International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July-2018 www.irjet.net p-ISSN: 2395-0072

Analysis of Various Watermarking Schemes

Geetanjali Gupta[1], Varun Jasuja[2], Dr. Rajesh Kumar Singh[3]

[1] Department of Computer Science and Engg. GNIT, Mullana (Haryana), India.
[2] Asst. Professor, Department of Computer Science and Engg. GNIT, Mullana (Haryana), India
[3] Professor, SUS institute of computer, Tangori, Punjab.

Abstract- *The watermarking is the approach which can generate the secure image data. To watermarking schemes are broadly classified into blind and semi-blind schemes. To generate efficient watermark image various techniques has been proposed by the authors. The common watermarking schemes are DCT, DWT and SVD. In this paper, various watermarking schemes are reviewed and analyzed in terms of certain parameters. It is analyzed that wavelet transformation techniques are most efficient techniques for the generation of watermarking schemes.*

Key Words: DCT, DWT, SVD, Watermarking, Blind Watermarking, Texture Features.

1. INTRODUCTION

Digital watermarking is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media. Over recent years, there has been tremendous effort in order to understand and model the Human Visual System and applying it to different image processing applications. Such effort has been examined for solving various problems and has resulted in different levels of success. Recently, visual models have been developed as a result of the efforts taken place in the field of image and video compression, which desire to improve the quality of the compression exploiting HVS characteristics [1]. Basically, both image watermarking and image compression are concerned of the image redundancy, which is to be reduced in the case of compression, while is employed to insert the mark in the case of watermarking. As a result, visual models devised in the area of image compression can also be suited to the watermarking problem. Watermark insertion process exploits the weakness of human visual system properties to make the watermark imperceptible with maximal strength. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal. The needed properties of a digital watermark depend on the use case in which it is applied [2]. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganography techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data. One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution [3]. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

1.1 Types of Watermarking: Following are the broader categorizations of watermarking:

a. Video watermarking: Video watermarking can be considered as a superset of normal image watermarking. As such, all the techniques applicable to static images can be applied to video images [4]. However, due to the high frame rate of video, the embedding process must occur almost in real time for live transmissions (it takes a finite time to embed the watermark, which might influence the transmission rate). If the content is generated off-line, this limitation does not exist. A very popular form of on-line (live) video watermarking is the usage of a visible watermark (normally a logo or other distinguishing sign placed in an unobtrusive place on each frame of video.

b. Audio watermarking: Audio watermarking is currently at the forefront of technology development in an attempt to prevent illegal reproduction and redistribution. One implementation receiving widespread attention is the MP3 approach to audio compression and watermarking [5]. Audio watermarking can be successfully implemented at frequencies outside the normal human audible range. (This is also the approach followed by compression schemes, in which frequencies outside the human audible range are removed from the original audio soundtrack.

c. Text watermarking: Text can be subdivided into two categories: raw unformatted ASCII text and formatted text (typically Postscript, PDF or RTF formats). Watermark information can be embedded into a formatted document using an approach based on the slight adjustment of inter-line and inter-word spacing's. Another approach to watermark embedding is to consider the typeset text as one large image and thus to use the typical approaches used for images. One possible approach is based on adding white space characters after each sentence (and is thus hidden to the casual observer). However, this approach is easily bypassed using a normal text editor [6].

1.2 Algorithms for Watermarking:

a. Singular Value Decomposition (SVD): Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians. SVD has many practical and theoretical values; special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix A with m rows and n columns, with rank r and $r \leq n \leq m$. Then the A can be factorized into three matrices:

$$A = USV^T$$

The SVD is the optimal matrix decomposition in a least square sense that it packs the maximum signal energy into as few coefficients as possible. Singular value decomposition (SVD) is a stable and effective method to split the system into a set of linearly independent components, each of them bearing own energy contribution.

b. DWT in Image Processing: The discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length [7]. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale. DWT is computed with a cascade of filtering followed by a factor 2 sub sampling. The Discrete Wavelet Transform (DWT) is used in a wide variety of signal processing applications. 2-D discrete wavelet transform (DWT) decomposes an image or a video frame into sub-images, 3 details and 1 approximation. The approximation sub-image resembles the original on 1/4 the scale of the original.

1.3 Artificial Neural Networks

A neural network is defined as "...a computing system made up of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs." The idea of ANNs is based on the belief that working of human brain by making the right connections can be imitated using silicon and wires as living neurons and dendrites [8].

The human brain is composed of 100 billion nerve cells called neurons. They are connected to other thousand cells by Axons. Stimuli from external environment or inputs from sensory organs are accepted by dendrites. These inputs create electric impulses, which quickly travel through the neural network. A neuron can then send the message to other neuron to handle the issue or does not send it forward.

ANNs are composed of multiple nodes, which imitate biological neurons of human brain. The neurons are connected by links and they interact with each other. The nodes can take input data and perform simple operations on the data [9]. The result of these operations is passed to other neurons. The output at each node is called its activation or node value. Each link is associated with weight. ANNs are capable of learning, which takes place by altering weight values.

2. LITERATURE REVIEW

Yudit Arum Mekarsari, et.al (2018) presented in order to secure digital images watermarking techniques has been utilized which has various major challenges. They discussed how the effect of distortion and imperceptibility on watermark insertion can be minimized by optimizing the trade-off between robustness watermarked images [10]. They proposed a method for water mark insertion so that copyright in true color (RGB) images can be protected this can be possible by combining Discrete Wavelet Transform and Singular Value Decomposition algorithms. In this process, the DWT process is done up to 2 levels after which selected sub-band LL2 are utilized to insert watermark for which Singular Value Decomposition method has been utilized. Gaussian noise, salt & pepper noise, crop, blur and rotate are some attacks that break the toughness of watermarked image. Proposed method provides the PSNR and SSIM values which have values above 40 dB for PSNR and above 0.99 for SSIM. 1 is the average value of NC obtained from this result.

M. Islam, et.al (2017) proposed a robust image watermarking technique in this paper, which is the combination of discrete wavelet transform and discrete cosine transform. For the correction of geometric distortion, they included the SVM regression model so that improved robustness against de-synchronization attacks such as rotation, translation etc can be achieved easily. In the SVM regression model, they utilize the Low order

Pseudo Zernike moments as the feature vector. In order to insert a binary bit, they modified the 3-level DWT transformed DCT coefficients in this paper [11]. For both intentional and non-intentional attacks, they measured the performance of algorithm. An average imperceptibility of around 42.45 dB is provided by the proposed approach. With the help of trained SVM regression model, the effect of rotation and translation attack has been measured. After done changes in attacked watermarked images, they performed the robustness against desynchronization attack. On the basis of the done experiments, it is concluded that optimal robustness both for geometric and non-geometric attacks are provided by the proposed algorithm.

Olivia Zacharia, et.al (2017) presented it is required to propose new reliable and robust techniques so that digital data can be secured in this digital worlds which is easily available and accessed by anyone nowadays. The applications of watermarks have been utilized at the greater extent in order to protect the digital images. In the past decades, large number of watermarking techniques has been developed which provide useful results by providing security to digital data. They presented the comparison between two different digital image watermarking algorithms in this paper. In which one is based on Haar DWT and bit-plane slicing and the other is a histogram shape based method where embedded security key was utilized to done watermarking. On the basis of the performed experiments and simulation results they compared the two methods using Xilinx ISE Design Suite [12]. On the basis of Peak Signal to Noise Ratio and Mean Signal Error values the comparison was made for the images.

Issam Dagher, et.al (2017) presented for the extraction of the watermark image, they proposed a method of blind algorithm in this paper. This proposed algorithm is powerful for grayscale images as it minimizes the noise and geometric attacks [13]. Within its neighboring pixels, this region is moved horizontally and vertically. In the matrix, each move must be registered as a correlation value of this region with the initial sequence. For all the feature points this procedure is repeated continuously until all the watermarked regions are not identified. In the watermarked images the center is determined by the obtained maximum correlation. Compared the proposed method with other methods and concluded that proposed method is vigorous against a wide variety of tests.

Shachi Natu, et.al (2017) proposed two methods of color image watermarking in this paper in which SVD and DCT Walsh hybrid transform has been utilized by both techniques. On the column hybrid transformed host SVD is utilized by the first method also on watermark images. On sorted column hybrid transform coefficients of host and watermark images SVD has been utilized by the second method [14]. In the traditional method middle frequency coefficients was utilized in contrast to both methods in which low frequency transform coefficients are used. In order to embed watermark in host, 30 singular values of watermark is required in the first method. But in case of second method this value is reduced to 3 values. Due to transformation of coefficients prior to SVD as there is enhancement in the high energy compaction property of SVD. On the basis of compression, noise addition, resizing, cropping, and histogram equalization performance of both the methods are compared to each other.

Hansa Mehra, et.al (2017) presented due to the presence of large amount of data over the internet, it becomes difficult to secure data. The security to the digital data is provided by the watermarking technology. It is the process in which the original image is embedded with the water marked image so that a new image can be obtained after which watermark from the obtained image is extracted [15]. They proposed a frequency domain watermarking process in this paper which is based on the discrete cosine transform in which different sizes of original and watermark images are presented. They also presented the noise effects on the selected test images and also compared different test images using the PSNR values. The obtained results also provide the correlation between both watermark & watermarked image.

Monika Dahiya, et.al (2017) presented the security of the image can be enhanced by the proposed method in which one images is concealed with another image. This method utilizes the Fourier transform with random phase masks so that the secret images cannot be detected easily. The reliability of the image is enhanced using the scrambling [16]. The obtained results are further improved using the computer simulations. They also assessed the effects of occlusion on the peak Signal to noise ratio in this paper. They considered the Correlation coefficients, Standard Deviation error and mean error values as the proposed scheme has been subjected to various attacks for steganalysis.

Nazir A. Loan, et.al (2017) presented a digital image watermarking technique in this paper which is based on a chaotic encryption can be applicable to both grayscale and color images. Before embedding the watermark in the host image, Discrete Cosine Transform has been utilized [17]. In this paper, they tested and analyzed the three different variants of the proposed algorithm. as per done simulation

results, it is concluded that proposed method is robust to most of the image processing operations like JPEG compression, sharpening, cropping, median filtering, and many more. They compared the obtained simulation results with other methods in order to validate the efficiency of the proposed technique. The proposed method has better performance as compared to other methods illustrated by the results in terms of robustness, security and imperceptivity.

Dimple Bansal, et.al (2017) presented due to invent in the technology there is large transformation of data or information using digital technology which becomes a fast process. Security is the major concern while transmitting information through digital techniques. Hence, this issue can be overcome by the digital watermarking technology which prevent the unauthorized access and provide the copyright protection to the digitize data also differ information against illegal misuses and allocation [18]. It is necessary that digital watermarking method is powerful so that defected part can be easily recovered. Hence, for embedding the watermark, red color component of the image has been utilized in order to apply DWT technique. They implemented the 8X8 block of the image with the help of DCT which help in forming a secure and powerful image at the end.

Nasir N. Hurrah1, et.al (2017) presented on the basis of hybrid transform domain an efficient and effective watermarking scheme has been proposed in this paper. This scheme is powerful, blind and provides security. With the help of this scheme dual attacks can be endured which is the combination of the signal processing and geometric attacks. In order to increase the security of the watermark, they implemented the multiple encryption techniques in this paper [19]. On the basis of the done experiments, it is concluded that proposed method is more powerful and optimal to all types of signal processing and geometric attacks such as rotation, cropping and resizing as compared to other methods. The strength of the proposed method for dual attacks is proved by the simultaneous attacks on the watermarked images which are hindered by this method. The performance of the proposed method is measured in term of parameters such as PSNR, NCC, BER and BCE.

3. TABLE OF COMPARISON

Author's Name	Year	Description	Outcomes
Yudit Arum Mekarsari,	2018	They proposed a method for water mark insertion so that copyright in true color (RGB) images can be protected this can be possible by combining Discrete Wavelet Transform and Singular Value Decomposition algorithms.	Proposed method provides the PSNR and SSIM values which have values above 40 dB for PSNR and above 0.99 for SSIM. 1 is the average value of NC obtained from this result.
M. Islam,	2017	They proposed a robust image watermarking technique in this paper, which is the combination of discrete wavelet transform and discrete cosine transform.	On the basis of the done experiments, it is concluded that optimal robustness both for geometric and non-geometric attacks are provided by the proposed algorithm.
Olivia Zacharia,	2017	They presented the comparison between two different digital image watermarking algorithms in this paper. In which one is based on Haar DWT and bit-plane slicing and the other is a histogram shape based method where embedded security key was utilized to done watermarking.	On the basis of the performed experiments and simulation results they compared the two methods using Xilinx ISE Design Suite. On the basis of Peak Signal to Noise Ratio and Mean Signal Error values the comparison was made for the images.
Issam Dagher,	2017	For the extraction of the watermark image, they proposed a method of blind algorithm in this paper. This proposed algorithm is powerful for grayscale	Compared the proposed method with other methods and concluded that proposed method is vigorous against a

		images as it minimizes the noise and geometric attacks	wide variety of tests.
Shachi Natu,	2017	They proposed two methods of color image watermarking in this paper in which SVD and DCT Walsh hybrid transform has been utilized by both techniques.	On the basis of compression, noise addition, resizing, cropping, and histogram equalization performance of both the methods are compared to each other.
Hansa Mehra,	2017	They proposed a frequency domain watermarking process in this paper which is based on the discrete cosine transform in which different sizes of original and watermark images are presented.	The obtained results also provide the correlation between both watermark & watermarked image.
Monika Dahiya,	2017	The proposed method utilizes the Fourier transform with random phase masks so that the secret images cannot be detected easily. The reliability of the image is enhanced using the scrambling	They considered the Correlation coefficients, Standard Deviation error and mean error values as the proposed scheme has been subjected to various attacks for steganalysis.
Nazir A. Loan,	2017	In this paper, they tested and analyzed the three different variants of the proposed algorithm.	The proposed method has better performance as compared to other methods illustrated by the results in terms of robustness, security and imperceptivity.
Dimple Bansal,	2017	For embedding the watermark, red color component of the image has been utilized in order to apply DWT technique.	They implemented the 8X8 block of the image with the help of DCT which help in forming a secure and powerful image at the end.
Nasir N. Hurrah	2017	They presented on the basis of hybrid transform domain an efficient and effective watermarking scheme has been proposed in this paper.	The performance of the proposed method is measured in term of parameters such as PSNR, NCC, BER and BCE.

4. CONCLUSION

In this paper, it is concluded that watermarking is the efficient approach to secure sensitive image information. The blind watermarking scheme is the efficient scheme for the generation of watermarks. The various schemes which generate efficient watermarks are reviewed in terms of certain parameters. In future, technique will be designed which will be reliable towards certain security attacks.

REFERENCES

1. D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto and C. A. Sari, "Fast and Efficient Image Watermarking Algorithm," in International Conference On Cyber And IT Service Management (CITSM), Denpasar, 2017.

2. J. Cox, M. L. Miller, J.A Bloon, J. Fridrich, T. Kalker, "Digital Watermarking and Steganography", Morgan Kaufman Publication, Second edition, 2011

3. S. Kumar and A. Dutta, "Performance Analysis of Spatial Domain Digital Watermarking Techniques", IEEE International Conference on Information Communication & Embedded System, Chennai, India, February 2016.

4. K. Verma and A. Dutta, "Comparative Analysis of Digital Image Watermarking Algorithms in Spatial Domain", IEEE International Conference on Telecommunication, Power Analysis and Computing Techniques, Chennai, India, April 6 - 8, 2017

5. K.K. Bohra, P. Patni, "Binary Integrity in RGB Image: A Case of LSB Technique for Watermarking", International Journal of Advanced Research in Computer Engineering & Technology, vol. 4, Issue. 12, pp. 4266-4269, 2015.

6. M. Radoune, T. Boujiha, R.Messoussi, N. Idrissi and A. Roukh, "A Method of LSB substitution based on image blocks and maximum entropy, International Journal of Advanced Research in Computer Engineering & Technology, vol. 10 , Issue. 1, pp. 371-374, 2015.

7. P. Lipiński, "On domain selection for additive, blind image watermarking", Bulletin of the polish academy of science technical sciences, vol. 60, Issue. 2, pp. 317-321, 2012.

8. S.K. Jayanthi and K. Sridevi, "Fidelity Analysis of Additive and Multiplicative Watermarked Images in Integrated Domain", IOSR Journal of Computer Engineering, vol. 16, Issue. 5, pp. 36-41, 2014.

9. P. Arora and Chandana, "Efficient Watermarking Algorithm for Digital Images", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, Issue. 8, pp. 243-248, 2015.

10. Yudit Arum Mekarsari, De Rosal Ignatius Moses Setiadi, Christy Atika Sari, Eko Hari Rachmawanto, Muljono, "Non-Blind RGB Image Watermarking Technique using 2-Level Discrete Wavelet Transform and Singular Value Decomposition", 2018 International Conference on Information and Communications Technology.

11. M. Islam, G. Mallikharjunudu, A. S. Parmar, A. Kumar, R. H. Laskar, "SVM regression based robust image watermarking technique in joint DWT-DCT domain", 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies.

12. Olivia Zacharia, Nimmy George, "A Comparative Analysis between DWT-Bitplane Slicing Algorithm and Histogram Shape Based Algorithm for Image Watermarking", 2017 IEEE International Conference on Circuits and Systems.

13. Issam Dagher, Patrick Hanna, "AN IMPROVED WATERMARKING ALGORITHM USING VARIABLE BLOCK IMAGE FEATURES", 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry.

14. Shachi Natu, Prachi Natu, Tanuja Sarode, "Improved Robust Digital Image Watermarking with SVD and Hybrid Transform", 2017 International Conference on Intelligent Communication and Computational Techniques.

15. Hansa Mehra, Silviya Chouhan, Rita Choudhary, "Forgery Resistant Image Watermarking Technique using Discrete Cosine Transform (DCT)", 2017 Fourth International Conference on Image Information Processing.

16. Monika Dahiya1, Sanatan Sukhija2, Deepak Kumar3 and Hukum Singh, "Image Encryption based on watermarking technique in Fourier domain using Pixel scrambling", 2017 Fourth International Conference on Image Information Processing.

17. Nazir A. Loan, Nasir N. Hurrah1, Shabir A. Parah1, Jeon W. Lee2, Javaid A. Sheikh, G. M. Bhat, "Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption", IEEE, 2017.

18. Dimple Bansal, Manish Mathuria, "Color Image Dual Watermarking using DCT and DWT Combine Approach", International Conference on Trends in Electronics and Informatics ICEI 2017.

19. Nasir N. Hurrah1, Student member, IEEE, Nazir A. Loan2, Shabir A. Parah3 and Javaid A. Sheikh, "A Transform Domain Based Robust Color Image Watermarking Scheme for Single and Dual Attacks", 2017 Fourth International Conference on Image Information Processing.