArunkumarThangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Spaces", International Journal of Computer Theory and Engineering, 2009, Volume 1 (4), pp: 424 - 429.
7. **[6]**ManjitThapa, Dr. Sandeep Kumar Sood and A.PMeenakshi Sharma, " Digital Image Watermarking Technique Based on Different Attacks" in the *International Journal of Advanced Computer Science and Applications, Vol. 2, No. 4, 2011.*
8. **[7]**Shraddha S. Katariya, "Digital Watermarking: Review" in the International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 2, February 2012.
9. **[8]**Prerna Singh, *"Robust Digital Color Image Watermarking in Hybrid Domain RDWT-DCT-SVD",* International Journal of Latest Technology in Engineering & Management (IJLTEM) ISSN: 2456-1770 Volume 1 Issue 1 ǁ June. 2016 ǁ PP 33-41
10. **[9]**DeeptiShukla and NirupamaTiwari, "Survey on Digital Watermarking Techniques" in the International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.9 (2015), pp.121-126.
11. **[10]**Prabhishek Singh and R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" in the International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.
12. **[11]**Radhika v. Totla and K.S.Bapat, "comparative analysis of Watermarking in Digital Images using DCT & DWT" International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.
13. **[12]**Christian Rey, Jean-Luc Dugelay, *"A Survey of Watermarking Algorithms for Image Authentication",* EURASIP Journal on Applied Signal Processing 2002:6, 613–621.