IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Image Tamper Detection and Recovery Using Water Marking Scheme

M Ram Bhupal, Rama Venkata Praneeth Sriram, Rahul Dinakar Papathoti, Manoj Sai Harsha Pasupuleti, Vinay Naga Venkata Santosh S

Assistant Professor, Department of IT, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh, India

UG Students, Department of IT, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh. India

ABSTRACT

Tampering of images is one of the serious threats in today's digital world in which the images are being transferred via networks. Preventing the tampering of images is a tedious task that needs the involvement of various network protection mechanisms which can be vulnerable. Avoiding of these attacks is not suggestible as these images may have to pass significant information like the case of forensic department networks and other highly confidential communications. Also the tampering of images have became easier for present generation as there are several image editing softwares which can cause significant damage to the photos. This is the area where the proposed system can be an useful resource as it can detect the images that were affected by various signal procesisng attacks like constant avergage. Initially the image is embedded with watermark which can be attacked while passing it through a communication channel. At the reciever side, the image is moved for the detection of tampering after the extraction of watermark is completed from the image obtained via communication channel. In the case of any occurrence of tampering, the image is recovered by using the recovery bits generated.

KEYWORDS: Tamper Detection, Digital image watermarking, Tampered Image Recovery, 2-level Discrete Wavelet Transform.

I.INTRODUCTION

Tampering of images is one of the serious threats in today's digital world in which the images are being transferred via networks. These images can be easily modified using photo manipulating software which makes the end user difficult to decide the genuinity of image. Image forgery is the process of modifying content in an image purposefully to fudge the data in the host image. It involves modifying the content of particular part of the image or collective parts of the image. Image tampering has become one of the major threats as it became very hard for the naked eye to detect the changes.

Many technologies have come into force in the recent years for contributing an easy way to modify the image. It became easy for the falsifier to execute their interests in image tampering by using emerging technologies.

II.WATERMARKING

The process of burying the computerized data in a carrier signal; the buried data may or may not contain the relation with the carrier signal. We can insert the images directly through pixels or can be inserted through block patterns. Watermarks are used to protect authentic information and to provide the validity of a legal document. Watermarking based authentication is used for detecting the tamper and recovery.

Watermarking is classified into two types. They are

1. Robust watermarking
2. Fragile watermarking.

Fragile watermarks are sensitive and are used for tamper detection. Robust watermarks are used to combat common image processing operations. Fragile watermarking is one of the authentication mechanisms of multimedia data like image, video, and audio.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Tamper Detection:

Tamper detection is the process of detecting whether the image is tampered or not. There are two forms of tamper detection. They are

1. Passive approach
2. Active approach

The active approach is subdivided into two types as follows.

1. Digital Signature
2. Digital Watermarking

With the active approach, a watermark or digital signature is embedded when the image is created. While using these embedding's, we can analyze the image has been tampered with or not at later stages.

The passive approach is known as the blind approach because there is no additional information required for image forgery detection. This approach is based on the features brought out directly from the image. The passive approach is subdivided into two types as follows.

1. Dependent approach
2. Independent approach

The dependent approach detects the following forgeries,

1. Splicing forgery
2. Copy-move forgery

The independent approach detects the following forgeries,

1. Resampling

2. Compression forgeries

The proposed solution introduces block reliance in the authentication module by using the block bridging mechanism. Initially each image block is taken from which the features are extracted using the Discrete Cosine Transform (DCT) and the 5 MSB bits are extracted. Using the block linking another 5 authentication bits are generated. These values are combined and XOR operation is performed with the key.

For the recovery bit generation the 2x2 sub-blocks of each block are taken and are grouped. Horizontal grouping, vertical grouping, and diagonal grouping are the three options. Determine the sub-grouping block's type. Depending on the Grouping type, choose the pixel values for G1 and G2. Calculate the average of the values in the G1 and G2 categories. All values must be preserved in the original dataset. Euclidean distance is measured with the help of k-means clustering and selects the cluster number that goes to the shortest possible distance and converts to 8 bit binary values and appends the two bits thus recovery data is produced. The combination of restoration bits and the verification bits act as a watermark. The watermark can be extracted by applying the same procedure in reverse.

In the step 2, the goal is to verify that each image block is legitimate. and identify the location where the tamper has occurred. To detect the image tampering the extricated authentication data bits are weighed with the original authentication bits. If both are matched then the image is not tampered and there is no need to recover the image. If the data doesn't match then the image block is marked as invalid.

The recovery procedure is used to retrieve the original contents when the invalid image blocks are detected. The faulty image block's recovery data is taken from the associated mapped block. The average of the nearby blocks' values is computed. The recovered 10 bits recovery data is used in the sub-block recovery process to restore the original pixel values of the tampered sub-block. The grouping type is represented by the first two bits. The remaining eight bits are the cluster number, which is used to calculate the mean utilizing K-Means clustering technique.

III.SYSTEM IMPLEMENTATION

In the proposed method, the fragile watermarking technique is being used as the fragile watermarks are very sensitive such that even a minute change in the image will affect the embedded data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

In the proposed method, two-level wavelet transform will be used for watermarking scheme. The embedding algorithm is utilized to embed the watermark using secret key (scaling and embedding). In DWT transform image will be divided into 4 sub-bands at each level (LL, LH, HL, and HH). The watermarked image thus produced is sent through a communication channel.

The blind watermark extraction algorithm extracts the watermark by utilizing the key without the help of the original image. The active tamper detection is applied to the image if the watermark retrieved is distorted. The recovery algorithm can be applied to the attacked watermarked image by producing the recovered image. The recovery of the image can be performed using K-means clustering algorithm.

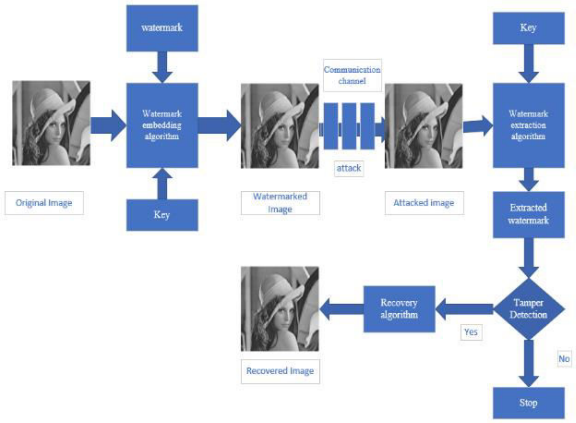

Fig 1: Architecture

IV.PREREQUISITES

Schur Decomposition

The Schur decomposition of a matrix X yields two matrices V & S, with

$X = V S V^T$

S being the upper triangular matrix. A unitary matrix is V. V T is the inverse of V. Real Eigen values are diagonally distributed in S, and complex Eigen values are distributed in 2 x 2 blocks. SD requires $8/3N^3$ flops, which is less than the (1/3) number of computations required by SVD, which is around $11N^3$ flops. The major rationale for using SD in ABB calculation is to validate each block separately with 16 authentication bits. The important image is divided into 128 x 128 blocks, each block having a size of 4 x 4, and the SD is computed for each block.

Discrete Wavelet Transform:

An image is decomposed into four sub-bands (SBs) using the 2-D DWT (LL, LH , HL, HH). Diagonal details make up the high frequency band. Low frequency components are represented by the approximation band, whereas high frequency components are represented by the detail band. This domain is difficult to set up and defend against attacks. Haar wavelet is used in the proposed scheme.

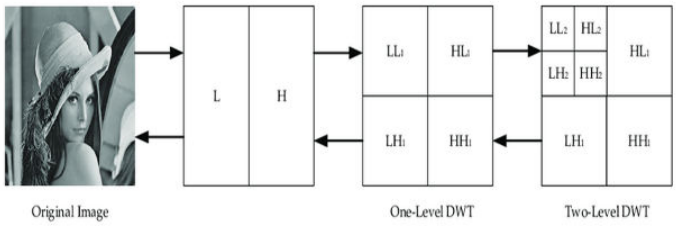

Fig 2: Discrete Wavelet Transform

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Streamlit:

Streamlit is a special framework belongs to Python language which is mainly useful to create web apps for machine learning and data science based applications. It can handle almost all the Python libraries such as open-cv, tkinter, NumPy etc.

Tkinter:

This module offers a set functions that enables the user to browse the images from the computer such that these images can be used with in the program. It improves the user intercation with the webiste which was created by the streamlit framework.

K-means Clustering:

K-Means follows centroid based technique to group the data into categories. It is an unsupervised clustering algorithm used in machine learning. The main aim of this algorithm is to form the clusters in such a way that the distance between the clusters is more than the distance between the points inside the cluster.

V.MODULES

There are four modules for the project. They are as follows:

Watermark Embedding

Watermark Extraction

Tamper Detection

Tamper Recovery

Watermark Embedding

Module 1:

Step 1: A host image (I) with 512x512 pixels and a watermark (W) with 128x128 pixels are used in this described fragile watermarking system.

Step 2: The "Haar" wavelet is applied to the host image utilizing 2-level DWT.

$$[\mathrm{LL1}, \mathrm{LH1}, \mathrm{HL1}, \mathrm{HH1}] = \mathrm{DWT2(I)}$$

$$[\mathrm{LL2}, \mathrm{LH2}, \mathrm{HL2}, \mathrm{HH2}] = \mathrm{DWT2(LL1)}$$

Step 3: Both the Scaling (α) and embedding (β) factors are used as the key values for the watermark embedding. Because it contains the majority of the image information, the watermark is incorporated in the Low-level sub-band retrieved from the second level of DWT.

$$LL2^{W} = (\alpha \times LL2 + \beta \times W)$$

Step 4: For two layers, inverse DWT is applied using the "Haar" Wavelet. The watermarked image is created by using altered low-level subband.

$$LL1^{W} = IDWT2\,[LL2^{W}, LH2, HL2, HH2]$$

$$I^{W} = IDWT2\,[LL1^{W}, LH1, HL1, HH1]$$

Module 2:

Step 1: The watermark embedded image is used as the module's input.

Step 2: The watermarked image is now separated into 128x128 blocks, each measuring 4x4 pixels.

Step 3: The Least Significant Bit(LSB) value is changed with zero for each block of the image.

Step 4: On each block of the image, the Schur decomposition (SD) is applied. SD of matrix Y outputs Unitary Matrix (U) and Schur form (T).

$$U \times T = Schur(Y)$$

Step 5: After completing Schur decomposition, the appropriate Schur form traces for each block of the picture are calculated. The Authenticated Block Bits (ABB) are created from the collected traces. The amount of bits for each block of the image is 16 bits, hence these traces are mapped to [0 - 262144].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Step 6: Next, the Authentication block bits for every block will be utilised in place of the watermarked picture's Least Significant Bits (Iw), resulting in an authenticated watermarked image (IwA).

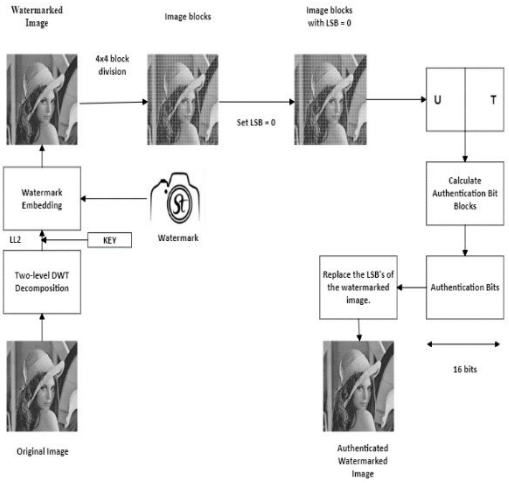

Fig 3: Watermark Embedding Algorithm

Watermark Extraction

Step 1: The "Haar" wavelet is applied to the authenticated image utilizing 2-level DWT. $[LL1', LH1', HL1', HH1'] = DWT2(I_A^W)$

$$[LL2', LH2', HL2', HH2'] = DWT2(LL1')$$

Step 2: For the watermark extraction, the Key Value, (α , β) and Low-level sub-band LL2 are taken into account, as indicated below.

$$W'_S = \frac{LL2'_W - (\alpha \text{ x } LL2)}{\beta}$$

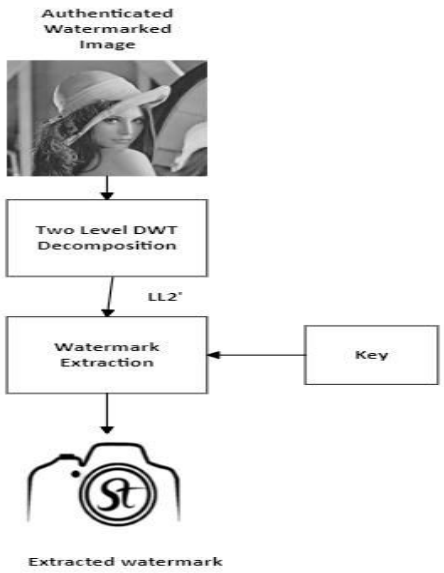

Fig 4: Watermark Extraction Algorithm

Tamper Detection

Step 1: The Authenticated watermarked image (I^w_A) is taken into consideration for image tamper detection.

Step 2: I^w_A is now divided into 128x128 blocks, each of which is 4x4 in size.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Step 3: The Least Significant Bit(LSB) value is changed with zero for each block of the image.Step 4: On each watermarked block, schur decomposition is applied.

$$U' \times T' = Schur(Y')$$

Step 5: After completing Schur decomposition, the appropriate Schur form traces for each block of the picture are calculated. The Authenticated Block Bits (ABB) are created from the collected traces. The amount of bits for each block of the image is 16 bits, hence these traces are mapped to [0 - 262144].

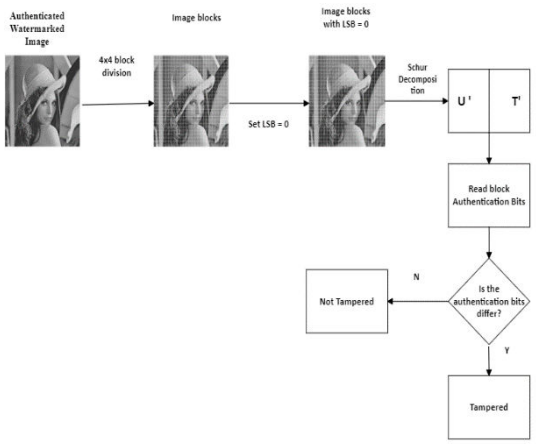

Fig 5: Tamper Detection Algorithm

Tamper Recovery

For recovering the tampered image K-means clustering algorithm is performed on the 2x2 sub-blocks of each block are taken and are grouped. Horizontal grouping, vertical grouping, and diagonal grouping are the three options for grouping. Decide on the sub-grouping block's type. Depending on the Grouping type, choose the pixel values for each of the two groupings.

Calculate the average of the values in the G1 and G2 categories. Those values should be saved in the dataset. Measure the Euclidean distance using k-means clustering, choose the cluster number that yields the shortest distance, convert to 8-bit binary values, and append the two bits, and you'll get recovery data. The watermark is made up of the authentication and recovery bits together.

V.RESULTS

Input images:

Fig 6: Original Image

Fig 7: Watermark

Fig 8: Tampered Image

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103092 |

Output:

Fig 9: Displayed message along with Recovered Image

VI.CONCLUSION

This paper consists of the image tampering detection along with the recovery algorithm. In this method each image block, of size 4 × 4, is being authenticated using the DWT coefficients. The K-means clustering algorithm is used in this research to propose a recovery approach for each 2 2 sub block of the image. To implant the created authentication data and recovery data in the spatial domain of the original image, a fragile watermarking approach is used. The authentication data is crucial in detecting tampering. The reliance between the blocks aids in more precisely detecting the tamper. The K-means clustering approach can help improve recovery performance. When compared to the existing system, the proposed solution produces the best outcomes. For the typical test photos, the proposed approach produces better results. It will be possible to apply it to medical photos in future. Cryptography algorithms can be applied further to increase the security.

REFERENCES

[1]: Bhalerao, S., Ansari, I.A. and Kumar, A., 2021. A secure image watermarking for tamper detection and localization. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), pp.1057-1068.

[2]: Siddiqi, M.H., Asghar, K., Draz, U., Ali, A., Alruwaili, M., Alhwaiti, Y., Alanazi, S. and Kamruzzaman, M.M., 2021. Image Splicing-Based Forgery Detection Using Discrete Wavelet Transform and Edge Weighted Local Binary Patterns. *Security and Communication Networks*, *2021*.

[3]: Bansal, D. and Passi, A., 2021. Image Forensic Investigation Using Discrete Cosine Transform-Based Approach. *Wireless Personal Communications*, *119*(4), pp.3241-3253.

[4]:Abdelhakim, A., Saleh, H.I. and Abdelhakim, M., 2019. Fragile watermarking for image tamper detection and localization with effective recovery capability using K-means clustering. *Multimedia Tools and Applications*, *78*(22), pp.32523-32563.

[5]: Rakhmawati, L., Suryani, T., Wirawan, W., Suwadi, S. and Endroyono, E., 2019. Exploiting self-embedding fragile watermarking method for image tamper detection and recovery. *International Journal of Intelligent Engineering and Systems*, *12*(4), pp.62-70.

[6]: Lai, C.C., 2011. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, *21*(4), pp.522-527.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details