CHT-domain Watermarking Technique for still Images: Robust and Imperceptibility Analysis under Noise

Prajwalasimha S N, Yashaswini L, Bharath Kumar M, Manoj M, Amrutha R

Abstract: In this article, a new frequency domain image watermarking scheme has been proposed, which uses Cosine Hyperbolic transformation for embedding propose. Due to vulnerability of watermarked image against noise interference, geometrical attacks and data modification attacks in a channel, many spatial and frequency domain approaches are less robust and imperceptible. In the proposed algorithm, multiple watermark images are embedded into host. During de-watermarking process, the multiple watermark images in bulk recovered watermark are combined to get resultant watermark image. Hence any modification in pixel values of watermark image can be retrieved. The resultant watermark image is subjected for various security tests and obtained results are better compared to other existing techniques. Compared to other existing frequency domain approaches, the algorithm utilizes very less execution time.

Keywords: Cosine Hyperbolic transformation, Robustness, Imperceptibility, Vulnerability, Execution time and Security tests.

I. INTRODUCTION

Digital watermarking is an imperative and non-intrusive technique that embraces identification of signature information into cover data [1]. This technique has been chosen by International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) to protect the copyright over the internet. Rightful licensing authority of an authorized user can be identified by the watermark which is embedded into a document in different moralities [2-3].

Robustness, imperceptibility and data embedding capacity are the major parameters of an efficient watermarking technique. Digital watermarking is an expectant technique to make definite the copyright of digital data. In digital watermarking, the watermark is a recognition cryptogram that takes information of the copyright owner. Watermarking is a significant technique in the region of information security [1]. It is one of the important techniques which are used for preservation the genesis of the image by defensive it against Piracy.

Multiple watermarking closely combines the compensation of single watermarking to produce classy watermarking techniques for high security and robustness. There are various techniques for developing the embedding algorithms, but realization of the outcome depends on conservation of authenticity of the watermarks under several security attacks and filtering processes. The quality of the host signal should not be degraded after the insertion of watermarks in case of imperceptible embedding processes [12].

Discrete Wavelet Transformation based watermarking scheme sensitive to the geometric distortion such as translation and cropping. A combined Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD) based watermarking scheme has been developed by Nasrin M & et al. [4]. The host image is first subjected for IWT and then decomposed into subbands. The watermark element is then embedded into these subbands. The algorithm embeds watermark with $1/4^{th}$ the size of host indicating more capacity and provides better robustness against differential and geometrical attacks. The time of execution is unnoticed and comparatively less imperceptibility is observed. Visual texturization method has been adopted by Mehran A & et al. [5] to embed gray scale logo image into host. The texture similarity is matched between host and watermark in order to provide high degree of invisibility. Affine parameter compensation method has been adopted to increase the robustness against noise interference. The method embeds watermark with $1/16^{th}$ size of host, indicating less data capacity. The algorithm utilizes huge time for execution, even with the modern high speed processors.

A hybrid two stage watermark embedding process has been proposed by Lai & et al. [6]. They adopted both Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) techniques for embedding process. The host image is first subjected for DWT and watermark is then embedded into the singular value co-efficients of the host image’s DWT subbands. The algorithm gives better imperceptibility, robustness and data capacity by embedding watermark with $1/4^{th}$ size of the host. The algorithm utilizes more time of execution due to two stage embedding process. The algorithm utilizes more time for execution due to two stage authentication process. Musrat & et al. [7] designed a hybrid technique which combines SVD and Artificial Bee Colony (ABC) in order to embed watermark into host.
The host image is first subjected for transformation using invariant wavelet transform. The low frequency subbands are then decomposed. These are then optimized using ABC techniques and then subjected for embedding process with the watermark. Better invisibility is observed, but the algorithm support watermark with 1/16th the size of host indicating comparatively less data capacity. Hong-Ying Yang & al. [8] adopted Undecimated Discrete Wavelet transformation (UDWT) and Fuzzy Support Vector Machine (FSVM) model to embed watermark into host image. The algorithm is developed to provide better imperceptibility to geometrical attacks, but supports less data capacity by embedding watermark with 1/16th size of the host image. The algorithm utilizes more execution time.

A new frequency domain watermarking scheme has been developed by Prajwalasimha S N & al. [9]. Logarithmic transformation has been adopted to embed watermark into host image. The watermark of size 1/4th the size of host is first subjected for logarithmic transformation and embedded into the host. Better imperceptibility and data embedding capacity is observed. The algorithm utilizes very less execution time, but robustness against noise interference is unnoticed.

A robust multiscale gradient direction quantization and DWT based watermarking scheme has been proposed by Eshan N & al. [10]. In this method, the invisibility of watermark is enhanced by embedding watermark into gradient vectors of subbands of transformed host at multiple wavelet scales in different angles. The algorithm provides better robustness against noise attacks and more data capacity by embedding watermark with 1/4th the size of host. Robustness against geometrical attacks is unnoticed in the algorithm.

II. PROPOSED METHOD

The proposed algorithm comprises watermarking and de-watermarking processes. Fig. 1 shows the flow diagram of proposed watermarking scheme.

A. Watermark Embedding Process

**Step1:** Watermark of size \( \omega(m, n) \) is taken as input and is combined to form a bulk watermark of size \( \omega^b(M, N) \)

\[
\omega^b(M, N) = \begin{bmatrix}
\omega(m, n) & \omega(m, n) \\
\omega(m, n) & \omega(m, n) \\
\vdots & \vdots & \ddots & \vdots \\
\omega(m, n) & \omega(m, n) \\
\end{bmatrix}
\]  

Where,

\[ m \leq \frac{M}{4} \quad \& \quad n \leq \frac{N}{4} \]

**Step2:** The bulk watermark image is subjected for Cosine Hyperbolic Transformation (CHT).

\[
\omega^f(M, N) = \frac{e^{2\omega^b(M, N)} + e^{-2\omega^b(M, N)}}{2}
\]

**Step3:** The transformed watermark is then subjected for de-intensification.

\[
\omega^d(M, N) = \frac{\omega^f(m, n)}{[\text{Maximum pixel intensity}]}
\]

**Step4:** The host image \( \varepsilon(M, N) \) is taken as another input to embed the watermark.

**Step5:** The host image and the transformed watermark are subjected for arithmetic addition with respect to each pixel individually.

\[
\psi(M, N) = \varepsilon(M, N) + \omega^f(M, N)
\]

Where,

\( \psi(M, N) \) is the watermarked image

\( \varepsilon(M, N) \) is the host image

\( \omega^f(M, N) \) is the transformed watermark
Fig. 1 Flow diagram of the proposed scheme

Table 1 Revelation of images in the algorithm

| Cover Image | WM | Transformed WM | Retrieved WM | Bulk WM Embedded Image |
|-------------|----|----------------|--------------|-----------------------|
| ![Image 1] | ![Image 2] | ![Image 3] | ![Image 4] | ![Image 5] |
| ![Image 6] | ![Image 7] | ![Image 8] | ![Image 9] | ![Image 10] |
III. EXPERIMENTAL RESULTS

The robustness of an algorithm can be decided based on its performance against various security attacks like noise interference, data tampering and modification attacks. The retrieved watermark image is compared with original watermark based on correlation between them. Each pixel value in the original image is compared with the respective pixel in the retrieved image. A maximum value of one can be achieved when both the images are same.

Table 2 Comparison of PSNR, MSE, WDR and Correlation between host and watermarked Images

| Images   | PSNR (dB)   | MSE        | WDR (dB) | Correlation |
|----------|-------------|------------|----------|-------------|
| Lena     | 49.29 (Wavelets) [9] | 1 (Wavelets) [9] | -64.4906 | 1 (Wavelets) [9] |
|          | 29.589 (DCT) [9] | 26 (DCT) [9] | 0.984 (DCT) [9] |
|          | 37.27 (HFT) [9] | 12 (HFT) [9] | 0.994 (HFT) [9] |
|          | 41.28 (IMD-WC-T) [9] | 5 (IMD-WC-T) [9] | 0.999 (IMD-WC-T) [9] |
|          | 40.6926 (GA) [9] | 1.5447 | 0.9997 |
|          | 46.2423 | | |
| Cameraman | 40.2608 (GA) [9] | 1.8079 | -63.8073 | 0.9998 |
|          | 45.5590 | | |
| Peppers  | 45.8158 | 1.7041 | -64.0642 | 0.9997 |
| Baboon   | 45.5155 | 1.8261 | -63.7638 | 0.9997 |
| Donna    | 46.4931 | 1.4581 | -64.7414 | 0.9998 |
| Carnev   | 47.8927 | 1.0564 | -66.1410 | 0.9994 |
| Elaine   | 45.1592 | 1.9823 | -63.4075 | 0.9997 |
| Galaxia  | 47.0409 | 1.2853 | -65.2893 | 0.9985 |
| Montage  | 45.7646 | 1.7243 | -64.0129 | 0.9999 |
| Tulips   | 45.6473 | 1.7715 | -63.957 | 0.9998 |
Table 3 Comparison of NC under cropping process

| Cropping the watermarked image (%) | Correlation of Watermark |
|-----------------------------------|--------------------------|
| 0                                 | 0.9997                   |
| 25                                | 0.9994                   |
| 50                                | 0.9972                   |
| 75                                | 0                        |

Table 4 Comparison of NC under LSB modification attack

| Watermark Images | Correlation with LSB modification | Correlation without LSB modification |
|------------------|----------------------------------|-------------------------------------|
| Watermark        | 0.9341                           | 0.9997                              |

Table 5 Comparison of NC under noise interference

| Noise density in watermarked image (%) | Correlation of Watermark |
|---------------------------------------|--------------------------|
| 10                                    | 0.9684                   |
| 20                                    | 0.9336                   |
| 30                                    | 0.8906                   |
| 40                                    | 0.8473                   |
| 50                                    | 0.7962                   |
| 60                                    | 0.7321                   |
| 70                                    | 0.6615                   |
| 80                                    | 0.5462                   |

![Fig. 3 Revelation of retrieved watermark images under different noise densities](image1)

![Fig. 4 Revelation of original and retrieved watermark image under LSB attack neutralization attack conditions](image2)

Original Watermark

Retrieved Watermark image with LSB modification

Fig. 4 Revelation of original and retrieved watermark image under LSB attack neutralization attack conditions
The proposed watermarking technique embeds watermark image into host using cosine hyperbolic transformation. The algorithm supports bulk data capacity by embedding watermark with 1/16th size of the host. Better robustness is achieved against noise interference, geometrical attacks and data modification attacks. More than 90% of watermark information can be retrieved from the host, under LSB modification attack, which is the major drawback of many time domain approaches. More than 50% of watermark information can be retrieved under 80% noise density in the watermarked image. More than 99% of the watermark information can be retrieved against noise interference, geometrical attacks and modification attack, which is the major drawback of many time domain approaches. More than 90% of watermark information can be retrieved from the host, und...

REFERENCES

1. Ziqiang Chen, Lixiang Li, Haipeng Peng, Yuhong Liu and Yixian Yang, “A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization,” IEEE Transactions on Multimedia, Vol.20, No.8, pp. 1973-1986, 2018
2. Prajwalasimha S N et. al., “2D-Crypt: Image Encryption and Decryption in Chaotic Domain,” International Journal of Engineering and Advanced Technology, Vol. 9, Issue 2, 2019
3. Prajwalasimha S N et. al., “Modified Gingerbreadman Chaotic Substitution and Transformation based Image Encryption,” Computational Vision and Bio-Inspired Computing, Advances in Intelligent Systems and Computing, Springer, Vol. 1108, 2020
4. Nasrin M. Makbol and Bee Ee Khoo, “A new Robust and Secure Digital Image Watermarking Scheme based on Integer Wavelet Transform and Singular Value Decomposition,” Journal of Digital Signal Processing, Elsevier, Vol. 33, pp. 134-147, 2014
5. Mehran Andalibi and Damon M. Chandler, “Digital Image Watermarking via Adaptive Logo Texturization,” IEEE Transactions on Image Processing, Vol.24, No.12, pp. 5060-5073, 2015

6. Chih-Chin Lai and Cheng-Chih Tsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition,” IEEE Transactions on Instrumentation and Measurement, Vol.59, No.11, pp. 3060-3063, 2010
7. Musrat Ali, et al., “An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony,” Journal of Information Sciences, Vol. 301, No. 20, pp. 44-60, 2015
8. Hong-ying Yang, et al., “A Robust Digital Watermarking Algorithm in Undecimated Wavelet Transform Domain,” Journal of Computers and Electrical Engineering, Vol. 39, pp. 893-906, 2013
9. Prajwalasimha S.N., Sonashree S., Ashoka C.J., Ashwini P. (2019) Digital Image Watermarking Using Sine Transform Technique. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CV8). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, Vol 30. Springer, Cham
10. Ehsan Nezhadarya, Z.Jane Wang and Rabab Kreidieh Ward, “Robust Image Watermarking Based on Multiscale Gradient Direction Quantization,” IEEE Transactions on Information Forensics and Security, Vol.6, No.4, pp. 1200-1213, 2017

AUTHORS PROFILE

Prajwalasimha S N, Researcher from ATME Research Centre, India. His research interest includes Cryptography, Steganography, Digital Image Watermarking and Image Processing. He has published many research papers in International Journals, Conferences & Book Chapters indexed by Scopus and Web of Science. He is serving as Reviewer for many International Journals and has been conferred with the best research contribution award from IEEE ICECCT 2017.

Yashaswini L, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. Her research interest includes Signal and Image Processing.

Bharath Kumar M, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.

Manoj M, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. His research interest includes Signal and Image Processing.

Amrutha R, Scholar from Dept. of Electronics & Communication, ATME College of Engineering affiliated to Visvesvaraya Technological University, India. Her research interest includes Signal and Image Processing.