International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

IMAGE TAMPER DETECTION BY USING SINGULAR VALUE DECOMPOSITION

Ganga Vara Lakshmi Sada
Dept. of ECE, Aditya Engineering College, (affiliated to JNTUK), Surampalem, A.P., India
sadagangavaralakshmi@gmail.com
Vinay Medidi
Dept. of ECE, Aditya Engineering College, (affiliated to JNTUK), Surampalem, A.P., India
vinaymedidi45@gmail.com
Mr. S. Jagadeesh
Associate Professor, Dept. of ECE, Aditya Engineering College, (affiliated to JNTUK)
Surampalem, A.P., India

Abstract
In this fast-developing world, Digital image plays a vital role in several application areas and the digital dependency has taken up great heights. With this large usage of digital dependencies, the multimedia data can be copied or edited in an easy form and this can be affecting its original content. The changing of original content of image or adding extra information is tampering and providing false information. In the last few decades, it has been an urgent concern for researchers to ensure the authenticity of digital images. Based on the desired applications, several suitable watermarking techniques have been developed to mitigate this concern. This paper provides the imagetamper detection algorithm by using watermarking. Watermarking is used for copyright protection. It gives high quality watermarked image and high robustness to attacks. Watermarking is done by using LSB embedding, SVD and chaotic sequence. SVD is used fordigital security of an image and ownership identification.

Keywords: Image processing, Watermarking, SVD (singular value decomposition), LSB (Least significant bit) embedding, Chaotic sequence, Tamper detection and Attacks on image.

Introduction

Watermarking is the process of imperceptibly altering a piece of data in order to embed information about the data. That definition reveals two important characteristics of watermarking. First, information embedding should not cause perceptible changes to the host image (sometimes called cover image or original image). Second, the message should be related to the host image. In this sense, the watermarking techniques form a subset of information hiding techniques, which also include cases where the hidden information is not related to the host medium (e.g., in covert communications).

Singular Value Decomposition (SVD) is a matrix factorization method that decomposes a given matrix into three matrices: a left singular matrix, a diagonal singular value matrix, and a right singular matrix.Let A be an m x n matrix, then SVD of A is given by:

$$A = USV^T$$

where U is an m x m left singular matrix.,

S is an m x n diagonal singular value matrix,
V is an n x n right singular matrix, and T denotes transpose.
The diagonal entries of S are non-negative and are arranged in descending order, i.e., $\sigma 1 \geq \sigma 2 \geq \ldots \geq \sigma r \geq 0$, where r is the rank of the matrix A. The columns of U and V are orthonormal, i.e.,

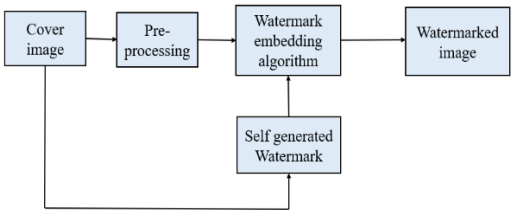
$$U^T * U = V^T * V = I$$

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

where I is the identity matrix.

Proposed Methodology

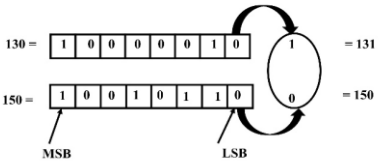
In this paper, the framework of general watermarking methods, separated into the processes of embedding and extracting watermarks, along with a general background, is shortly revised in the first section. Some standard design requirements for evaluating the performance of watermarking systems are listed in the following subsections. Related applications that make watermarking systems a highly focused research area also described. Based on the working domain, a survey of digital image watermarking techniques is subsequently presented. Then, a summary of the research results of the discussed state-of-the-art methods and current trends in the field is described in tabular format. Next, we list some conventional attacks or threats which must be treated as a challenge for designing an efficient system.



Watermark generation block diagram

The watermark is generated by using SVD algorithm and embedded into image by using LSB embedding.

Least significant bit modification is the most commonly used algorithm for spatial domain watermarking. Here, the least significant bit (LSB) of randomly chosen pixels can be altered to hide the most significant bit (MSB) of another. It generates a random signal by using a specific key. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way. Several techniques may process the host image. This type of algorithm is easy to implement and is image is not affected. It provides high perceptual transparency with a negligible impact on the host image. However, this algorithm can be affected by undesirable noise, cropping, lossy compression, and so on, and may be attacked by a hacker by setting all the LSB bits to "1," modifying the embedded watermark easily without any difficulty. The LSB technique can easily be understood by the example depicted in Figure 8. Suppose two pixel values in the host image are 130 (10,000,010) and 150 (10,010,110). Then, using the LSB technique, if the embedded watermark is 10, then the watermarked pixel values pixel values will be 131 (10,000,011) and 150 (10,010,110), respectively.

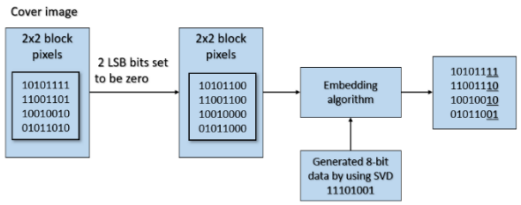


Several researchers have studied modifications of the LSB technique, which are commonly related to the spatial domain. LSB techniques have been developed based on a bit-plane of digital discrete signals (e.g., audio or images). A bit-plane that represents the signal is a set of bits having the same bit position in each of the binary numbers. Most techniques use only one bit-plane for embedding. This technique works on the least significant bits (i.e., the seventh-eighth bit-planes), but others have used three bit-planes (i.e., the sixth–eighth bit-planes) or even four bit-planes (i.e., the fifth–eighth bit-planes) for embedding with acceptable image quality. The two least significant bits (i.e., the seventh–eighth bits of the cover image) can be replaced with the chosen bit of the secret image by simply using an OR operation in a specific manner.

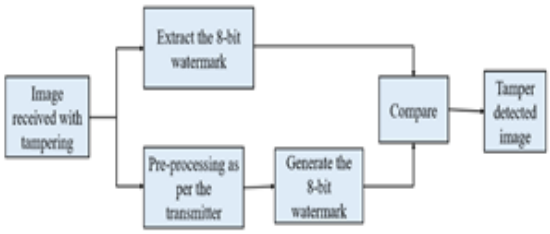
This method first converts the host image into a stream of binary bits, outputs zero in the embedded bit, and then shifts the secret image to the right by 4 bits. Then, an OR operation is performed on these two (i.e., the host and secret images) to obtain the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

combined image. This operation is illustrated in below Figure.



Extraction of watermark: The watermark extraction is as same as the process of transmitter region. Watermarked image is taken. The 8-bit data is extracted from the watermarked image by following the procedure done for watermarking the image. On the other the 8-bit data is generated in receiver section by following same procedure followed in watermarking image at the transmitter section. To embed watermark to an original image here we are using LSB (Least significant bit) embedding technique.



Watermark Extraction and Tamper Detection

Algorithm Implementation

Transmitter Region:

In this section, a watermarking algorithm based on SVD (singular value decomposition) is proposed. Singular value decomposition (SVD) is used to extract the feature information from the singular value of the image. The proposed algorithm can be divided into three parts: watermark generation, watermarking and tampering detection.

Watermark generation:

In this the watermark is generated from the image i.e., self- generated watermark. Water mark is generated by using singular value decomposition. The specificsteps of generating authentication watermark are as follows:

Image blocking:A gray scale image of NxN size is taken. Convert into binary image and make the two LSB planes zero, reshape that into an image of 256x256 blocks.

Apply SVD:

The image is now divided into 2x2 non-overlapping blocks. Generate 6-bit data from maximum SVD value of each 2x2 block. From 6-bit datagenerate 8-bit.By dividing 6-bit into two bits and performs binary AND operation and add that generated 2-bit datato the 6-bit data.

S=svd(i)

Where I is the pixel value of an image.

Watermark embedding:

LSB embedding technique is used to embed the watermark to the original image. The self-generated watermark is embedded into the image which 2 LSB planes are zero. To embed the data into the data here we are using chaotic sequence.

Chaotic sequence generation: Chaotic sequence is random sequence. This is to embed the data into image in chaotic sequence order.

x(n+1)=r*x(n)*(1-x(n))

Generate the sequence by using below formula take the value of r=4. Take the value A=4 and x(0)=0.2027 generate chaotic sequence and sort the sequence. Map the indices of the previous order and generate an array of indices name as ‘C1’.Now embed the 8-bit data in the order of the array. Divide the image I1 into 2x2 non overlapping blocks, take the first block and take the first index value that C1(0) and take the 8-bit data from smax_bits from the index C1(0). Like wise embed the data into image that image is watermarked image.

The tampered image is received which is tampering is done on watermarked image which is embedded in transmitter part.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

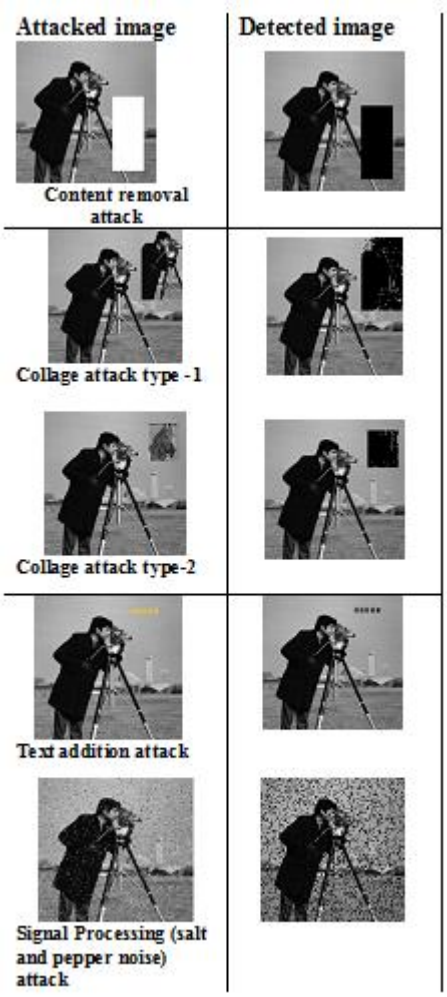
Different attacks are given to the image that are tampered images. In this receiver part tamper detection is done.

Watermark extraction:
From the tampered or attacked image 8-bit data is extracted by following the transmitter process that means the way how the 8-bit data is embedded into the image by using chaotic sequence. The tampered image size reshaped into 256x256, then it is divided into 2x2 non-overlapping blocks and 8-bit data is extracted from each pixel 2 LSB bits.

Receiver Region:
In receiver part generate the 8-bit data from tampered image. The specificsteps of generating 8-bit same as transmitter region.
Image blocking:A gray scale image of NxN size is taken. Convert into binary image and make the two LSB planes zero. The image is now divided into 2x2 non-overlapping blocks, reshape that into an image of 256x256 blocks.
Apply SVD: Divide the reshaped image into 2x2 non overlapping blocks. Generate 6-bit data from maximum SVD value of each 2x2 block. From 6-bit data generate 8-bit. By dividing 6-bit into two bits and performs binary AND operation and add that generated 2-bit data to the 6-bit data
.
S=svd(i)

Where I is the pixel value of an image. Generate a matrix of 256x256 size, compare generated 8-bit data of tampered or attacked image and extracted 8-bit data of original image if both are same put the data as the original data otherwise make it as zero.

Results
Table 6.1 Attacked and detected images



Attacks:
Content removal attack: The content of original image is removed. In table 6.1 the first attack is content removal attack and the detected image. There is 100% detection in content removal attack as show in the above table. That is number of tampered blocks are equal to number of detected blocks.
• Collage attack-1: Some part of the original image is taken and added to the same image at another place. Collage attack-1 in the above table the number of detected blocks are not same as tampered blocks. The accuracy is 89%.
Collage attack-2: Some part of an image (other image) is taken and that is added to the original image. Collage attack-2 in the above table the number of detected blocks are not same as tampered blocks.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

The accuracy is 93%. Text addition attack: Text is added to the original image. The text is detected in the image but not exactly as added text. The accuracy is 90%.

Signal processing attack: In signal processing attack noise is added to the original image. The salt and pepper noise is detected by using this algorithm. It detected all added noise successfully. Accuracy is 99%.

Performance metrics:
True Positive (TP)
The detected blocks value matches the actually tampered blocks value.The actual value was positive, and the model detected a positive value.

True Negative (TN)
The detected blocks value matches the actually tamapered blocks value.The actual tampered blocks was negative, and the model detected blocks also a negative value.

False Positive (FP) – Type I Error
The detected block was falsely detected.The actual tampered blocks value was negative, but the model detected blocks value is a positive value.Also known as the type I error.

False Negative (FN) – Type II Error
The detected blocks value was falsely detected.The actual tampered blocks value was positive, but the model detected blocks value is a negative value.Also known as the type II error.

FALSE POSITIVE RATE(FPR):

$$FPR = \frac{FP}{FP + TN}$$

Accuracy:

Accuracy is one metric for evaluating correctly detected blocks of image. A high accuracy indicates good performance of a method. Accuracy has the following definition:
Accuracy can also be calculated in terms of positives and negatives as follows:

$$ACCURACY(ACC) = \frac{TN + TP}{TP + TN + FP + FN}$$

Attack	FPR	ACC
Content removal attack	0.1186	0.9914
Collage attack-1	0.1474	0.8526
Collage attack-2	0.0555	0.9445
Text addition attack	0.0031	0.9969
Signal processing attack	0.1730	0.8274

V. CONCLUSION

At present, information can be duplicated easily due to the interactive and digital communication of multimedia data. This issue makes digital image watermarking a significant field of research. Digital image watermarking using various techniques has been applied as an important tool for image authentication, integrity verification, tamper detection, copyright protection, and the digital security of an image. In this study, we reviewed the most dominant state-of-the-art watermarking techniques LSB embedding. Watermark is applied to the original image by using LSB embedding using chaotic sequence. On the basis of various performance metrics, it has concluded that the method proposed in this paper watermarking, SVD and LSB embedding for image tamper detection working effectively.

References

[1] Wang, Jianyu, and Zhiguo Du. "A method of processing color image watermarking based on the Haar wavelet." *Journal of Visual Communication and Image Representation* 64 (2019): 102627.
[2] Chang, Chin-Chen, Piyu Tsai, and Chia-Chen Lin. "SVD-based digital image watermarking scheme." *Pattern Recognition Letters* 26.10 (2005): 1577-1586.
[3] Lai, Chih-Chin. "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm." *Digital Signal*

Processing 21.4 (2011): 522-527.
[4] Huang, Fangjun, and Zhi-Hong Guan. "A hybrid SVD-DCT watermarking method based on LPSNR." *Pattern Recognition Letters* 25.15 (2004): 1769-1775.
[5] Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain." *National Academy Science Letters* 37 (2014): 351-358.
[6] Chandra, DV Satish. "Digital image watermarking using singular value decomposition." *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002.*. Vol. 3. IEEE, 2002.
[7]Guo, Jing-Ming, and HeriPrasetyo. "False-positive-free SVD-based image watermarking." *Journal of Visual Communication and Image Representation* 25.5 (2014): 1149-1163.
[8]Haribabu, Maruturi, ChHima Bindu, and K. Veera Swamy. "A secure & invisible image watermarking scheme based on wavelet transform in HSI color space." *Procedia Computer Science* 93
(2016): 462-468.
[9] Wang, Xin, and Li Jiang. "A Tampering Detection Algorithm Based on Multidirectional Authentication." *2022 4th International Conference on Advances in Computer Technology, Information Science and Communications (CTISC)*. IEEE, 2022.
[10] LV, LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." *Journal of Theoretical and Applied Information Technology* 42.2 (2012): 287-291.
[11] Wang, Haoyuan, Xin Wang, and Li Jiang. "A tampering detection algorithm based on multi-scrambling coding." *Thirteenth International Conference on Digital Image Processing (ICDIP 2021)*. Vol. 11878. SPIE, 2021.
[12] Zhang, Heng, Chengyou Wang, and Xiao Zhou. "Fragile watermarking for image authentication using the characteristic of SVD." *Algorithms* 10.1 (2017): 27.
[13] HU, Jun-quan, Ji-wu HUANG, and Da-ren HUANG. "An Algorithm for Fragile Watermarking Based on HVS." *ACTA ELECTONICA SINICA* 31.7 (2003): 1057.
[14] Liu, Guangqi, et al. "A tamper-resistant authentication scheme on digital image." *Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering*. Springer Berlin Heidelberg, 2013.
[15]Kansal, Megha, SukhjeetRanade, and Amandeep Kaur. "Fragile watermarking for image authentication using a hierarchical mechanism." *Int. J. Eng. Res. Appl.* 2.4 (2012): 1759-1763.