# Digital Image Forgery Detection Using Basic Manipulations In Facebook

S S.Patil, A N.Patil, N P.Patil, J D.Dhongde, B S.Khade

**Abstract**: In this modern age in which we are living, digital images play a vital role in many application areas like social networking websites, for example, Facebook. But at the same time the image retouching techniques has also increased which forms a serious threat to the security of digital images in Facebook. To cope with this problem, the field of digital forensics and investigation has emerged and provided some trust in digital images. In this paper we present a new algorithm to detect digital_image forgery based on cellular_automata and data embedding in spatial domain. The original JPEG image which the user upload's initially on his/her profile will be partitioned into some regions. We use region-based segmentation to specifying the desired regions of interest from the input image. First we extract the visual attributes of the original image and achieve the statistical information for the selected region and save it in the database. Then we apply linear cellular automata rules to create a robust cipher key from these values. We embed the cipher key into the spatial domain to authenticate and validate the original image. The proposed algorithm is applied on 100 numbers of grayscale images (size 800 × 600). The results have demonstrated the robustness and stable time complexity of the proposed method.

**Index Terms**: Digital Forensics, Digital image forgery, Fake image, Cellular_automata, Region-based segmentation, Data embedding, Facebook.

## 1 INTRODUCTION

Digital forensics has received more attention in the last few years due to its ability to restore the lost trust to digital images. Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software such as Photoshop. Nowadays, it is possible to add or remove important part from an image without leaving any obvious traces of tampering. During the availability of powerful software tools in the field of editing and manipulating the digital images, it is possible that someone use these tools to change the content of a digital image and violate its validation. Digital image forgery detection methods are significance in content authentication and validity protection for digital images. Authenticating digital images, validating their contents, and detecting forgeries are one of the critical challenges for governmental and nongovernmental organizations and departments. Detection of malicious manipulation with digital images (digital forgeries) in Facebook application is the topic of this paper. Our algorithm is based on embedding precious and unique characteristics of a digital image into the spatial domain of it. The forged region is determined as the one that lacks the data which is embedded. The method is tested both on examples of real forged and non-forged Digital Images.

The forgery detection techniques that are developed for digital images are mainly classified into active and passive approaches. While the active methods insert data or signature at the time of digitizing, the passive methods operate in the absence of any data or signature. In the active methods, we embed data into the original image to protect it against the forgery. For validation and authentication aspects, the data which is embed in spatial domain should be unpredictable, invisible and also sensitive to any modification. Data embedding in the spatial domain consists of insertion and detection stages. The insertion algorithms are used to embed the data into the digital image and detection algorithms extract those data.

**Fig. 1.1** Forged Images Example

- *S S.Patil is currently pursuing bachelor of engineering in information technology from Pune University, India ,E-mail: saileestar8@gmail.com*
- *A N.Patil is currently pursuing bachelor of engineering in information technology from Pune University, India ,E-mail: anpatil.26@gmail.com*
- *N P.Patil is currently pursuing bachelor of engineering in information technology from Pune University, India ,E-mail: nishappatil18@gmail.com*
- *J D.Dhongde is currently pursuing bachelor of engineering in information technology from Pune University, India ,E-mail: juidhongde8@gmail.com*
- *B S.Khade is Working as Asst.Professor in Pune University, India, E-mail: khadebeena@gmail.com*
- *(This information is optional; change it according to your need.)*

**Fig. 1.2** Forged Images Example

Fig. 1.1 and Fig. 1.2 is an example of mage forgery in which Fig. 1.1 is the original image which is carefully manipulated as shown in Fig. 1.2 i.e. forged image.

## 2 Related Work

Many image forgery detection techniques have been proposed in recent years. We have done survey of some of these proposed techniques. These techniques require prior knowledge regarding the Original image therefore they have limited applications as there is a possibility of unavailability of the original image. In case of the interactive generic algorithm the main idea is to create a user oriented image retrieval system. In this technique the models were implemented in a CBIR system for a specific application domain. This system uses the visual contents of an image such as color, shape, texture and spatial layout to represent and index the image. In another application of recognition of facial expressions and measurement of levels of interest from video, to uncover the hidden patterns associated with specific expressions, discrete HMMs were used to model the encoded time series describing facial expressions. The seed idea was to recognize six universal facial expressions from visual data and using them to compute levels of interest. By combining the techniques such as rescaling detection algorithm, rotation detection algorithm and contrast enhancement/histogram equalization the detection of image alterations such as re-sampling, contrast enhancement and histogram equalization has been implemented. The seed idea of this technique was to effectively recognize if any image is forged and identify the forged regions. As mentioned above techniques limitation of first is in this EVEN SEGMENTATION is a problem. Global features of image at object level i.e. intended to be close to the performance of human visual system. And in second it requires a multiple dimensions. Image & Video forgery detection is one of the most important techniques used now-a-days for original image detection.

## 3 Proposed Architecture

The main idea of our proposed algorithm is to create a robust secret key and embed it in the LSB of a layer of the original image, to protect it against forgery. Our proposed method is based on active approaches in which some data or secret key is embedded in to the spatial domain of the original image for the authentication. We have implemented our algorithm on a set of one hundred images and calculated the Singular Values, Right and Left Singular Vectors of the original image and pushed the SVD features into one dimensional cellular automata to generate the secret key as shown if Fig. 2.

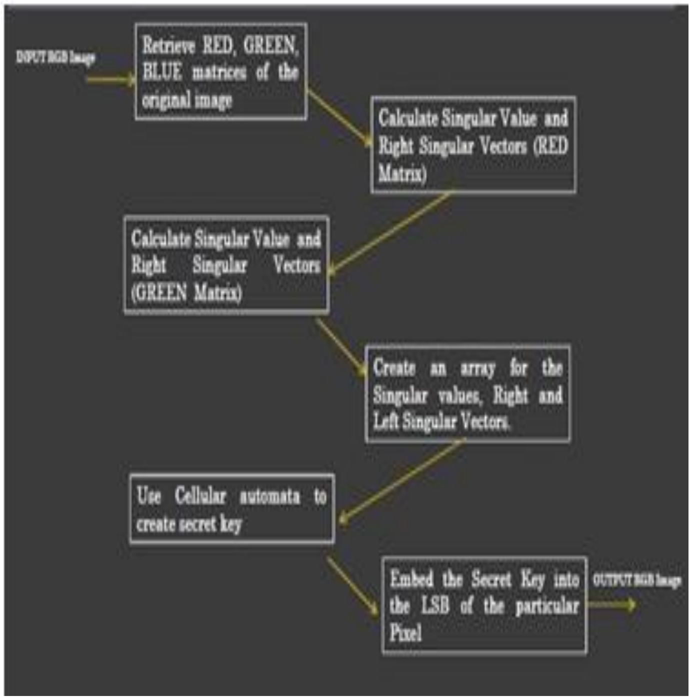
INPUT RGB Image
Retrieve RED, GREEN, BLUE matrices of the original image
Calculate Singular Value and Right Singular Vectors (RED Matrix)
Calculate Singular Value and Right Singular Vectors (GREEN Matrix)
Create an array for the Singular values, Right and Left Singular Vectors.
Use Cellular automata to create secret key
Embed the Secret Key into the LSB of the particular Pixel
OUTPUT RGB Image

**Fig. 2** Block Diagram for Proposed Architecture

The Image which the user wants to upload in his facebook profile will be first scanned to retrieve the RGB components and store other statistical data related to the original image and a cipher key will be generated of the original image for comparison. All the information will be stored in a database. After a while if the user wishes to check whether any manipulation has taken place on his/her image he can download the image to test. If the image is altered the results are shown that the image is altered or else its valid original image. In this way we can test the trust ability of such social networking websites and whether or not our images are secure in such applications.

## 4 Implementation Working

The basic implementation required for this proposed project Includes the basic operations performed using rotation, scaling, histogram, contrast enhancement, wrapping. These techniques are used to detect the forged image. Once we obtain any image we can check the image for any changes done overall. Usually digital image forgeries are created by copy-pasting a portion of an image onto some other image. While doing so, it is often necessary to resize the pasted portion of the image to suit the sampling grid of the host image. The resampling Operation changes certain characteristics of the pasted portion, which when detected serves as a clue of tampering. In This paper, we present deterministic techniques to detect resampling, and localize the portion of the image that has been tampered with. Two of the techniques are in pixel domain and two others in frequency domain. We study the efficiency of our techniques against JPEG compression and subsequent resampling of the entire tampered image using cellular automata. In this paper, we further investigate the properties of a resample discrete sequence and present deterministic techniques to detect resampling. We call an image *original*, whenever it is acquired out of a digital camera and has not been altered, even in its resolution or size. A *tampered image* is one which is deliberately altered in its content. We call that portion of the image which has been pasted from some other image as *alien* portion.

### 4.1 Active Approaches

The area of active methods simply can be divided into the data hiding approaches. By data hiding we refer to methods embedding secondary data into the image. Active approaches assume an inserting of a digital data at the source side (e.g., Scanner) and verifying the mark integrity at the detection side.

### 4.2 Passive Approaches

Passive methods are mostly based on the fact that forgeries can bring into the image specific detectable changes passive techniques for image forensics operate in the absence of any watermark or signature. These work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.

**A Digital image is a collection of various properties:**

- Color Schema (Black White, Grayscale, RGB …)
- Format (.JPEG, .TIF, .BMP, .PNG, .GIF …)
- Visual Properties (Brightness, Image Size …)
- Statistical Properties (Sum, Mean, Median, Mode, Range …)

## 5 Algorithms

### 5.1 Data Embedding Algorithm

Input: .JPEG grayscale image to apply data embedding to it for forgery protection.

Output: .PNG grayscale image file.

***Step1*****:** Open the JPEG original image and make a matrix of that.

***Step2*****:** Perform the region-based segmentation and grouping the neighboring pixels to specifying the separated parts in the original image.

***Step3*****:** Calculate the statistical information for each partition and create the array list of these values.

***Step4*****:** Perform the cellular automata rule. This rule performs on the array list to create a cipher key for each partition.

***Step5*****:** Convert the cipher keys to the binary representation.

***Step6*****:** Select the first eight pixels in the original image and embed the binary sequences of cipher key into the LSB of these eight pixels.

### 5.2 Forgery Detection Algorithm

Input: PNG image that contains the cipher key.

Output: Digital image forgery detection alarm.

***Step1*****:** Open the .PNG input image and make digital image matrix.

***Step2*****:** initial integer variable Cipher Value to zero.

***Step3*****:** initial integer variable PixelArrayValue to zero.

***Step4*****:** Perform the region-based segmentation and grouping the neighboring pixels to specifying the separated parts in the original image.

***Step5*****:** Calculate the statistical information for each partition and create the array list of these values.

***Step6*****:** Perform the cellular automata rule. This rule performs on the array list to create a cipher key for each partition.

***Step7*****:** Select the first eight pixels of the image and extract the LSB binary value of pixels.

***Step8*****:** set Cipher Value = value of the cipher key that generated in Step 4.

***Step9*****:** set PixelArrayValue = the extraction value in Step 5.

***Step10*****:** If PixelArrayValue = = Cipher Value then print message "False Forgery Alarm“ Else Print message "True Forgery Alarm";

### 5.3 Equations

ARITHMETIC MEAN
MEDIAN 1, 6, 2, 8, 7, 2. Sorting: 1, 2, 2, 6, 7, 8.
Median= (2 + 6)/2 = 4.
MODE 1, 2, 3, 3, 4, 7, 9 Mode= 3.
RANGE 89, 73, 84, 91, 87, 77, 94
Range= Highest - Lowest = 94 - 73 = 21
VARIANCE COEFFICIENT OF VARIATION.

## 6 Conclusion

The proposed algorithm has been applied successfully for digital image forgery detection. In this paper we present a new method based on data embedding in spatial domain and cellular automata which was done by calculating the invaluable statistical information of the digital image such as dominant values like C.V, Variance and Mean, median and so on. The cellular automata rule also generates a robust cipher key which can be used to embed into the image. This algorithm needs the original image to forgery detection. The result obtained from our algorithm clearly shown the robustness of our method and the trust ability of facebook application to check changes in profile pictures of users.

## REFERENCES

[1] H. Farid, "Image Forgery Detection a Survey", IEEE Signal Processing Magazine, March 2009.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking", San Francisco, CA: Morgan Kaufmann, 2002.

[3] A. Bovik, "The Essential Guide to Image Processing", Academic Press is an imprint of Elsevier, 2009.

[4] K.Z. Mao, “Identifying Critical Variables of Principal Components for Unsupervised Feature Selection”, IEEE Trans. Syst., Man, Cybern. B, vol. 35(2), pp. 339-344, 2005.

[5] M. Embree, "Numerical Analysis Lecture Notes”, Rice University, October 2009.

[6] Shatten A., "Cellular Automata", Institute of General Chemistry Vienna University of Technology, Austria, 1997.

[7] R. Grimaldi, "Discrete and Combinatorial Mathematics: An Applied Introduction", Prentice Hall, 2002.

[8] M. Kirchner, “Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue,” in ACM Multimedia and Security Workshop, 2008, pp. 11–20.