A Secure Image Watermarking Scheme Based on DWT, SVD and Arnold Transform

Lalan Kumar1 and Kamred Udham Singh1

1Graphic Era Hill University, Dehradun, India

E-mail: lalankumar100@gmail.com

Abstract. The rapid advancement and extensive growth in communication technology is creating a critical need to develop novel methods and techniques to protect copyright, ownership, authentication and content integrity of digital media. An efficient solution to this kind of problem is digital watermarking of multimedia. A watermark refers to a visible or invisible digital data to be embedded in a cover data so as to provide copyright protection at time when need arises. Numerous watermarking methods have been presented in the literature and several watermarking software packages have been developed in past decades. Still robustness and security of watermark against a variety of attacks is one of the most important issues to be solved. In this paper, techniques are presented for watermarking of 8-bit images. The watermark is subjected to Arnold Transform to introduce randomness, thus enhancing security and improving PSNR. Embedding is done in low frequency LL band of original image. Inverse Discrete wavelet Transform is then computed to obtain the watermarked image. The results are evaluated by applying number of attacks on the watermarked image. The experimental results show that the proposed watermarking technique is robust and efficient.

1. Introduction

Rapid development of computer hardware and software, the reproduction of digital images, video, audio or any other form of multimedia material is becoming increasingly simple and quick. It could be possible to make and transmit illicit copies of digital files to unauthorized beneficiaries. In certain cases, the effects of such behaviours are dangerous. For the film industry, this has a strong effect on sales reductions with the sponsorship of video and audio piracy. This leads to unauthorized copying of photographs in the case of copyrighted images, and also to future authorisation claims. Because of all these considerations, protection of digital information is a vital concern and must be taken into account with respect to all dimensions, including application requirement, form of digital media to be covered, security level to be inculcated and much more [1]. Watermark refers to digital content (usually compact), which is to be inserted in the host data (digital media) to subsequently provide evidence of ownership of the digital data. The watermark should include the name of the author, entity or other information so that the original author or owner of the information can assert possession of such information at the time of the need. Digital Image watermarking involves inserting digital data in the cover picture and later presenting proofs that the information is owned. Almost all copyright enforcement watermarking strategies need to be robust [2]. This refers to the watermark property since it is difficult to distinguish from the host image. Therefore, it is difficult or almost impossible for robust watermarking to isolate digital watermark data from host data, or to distort the watermark by a wide range of manipulations of host data, commonly known as attacks. The watermarking of digital images makes it possible for the embedded watermark not to jeopardize the image quality. The originality of the picture must also be retained. This can be expressed mathematically by saying that the watermark picture requires a high
PSNR value. This is later seen in this paper that robustness criteria and PSNR values give these two quantities a balance.

There are four main factors that make watermarking effective. The following are:

**Robust:** it should be impossible to erase or destroy the watermark. Robust image watermarking image is an indicator of the watermark's power against image processing operations such as scaling, rotating, conversion, cutting etc.

**Imperceptibility:** This means that there cannot be a better identification of the existence of the watermark. In the case of photographs this means that the background cannot be separated from the original image.

**Capacity:** Watermark capacity refers to the amount of digital content that can be integrated into the host image.

Multimedia content (picture, audio and video) copied and stored and easily damage to protect its originality on the content this internet world. That is why, proper use of any property rights protection system. Copies of the name of conservation of digital rights management (DRM time) transmission content is recorded in the incident and the mail it is also stored along with the incident can be written. This is the first time for the game in the content and then decrypted sports. This was the main problem DRM system, decrypted once it is easy to be false and distribution among others [1]. For these evictions was SNR and DRM we another protection system is known as a digital watermarking. Hiding the information science, its Steganography and digital watermarking a hiding the information science. This system of Steganography resources is kept in a secret information or then embed the content so that it does not cover. When one copy Steganography content then secret information and others to be false [2]. Digital watermarking on the proposed a solution to the preservation of copyright licensing multimedia information. This is more than in the digital process as there was no sign of overhead flights [3]. Compare the system of hiding the information can go to the three aspects that means the power, the security and robustness. We have the capacity to reveal the amount of information, the security of the power to anyone on secret information detection and robustness has said that, to prevent the content of cover before reform there is a secret information. There is a Watermarking Steganography differentiated based on the capacity of the security and robustness. Steganography system high security and ability, i.e., secret information is generally deteriorating were destroyed and even a trivial of reform. Watermarking system that means it is impossible to be like robustness watermark removed the severe quality deterioration of the subject of cover [4][5][6].

**1.1 Motivation**
As described above, the robustness of any automated watermarking technique is one of the key concerns. This applies to the consistency of the watermark which is not compromised by any attack to erase it. For certain multimedia files that are freely available over the internet or otherwise, other forms of watermarking are used, known as fragile watermarking. This is contrary to the rigorous watermarking since the watermark is tempered by some slight change in the watermark picture. Such watermarking is used for the avoidance of originality and protection of copyright as confirmation of possession of the digital text. The emphasis of this paper is on rigorous watermarking of the color image, so that no opponent can assert ownership by tempering the watermark in any way. The primary objective of the study is to establish strategies for effective and stable watermarking of color images in order to avoid watermarking from being tempered by attacks such as shifts in intensity and the pixels.

**2. Literature Survey**
This section survey literature, various research papers after reading and also some consideration for collecting information from the internet is the best knowledge of us we writing this literature survey, the first section watermarking digital the explanation and in the second part of history of watermark
embedding digital explanation and drainage system. The third and fourth section explains the digital watermarking and watermarking terminology respectively in the fifth section explains the consciousness of the digital watermark embedding and extraction algorithm. Last section closing section.

2.1. Digital Watermarking History

Ancient water mark paper is available archives before 1292 Fabriano Italy, [7] joined this marks the thin wire scattered the paper molds. Paper will be a little bit where screen had become thinner string was and so more transparent. At the end of the 13th century of 40 paper mills sharing the Fabriano paper in the market and another format paper, the standard of production and the price [8]. Every Digitization media, in today's world has been expanded and watermarking digital approaches to be assumed that-Chun twenty years demanded the ownership and protection of both countries preference to open sourcing over proprietary. Digital Watermarking became famous only 1990-1990, this idea digital watermarking. Due to the growth of the internet. Internet was a big because propelling growth of illegal copyrighted materials to be distributed is very simple. File sharing technology big and company of users to share such as the music and other copyrighted elements such as a video. This cost to the entertainment industry is not crores of million dollars lost revenue. It was a primary because watermarking digital development. The first publication in 1993 when Tickle and others to hide information presented by 1993 skill image [9] this system-based modernization less important bit (LSB), the pixel values. From the global research activities are increasing the digital watermarking [9]. This is the best way of watermarks was known to minus any possibility of confusion. This digitization in today's world has been expanded and watermarking digital approaches to be assumed that-Chun twenty years of both countries and demanded the ownership preference to open sourcing over proprietary interest reservation [10]. The Chinese Ambassador in Kenya, Chang [11] differentiated watermarking and among the other three important aspects of digital technology is the first: We are moving forward, unlike watermark imperceptible the image that there will be no detracting. Aesthetic value, secondly, these watermarks and they are embedded in the work, indifferent. Even if the work or any other file into media, watermarks not out of this different other technology. Last is trying to watermark transformation experience that means that you are working as information, transformation in the forest the watermarks [12].

2.2. Digital Watermark Embedding and Extraction

Digital watermarking framework in two phases. In the first stage watermark is embedded in the image of the host embedding text, audio and video, the identity of the creator of the image and in the second stage is to return to watermark water mark extracted from the image proof of identity of creator. The digital watermarking system in the basic modules shown as two figure 1.

![Figure 1. Watermark Embedding Module](image)

Figure 1 said watermark embedding module which is responsible for this kind of information without adding, such as numeric, text picture. Sometimes the main would not show diagram due to excessive security. Watermark detection and extraction: modules-Watermark detection and extraction modules to use this information in certain watermark or watermark can be. The basic modules watermark initiatives are secret information. Daily output module is a watermark the value of any kind of self-ability. This watermark detection and extraction modules number shown as in figure 2 [13].
2.3. Digital watermarking various applications

For adding watermark pixel evaluation of the picture is just a little and throughout the whole again and again. Watermark for adding music millisecond windows, which is an opportunity for the ear deaf, apart from the mind is primarily or audio watermark can be, other words the echoes of death.

Digital Watermarks people, there are many useful summarized under the as:
- The identity of the owner of - such copyright protection of the content of the ownership [14][15]
- Copies of conservation - one copy of the people to the control of illegal copy copyrighted content [16][17]
- Content, there are various benefits like authentication - the subject of various reforms to detect cancer in men, or as a sign to Bangladesh, there are various benefits like authentication [18]
- As a Fingerprinting - never mentioned about transactions or traitor tracking for a few months after the illegal and content [19]
- Broadcast monitoring - mainly the advertising and entertainment industry is being broadcast on the content of monitoring and legal source [20][21]
- Medical applications - invertible watermarking is known, there are various benefits like authentication and privacy policy of the two is not created in this way to the medical picture [22][23]

3. Design and Framework

This section we discussed Simulation Methods tool attack proposal analysis. Almost 82 sections of watermarking algorithm domain where it is assumed that transform domain watermark detection and explain about the insertion watermarking algorithms DCT and the DWT is used.

3.1. Proposed Watermark Embedding Algorithm

**Step 1** Input host image size 512 X 512 and watermark size of 64 X 64.

**Step 2.** Applied single level DWT on host image (LL, HL, LH and HH bands)

**Step 3** Arnold transform is applied to the watermark and them encryption key is set, and watermark is converted into a sequence. Further, element of this sequence is transformed into a bit stream of 8-bit binary numbers.

**Step 4** Applied SVD on LL band of the image.

**Step 5** Watermark components are embedded into D component of the LL band. Watermark insertion is done in the host image as below:

\[ p' = x + \alpha q \]

where \( p' \) is the transformed component of the watermark image.

\( q \) is the watermark component.

\( p \) is the transformed image of the host image

\( \alpha \) is the embedding strength.
Step 6 Perform Inverse SVD to reconstruct the component.
Step 7 Perform Inverse Discrete Wavelet Transformation to construct the final watermarked image.

3.2. Watermark Embedding Implementation of Proposal Algorithm
MATLAB platform has been used the implementation of the algorithm. Test pictures are shown table 1. This experimental set, we were taken to the test, picture shown in the table 2. Image name baboon, Barb, boat, daughter, Lena and houses. Table 1, in the first column a test image watermark in the second columns of the insertion test there is a picture of the third is a picture of the proposal to the effective watermark embedding algorithm [24][25].

Table 1. Showing the Host Image, Watermark Image and Watermarked Image

| Test image | Watermark | Watermarked image |
|------------|-----------|------------------|
| Baboon     | ![Baboon Watermark](image1.png) | ![Baboon Watermarked](image2.png) |
| Barb       | ![Barb Watermark](image3.png) | ![Barb Watermarked](image4.png) |
| Boat       | ![Boat Watermark](image5.png) | ![Boat Watermarked](image6.png) |
| Daughter   | ![Daughter Watermark](image7.png) | ![Daughter Watermarked](image8.png) |
3.3 Proposed Watermark Extraction Algorithm

Image of baboon, Barb, boat, daughter, Lena use for the experimental purpose and extracted has been shown in the house. In the first column table 2 overs, the main watermark image watermark image of the second column, there is a proposal to the watermark embedding algorithm, watermarking column third extracted watermark picture is found that the proposal for execution watermark extraction algorithm.

**Step 1**  Input original and watermarked image.

**Step 2**  Perform single level DWT on watermarked image and the original image.

**Step 3**  Apply SVD on LL band.

**Step 4**  Extract the watermark from the watermarked image using original image by reverse performing the embedding steps.

**Step 5**  Perform inverse Arnold transform with the decryption key on extracted components to generate the original watermark.

**Table 2.** Overs by Showing the Real, Water Mark Image and Extracted Watermark on the Proposed the Extraction Algorithm
4. Results and Discussion
SNR and PSNR values of the proposed scheme tested on images viz. baboon, Barb, boat, daughter, Lena and house. PSNR and SNR values of the watermarked images and extracted watermark, shown in table 3 and graphically represented in figure 3, 4 and 5.

Table 3. PSNR and SNR Values of the Watermarked Images and Extracted Watermark

| Image   | SNR (watermarked image) | PSNR (watermarked image) | SNR (extracted watermark) | PSNR (extracted watermark) |
|---------|-------------------------|--------------------------|---------------------------|----------------------------|
| Baboon  | 43.75                   | 48.32                    | 37.30                     | 37.78                      |
| Image       | Barb         | Boat        | Her Daughter | Lena         | Home        |
|-------------|--------------|-------------|--------------|--------------|-------------|
|             | 41.50 47.88 38.23 38.72 | 44.43 48.61 36.69 37.18 | 39.15 45.62 40.11 40.59 | 43.44 48.81 37.48 37.97 | 41.02 46.85 37.64 38.13 |
SNR values of the watermarked image in figure 5 and 6 lies between 39 to 45 whereas SNR values of the extracted watermark image is lies between the 36 to 40. And PSNR values of the watermarked image in depicted in figure 4 lies between 47 to 49 whereas SNR values of the extracted watermark image is lies between the 37 to 39 which shows that the result of proposed scheme is good.

**Figure 3.** PSNR Values of the Watermarked Image and Extracted Watermark

**Figure 4.** SNR Values of the Watermarked Image
Table 4 depicted the comparison of the proposed watermarking scheme with the existing scheme [1][2][3][4][5] and found that the PSNR value of the scheme is better than the existing scheme and graphically shown in figure 6.

**Table 4. PSNR Comparison of Different Watermarking Schemes**

| Scheme          | PSNR  |
|-----------------|-------|
| Proposed Scheme | 48.81 |
| Ref. [1]        | 44.36 |
| Ref. [2]        | 37.84 |
| Ref. [3]        | 46.66 |
| Ref. [4]        | 33.3870 |
| Ref. [5]        | 41.3784 |
5. Conclusion

A robust non-blind watermarking approach is proposed, watermark insertion and extraction have done successfully. The PSNR and SNR of watermarked image as well as extracted watermark are extremely considerable. In the proposed scheme, encrypted watermark (with the help of Arnold Transform) is inserted in D component of the LL sub-band of the host image which provides much robustness to scheme. The developed scheme makes efficient use of the low frequency components of the Discrete Wavelet Transform Image for watermark embedding. After the comparison analysis of the it observed that the PSNR of the proposed scheme is better than the existing schemes.

6. References

[1]. Ko, Lu-Ting, et al. "Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems." *Computational and mathematical methods in medicine* 2012 (2012).

[2]. Miyazaki, A. "An improved correlation-based watermarking method for images using a nonlinear programming algorithm." NSIP 2005. Abstracts. *IEEE-Eurasip Nonlinear Signal and Image Processing*, 2005. IEEE, 2005.

[3]. Giakoumaki A, Pavlopoulos S, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. *Medical & Biological Engineering & Computing* 44(8):619–631.

[4]. Al-qdah M (2018) Secure watermarking technique for medical images with visual evaluation. *Signal & Image Processing: An International Journal (SIPJ)* 9(1):1–9.

[5]. Jung K, Yoo K (2009) Data hiding method using image interpolation. *Comput Stand Interfaces* 31:465–447.

[6]. Mr. Pankaj Dadheech, Dr. Dinesh Goyal, Dr. Sumit Srivastava, Mr. Ankit Kumar, (2018), “A Scalable Data Processing Using Hadoop & MapReduce for Big Data”, *Journal of Advanced Research in Dynamical & Control Systems*, Vol. 10, 02-Special Issue, 2018, pp-2099-2109, ISSN: 1943-023X.
[7]. Vengatesan, K. et al. "Analysis of Mirai Botnet Malware Issues and Its Prediction Methods in Internet of Things". Lecture Notes on Data Engineering and Communications Technologies 31. (2020): 120-126.

[8]. Vimal, V. et al. "Artificial intelligence-based novel scheme for location area planning in cellular networks". Computational Intelligence. (2020).

[9]. Kumar, A. et al. "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm". Microprocessors and Microsystems. (2020).

[10]. Vengatesan, K. et al. "Credit card fraud detection using data analytic techniques". Advances in Mathematics: Scientific Journal 9. 3(2020): 1185-1196.

[11]. Kumar, V.D.A. et al. "Exploration of an innovative geometric parameter based on performance enhancement for footprint recognition". Journal of Intelligent and Fuzzy Systems 38. 2(2020): 2181-2196.

[12]. Pankaj Dadheech, Dinesh Goyal, Sumit Srivastava & C. M. Choudhary, (2018), “An Efficient Approach for Big Data Processing Using Spatial Boolean Queries”, Journal of Statistics and Management Systems (JSMS), 21:4, 583-591.

[13]. Vengatesan, K. et al. "Secure Data Transmission Through Steganography with Blowfish Algorithm". Lecture Notes on Data Engineering and Communications Technologies 35. (2020): 568-575.

[14]. Vengatesan, K. et al. "Simple Task Implementation of Swarm Robotics in Underwater". Lecture Notes on Data Engineering and Communications Technologies 35. (2020): 1138-1145.

[15]. Mallikalavala, V. et al. "Theft vehicle detection using image processing integrated digital signature-based ECU". Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020. (2020): 913-918.

[16]. Kesavan, S. et al. "An investigation on adaptive HTTP media streaming Quality-of-Experience (QoE) and agility using cloud media services". International Journal of Computers and Applications. (2019).

[17]. Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja & Ramesh C. Poonia (2019), “An Enhanced Quantum Key Distribution Protocol for Security Authentication”, Journal of Discrete Mathematical Sciences and Cryptography, 22:4, 499-507, DOI: 10.1080/09720529.2019.1637154.

[18]. Ankit Kumar, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia & Linesh Raja (2019), “An Improved Quantum Key Distribution Protocol for Verification”, Journal of Discrete Mathematical Sciences and Cryptography, 22:4, 491-498, DOI: 10.1080/09720529.2019.1637153.

[19]. Ankit Kumar, Linesh Raja, Pankaj Dadheech, Manish Bhardwaj (2020), “A Hybrid Cluster Technique for Improving the Efficiency of Colour Image Segmentation”, World Review of Entrepreneurship, Management and Sustainable Development, Nov. 2020, Vol. 16, Issue 6, pp. 665-679, Print ISSN: 1746-0573 Online ISSN: 1746-0581, https://doi.org/10.1504/WREMSD.2020.111405.

[20]. A. Kumar, P. Dadheech and U. Chaudhary, (2020), "Energy Conservation in WSN: A Review of Current Techniques," 2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), Jaipur, India, 2020, pp. 1-8, ISSN: 978-1-7281-1683-9, doi: 10.1109/ICETCE48199.2020.9091736.

[21]. Kumar, A. et al. "Teaching literacy through animation & multimedia". International Journal of Innovative Technology and Exploring Engineering 8. 5(2019): 73-76.

[22]. Kumar, A. et al. "3D Lighting Courseware development for 3D Motion Picture Science". 2018 International Conference on Recent Innovations in Electrical, Electronics and Communication Engineering, ICRIEECE 2018. (2018): 2621-2623.

[23]. Kumar, A. et al. "Study and Research of 3D Animation Courseware Development". 2018 International Conference on Recent Innovations in Electrical, Electronics and Communication Engineering, ICRIEECE 2018. (2018): 2514-2516.

[24]. Preetha, J. et al. "Data mining technique based critical disease prediction in medical field". Advances in Parallel Computing 37. (2020): 104-108.
[25]. Kumar, A. et al. "Comparative Analysis of Data Mining Techniques to Predict Heart Disease for Diabetic Patients". *Communications in Computer and Information Science* 1244 CCIS. (2020): 507-518.