Dr. Mohamed A. Elaskily

Ass. Professor at Informatics Dept., Electronics Research Institute (ERI)

Mohamed Elaskily currently works at the Department of Informatics, Electronics Research Institute (ERI). He is a member of Cybersecurity and Privacy LAB. Mohamed got his Ph.D. from CSE Dept., Faculty of Electronic Engineering, Menoufia University, 2019. Mohamed does research in Information Security, Network Security, Digital Forensics, Data Hiding, and Machine Intelligence & their applications. Their current projects are 'Digital Image and Video Forensics' & 'Multimedia Cybersecurity'.

E-mail: Mohamed_Elaskily@eri.sci.eg

Website: https://www.researchgate.net/profile/Mohamed-Elaskily

Mobile: +2 0100 78 99 8 66

Enhancement of Forensic Methods for Digital Images

Presented by:

Dr. Mohamed A. Elaskily

Researcher at Informatics Dept., Electronics Research Institute (ERI)

Thesis supervised by:

Prof. Heba K. Aslan

Professor & Ex. Head of Informatics dept. - Electronic Research Institute (ERI)

Prof. Dr. Heba Ahmed Elnemr

Prof. in Computers & systems Dept. - Electronic Research Institute (ERI)

Prof. Osama S. Faragallah

Dr. Mohamed M. Dessouky

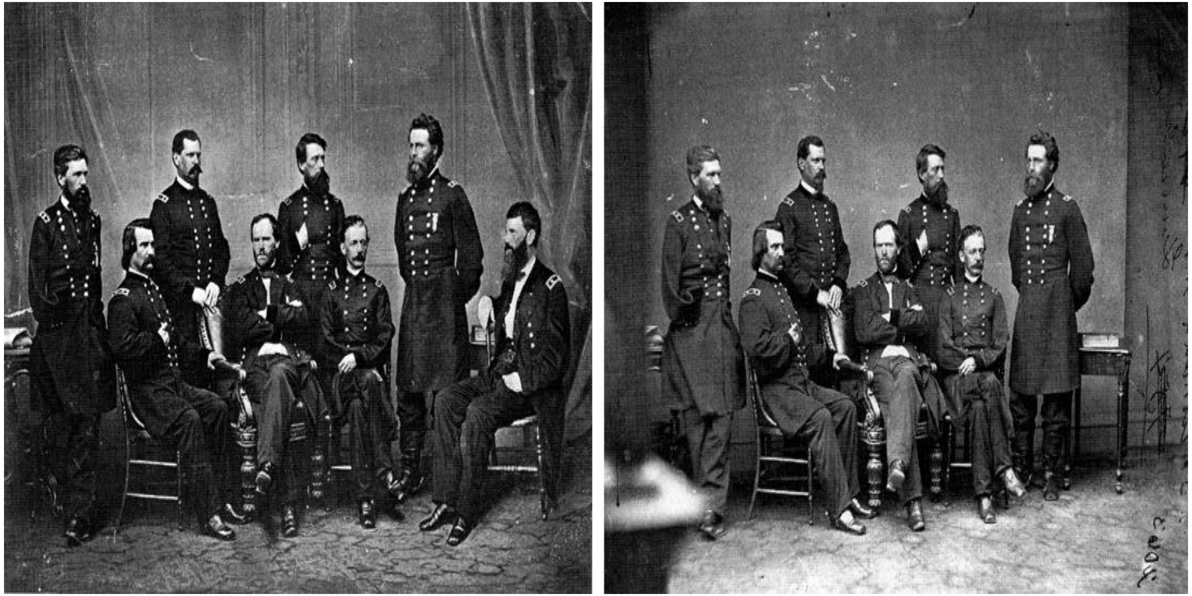
Computer Science & Engineering Department, Faculty of Electronic Engineering, Menoufia University

Outlines

- Problem definition
- Thesis Objectives
- Digital Forensics and digital image authentication
- Applications of detecting digital forgeries
- Types of digital image forgeries
- Why Copy-Move Forgery Detection (CMFD) ?
- Families of CMFD algorithms
- Enhanced Filter-based SIFT Approach for CMFD (First algorithm)
- Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)
- A Novel Deep Learning Framework for CMFD (Third algorithm)
- Research Outputs
- Conclusion
- Future Work

Problem Definition

Vision does not mean believing



In year 1865: the left is the forged photograph after General Francis P. Blair was added at the rightmost position and shown on right is the original photograph.

Problem Definition

Vision does not mean believing

Forged image used from North Korea to obscure the rumors of Kim Jong-II's death [2]

Problem Definition

Vision does not mean believing


BBC NEWS

Search

Explore the BBC

BBC NEWS CHANNEL

News Front Page

World

Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

England

Northern Ireland

Scotland

Wales

Business

Politics

Health

Education

Science/Nature

Technology

Entertainment

Also in the news

Video and Audio

E-mail this to a friend

Printable version

Mounting sense of crisis over Iran

By Jon Leyne

BBC News, Tehran

Some of the missiles tested could reach Israel

A day after a major Iranian ballistic missile test provoked international condemnation, the front pages in Iran are covered with pictures of the missiles soaring into the sky.

There is a note of pride in the coverage, and perhaps just a little

IRAN NUCLEAR CRISIS

KEY STORIES

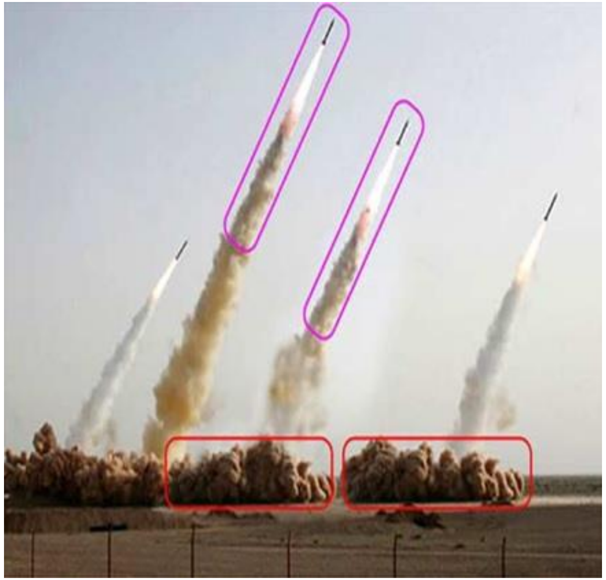
- Iran missile test 'provocative'
- Iran discounts 'attack by Israel'
- Israelis 'rehearse Iran attack'

ANALYSIS AND BACKGROUND

Mounting crisis

There is a building sense of crisis over Iran, says the BBC's Jon Leyne

- America's Israeli option on Iran
- West keen to keep talking
- Analysis: The rise of Ali Larijani
- Q&A: Iran and the nuclear issue
- Nuclear power in the Middle East
- Quick guide: Iran nuclear crisis
- Iran's key nuclear sites
- Q&A: Nuclear disarmament
- Timeline: US-Iran ties



Onset of BBC news about Iranian nuclear experiments

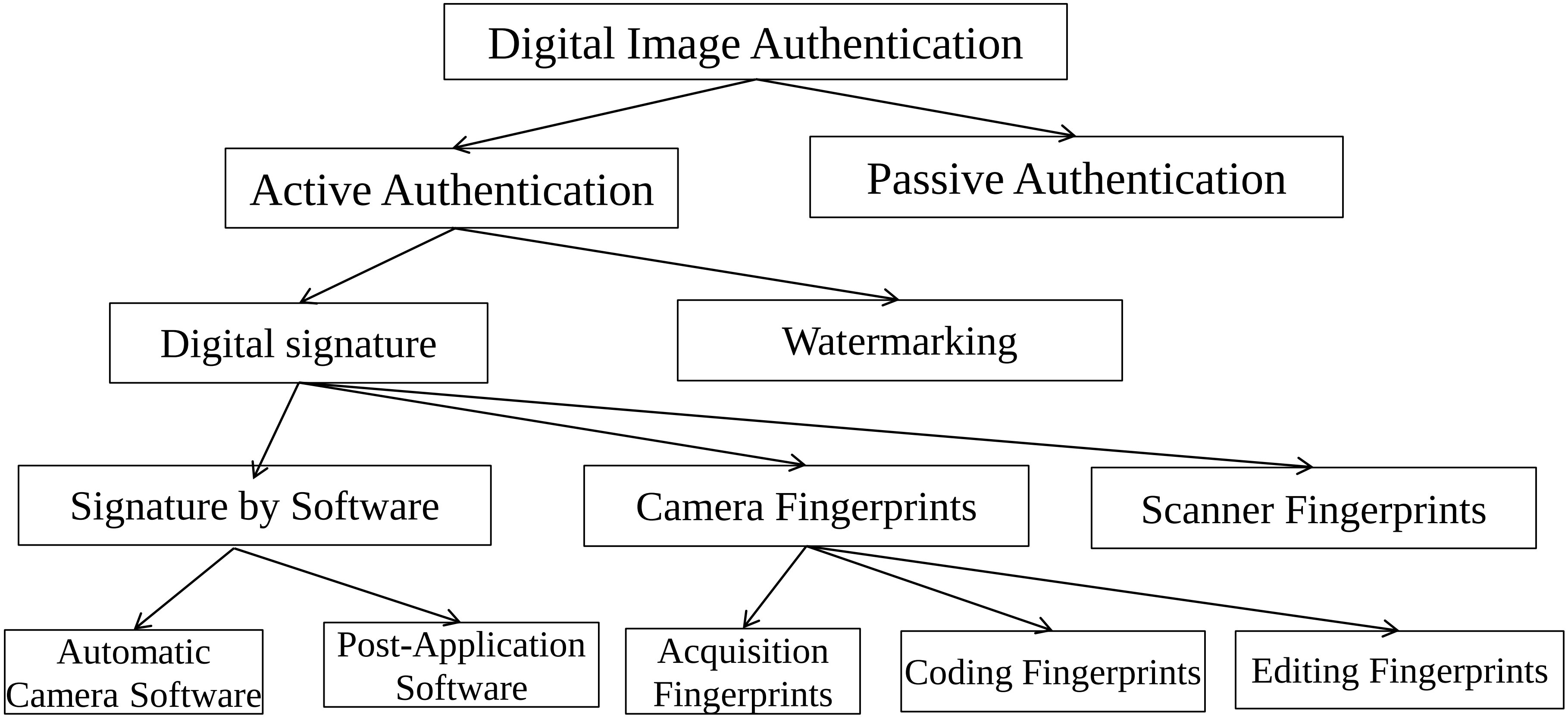
Thesis Objectives

- Building a general map in the areas of:
  - Digital image forensics
  - Copy-Move forgery
  - Evaluate existing CMFD algorithms
- Enhancing the existing algorithms of CMFD
- Building a new CMFD algorithms which outperform the traditional algorithms in efficiency, speed, and computational cost

Digital Forgeries

- Digital Forensics
  - Computer Forensics
    - Analysis digital modification on (OS, Storage, USB, Electronic documents, Embedded Sys.
  - Mobile Forensics
    - Analysis attacks on Comm. Systems such as (GSM, SMS, Email, data communication)
  - Multimedia Forensics
    - Image Forensics
    - Audio Forensics
    - Video Forensics
    - Text Forensics
    - Animation Forensics
  - Network Forensics
    - Analysis attacks on Net. logins, and Net. Traffic
  - Database Forensics
    - Analysis DB and Metadata, log files, RAM data

Digital Image Authentication



Digital Image Authentication

- Active authentication [3-4]:
  - Need a previous knowledge of the image
  - Embedded on the original image and checked in the other side
  - Take processing Time to embed and check

- Passive authentication [3-4]:
  - Does not need any previous knowledge of the image

Applications Digital Image Forgeries

- Military images authentication
- Intelligence images authentication
- Image authentication for using as evidences in courts
- Detecting of electronic crimes
- Detecting forgeries in electronic documents
- Counterfeit currency
- Defaming of persons
- Social media

Types of Digital Image Forgeries

- Copy-move Forgery
- Image splicing or composing
- Image resampling
- Image retouching or Enhancing
- Image Morphing
- Images Created by Graphical Software

Types of Digital Image Forgeries

- **Copy-move Forgery:** use one image only to duplicate or hide one or more object in the same image [5].




The two left images are original while the two right images are forged

Types of Digital Image Forgeries

- **Image splicing or composing:** Combining two or more images to create a new image [6].



The left and middle images are original while the right images is composed one

Types of Digital Image Forgeries

- **Image splicing or composing:** Combining two or more images to create a new image [6].

The left and middle images are original while the right is the forged image [7]

Types of Digital Image Forgeries

- **Image splicing or composing:** Combining two or more images to create a new image [6].

New York Times ten most impressive news photos of 2006: A newspaper apologized for the fake picture scandal, in which a photographer manipulated images to show Tibetan antelopes roaming under a bridge on the Qinghai-Tibet Railway

Types of Digital Image Forgeries

- **Image resampling:** Creating a new image with increasing/decreasing in height/width of a specific object in image or in all content of the image [8].

Types of Digital Image Forgeries

- **Image retouching or Enhancing:** is the process of enhancing an object or image to exhibit or hide a specific feature as coloring, lighting or background changing [9].



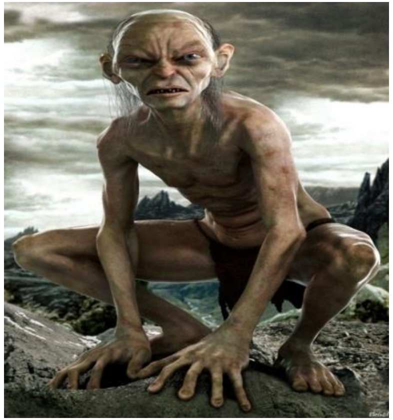


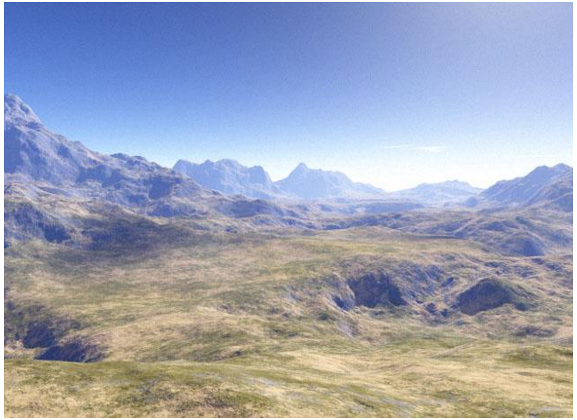
Types of Digital Image Forgeries

- **Image Morphing:** Creating process of gradually changing a shape of an image into another shape in another image and must be applied between two images [9].

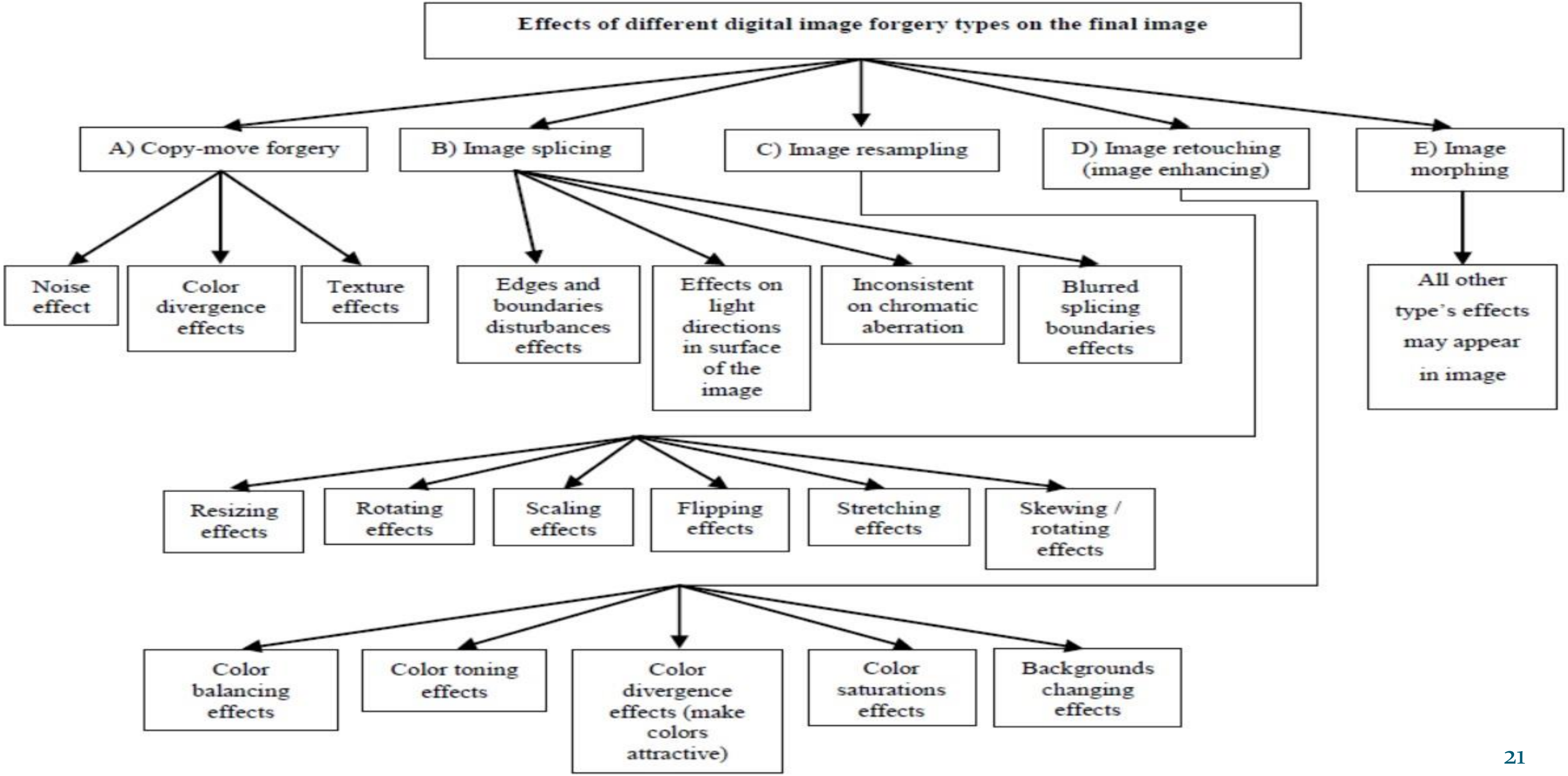
Types of Digital Image Forgeries

- **Images Created by Graphical Software:** is the process of creating a forged image not connected with reality by building its objects and features by computer [10].

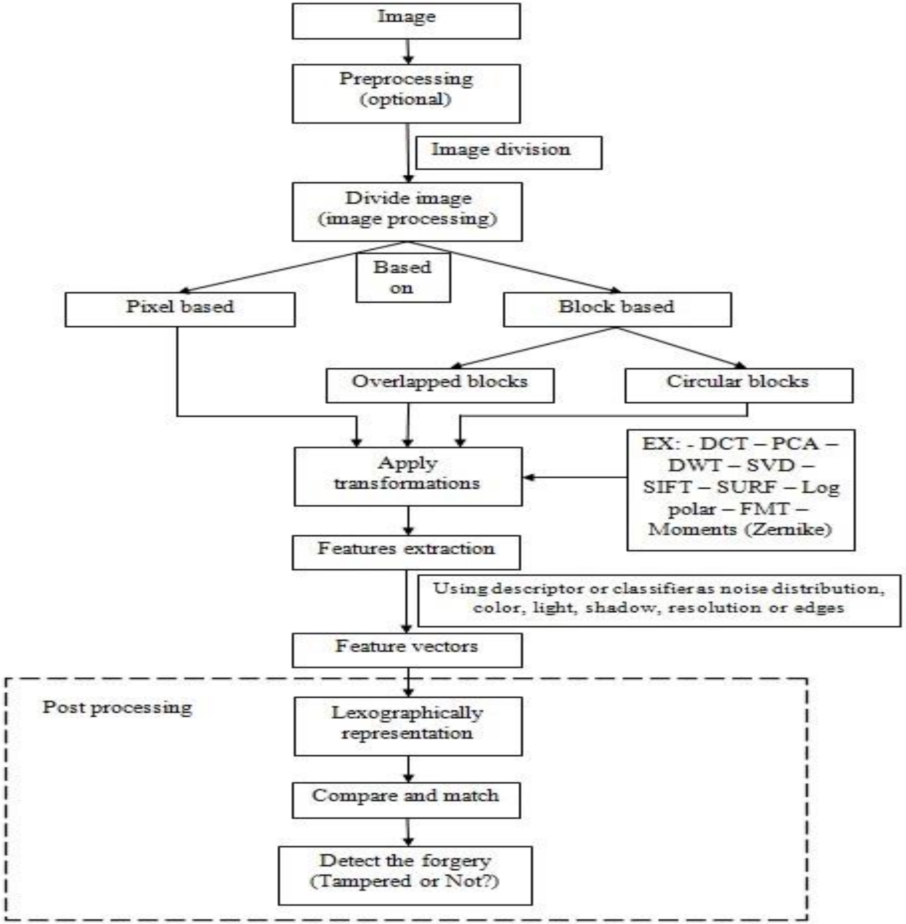




Why is Copy-Move Forgery The Most Difficult of Detection?

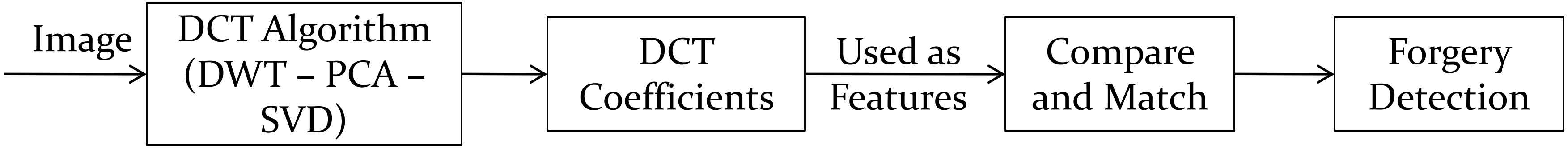


Copy-Move Forgery Detection Algorithms Methodology



Copy-Move Forgery Detection Algorithms

1) **Algorithms using DCT:** using Discrete Cosine Transform (DCT) to be applied on an image and extract DCT coefficients that are used as features and compare between these coefficients to find the duplicated regions [10].



- There are other techniques, which resemble DCT such as Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), and Singular Value Decomposition (SVD) [11].

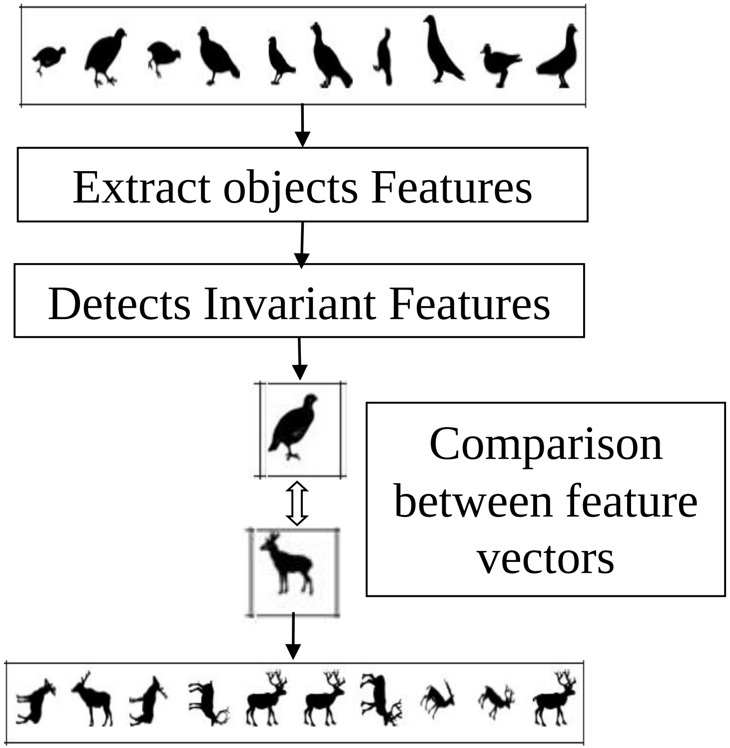
Copy-Move Forgery Detection Algorithms

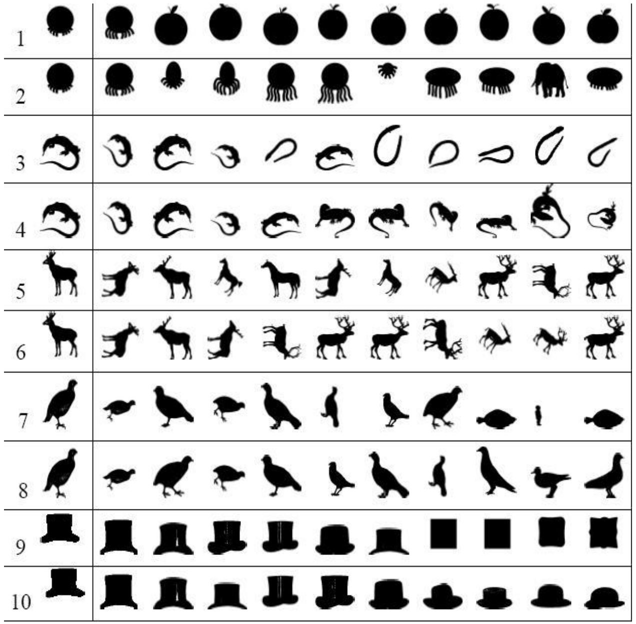
2) Algorithms using invariant image moments (Shape Analysis):

- Image moments: a certain particular weighted average of image pixels intensities or functions[12].

A. Perform shape analysis.
B. Detect image objects after segmentations.
C. Offer information about objects orientations.
D. Detect central points of each object.
E. Report the total image pixels intensities and prosperities.

Copy-Move Forgery Detection Algorithms





Copy-Move Forgery Detection Algorithms

3) Algorithms Using Texture and Intensity Descriptors:

- Based on analysis of **structure of the image** [13] inferred from:
  - Intensity or colors changes: appearing frequently in different patterns.
  - Relationship between pixels: properties in its local area.
  - Edges homogeneity.
  - Spatial arrangement of color: or intensities of a specific region.
  - Spatial relationship between neighbors using statistical method [14].

Tampering harms the texture patterns of an image.

Copy-Move Forgery Detection Algorithms

4) Algorithms Using Invariant Key Points [15-16]:

- It is classified as non-block based algorithms.
- Based on extracting image features from all parts of the image.
- Invariant against all geometrical transformation attacks such as scaling, rotation, translation, and reflection.

Copy-Move Forgery Detection Algorithms

5) **Algorithms Using Invariant Key Points:**

- Scale Invariant Feature Transform (SIFT)
  - A 128 bytes dimensional feature vector is generated for each key-point. The feature vector consists of a row, column, scale, and orientation [17].
- Speed up Robust Features (SURF) more speed and more stable than SIFT.
  - A 64 bytes dimensional feature vector is generated for each key-point.

A comparison between copy-move forgery detection algorithm's families

Performing Steps		Families and Algorithms					
		DCT Maind et al. [19]	**Invariant Image Moments** Ryu et al. [20]	**Texture and Intensity Descriptors** Sharma et al. [21]	**Invariant Keypoints** Costanzo et al. [22]	**Mutual Information** Chakraborty et al. [23]	**SVD** Zhao et al. [24]
Pre-processing	- Grayscale conversions: - Resizing :	-Yes -No	-Yes -No	-Yes -No	-Yes -No	-No -N0	-Yes -N0
Block division	- Division : - Block size :	-Overlapping circular blocks. -Fixed size 8x8 pixels.	-Overlapping blocks. - fixed size *(B x B)*.	-Overlapping blocks. - fixed size *(B x B)*.	- Non-overlapping blocks. -fixed size 32 x 32	- Non-overlapping blocks. -fixed size m x n.	- Overlapping blocks then non-overlapping sub-blocks. - Fixed size b x b.
Features Extraction	-Method : -Numbers :	- Apply DCT on each circular block to extract DCT coefficients. - Four features vector (V1, V2, V3 and V4).	-Use Zernike moments to extract feature vectors of each block. - 12 moments used as feature vectors.	- Apply (CSLBP) to each block and Feature of a block representing by a row in the feature matrix. - 2^ (N/2) binary patterns where N is the number of surrounding pixels.	Extracts SIFT features and use KCR, CHI square distance detector and SVM detector. -Depends on SIFT keypoints.	------------- -------------	- Gets DCT coefficients for each block then, apply SVD on each sub-block to extract the features vector. - Depends on sub-blocks numbers.
Matching	- Sorting : -Matching Methodology:	- Lexicographically representation. - Using Euclidean distance between vectors of two pairs blocks.	- Lexicographically representation. -Using locality Sensitive Hashing (LSH) to match similarities between Features vectors among all blocks.	- Lexicographically representation. - CSLBP produces 2^(N/2) binary patterns with circular radius R used as features.	- Lexicographically representation. - classify the output keypoints to *h1*,*hm* and *hh* then, use CLBA to detects the difference in variance between tested image and CLBA tampered image.	------------- - By histogram, calculate two matrices represents the joint probability distribution of two regions block *B(i)* & embedded image *R(j)* with test threshold.	- Lexicographically representation. - Using a threshold *T(shift)* to match similar pairs of blocks with user-specified parameter Td and Euclidian distance threshold *(dist)*.
Verification Test		Threshold distance and morphological operation is used.	Use set of SATs thresholds for minimum Euclidean distance in addition to Space Error Reduction procedure (ERP).	Using shift frequency threshold *T(shift)* and Euclidian distance threshold *(dist)*.	**KCR** value should be smaller than its value in the authentic image. If **SVM** output is higher than a certain threshold value the image is tampered	Using mutual information value, if the regions are not duplicated its mutual information value equal zero otherwise it gives a diagonal value.	The morphologically open operation is applied to fill the holes in marked regions and remove the isolated blocks.
Computational Complexity		Low computational complexity due to low dimension size of features vectors and block size.	Medium computational complexity because it performs two matching procedure LSH and ERP.	Low computational complexity.	High computational complexity due to large number of its iteration with large number of detectors and features	Low complexity because it not needs to extract features or apply matching procedure.	Low computational complexity due to reducing the size of the checked region by divide the image into two sub-blocks levels.

A comparison between algorithms robustness against different processing operations

Families and algorithms		Number of thresholds	Robustness against intermediate processes				Robustness against post-processing operations			Estimate the affine transform
			Reflection	Rotation	Scaling	Illumination changes	JPEG compression	Blurring	Gaussian white noise	
DCT	Maind et al. [19]	2	No	No	No	No	Yes	Yes	Yes	No
Invariant Image Moments	Ryu et al. [20]	4	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Texture and intensity	Sharma et al. [21]	2	No	No	No	No	Yes	Yes	Yes	No
Invariant Keypoints	Costanzo et al. [22]	3	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Mutual Information	Chakraborty [23]	1	No	No	No	Yes	No	No	No	No
SVD	Zhao et al. [24]	3	No	No	No	No	Yes	Yes	Yes	No

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

Preprocessing Attacks

- Noise addition
- Image blurring
- Color changing
- Brightness adjustment
- Contrast adjustment
- JPEG compression
- Rotation, Scaling, Reflection, and Translation

Filtering Objectives

- Noise reduction
- Image smoothing
- Image sharpening
- Show edges and details of the image (image enhancement)
- Contrast Enhancement

Filters Types

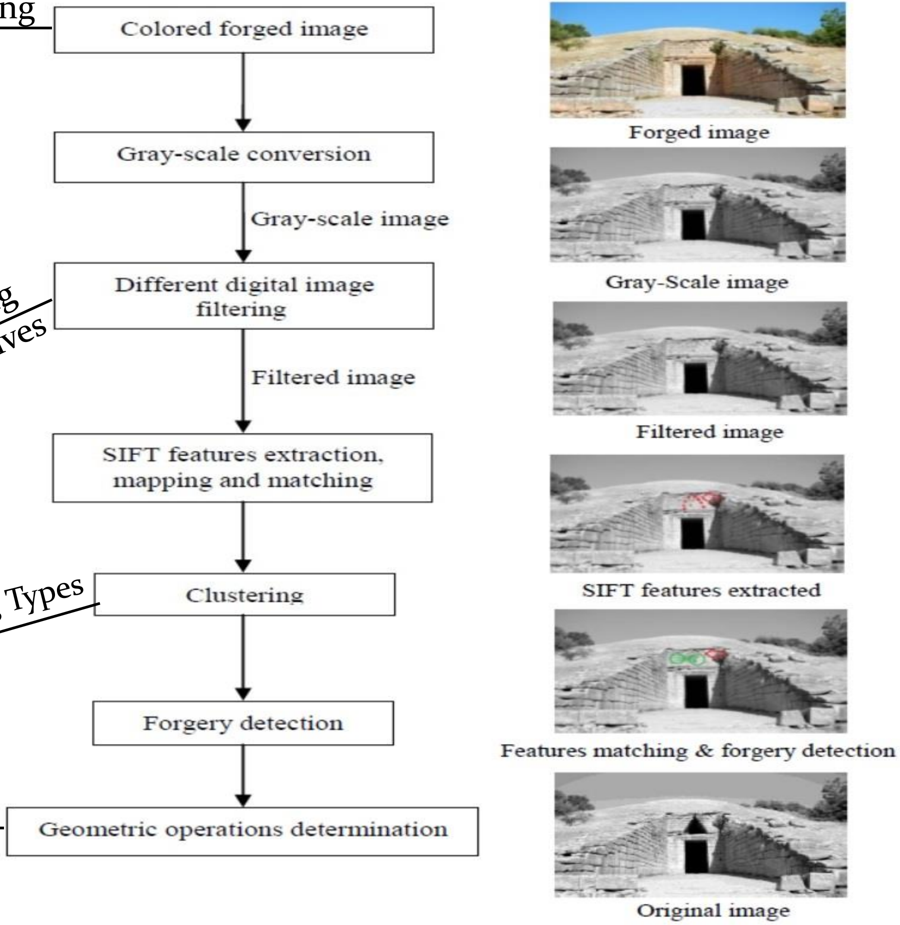
- High pass filter.
- Low pass filter.
- Butterworth low pass filter.
- Combination of them.

Clustering Types

- Single Linkage
- Centroid Linkage
- Ward Linkage

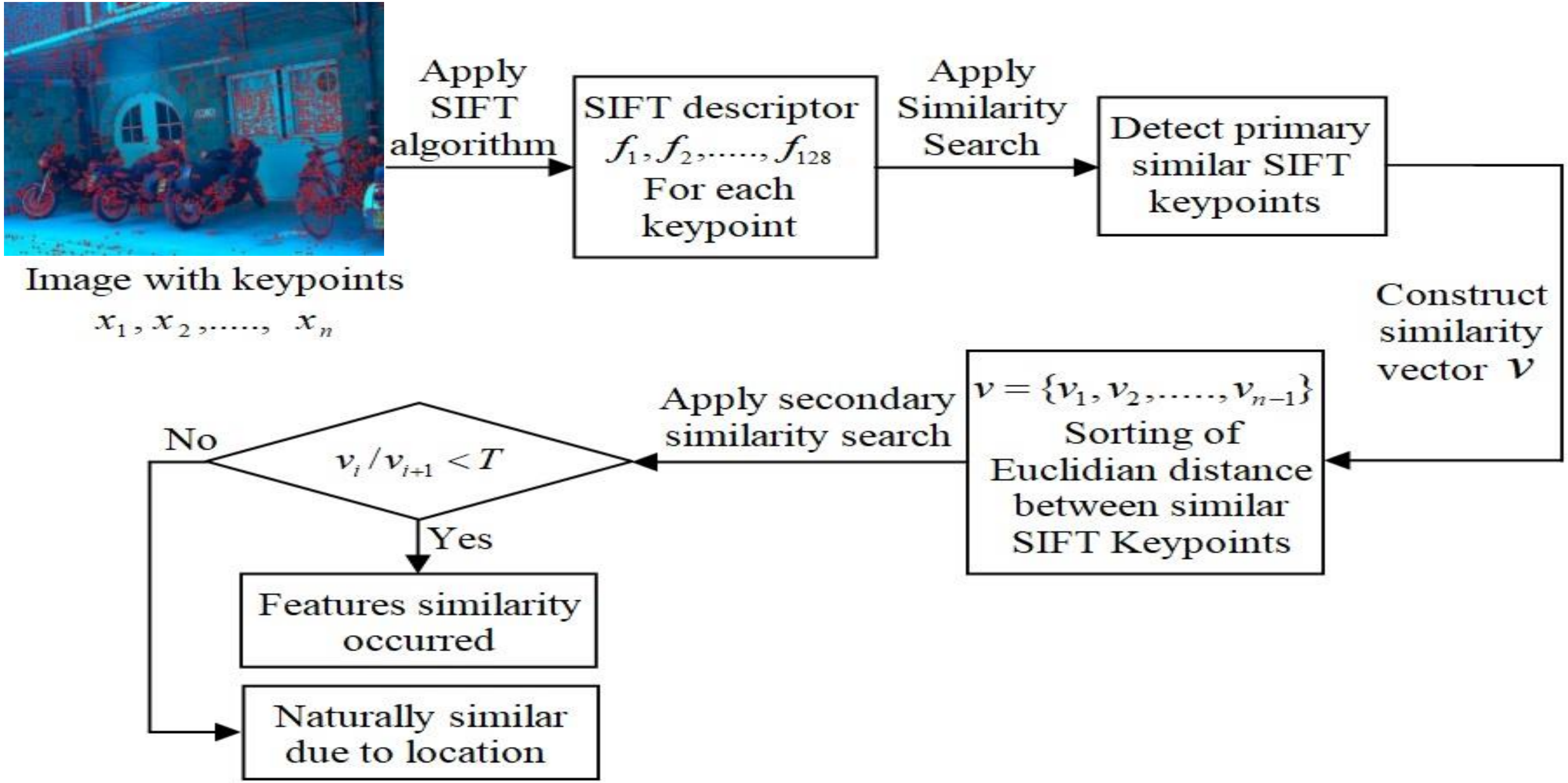
Using

- Homography Function.



Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Extracting SIFT features, mapping and matching



Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:
  - Datasets:

The proposed algorithm is using the most famous four datasets MICC-F220 [25], MICC-F2000[25], MICC-F600 [26], and SATS-130 [27].

Dataset	Composition	Size of Images	Size of Forged Region
MICC-F220	Consisted of 220 images divided into 110 tampered images and 110 originals.	Between 722 × 480 and 800 × 600 pixels	The forged region represents 1.2% of the whole image.
MICC-F2000	Consisted of 2000 images divided into700 tampered images and1300 originals.	2048 × 1536 pixels	The forged region represents 1.12% of the whole image.
MICC-F600	Consisted of 600 images divided into 152 tampered images and 448 originals.	Between 800 × 532 and 3888 × 2592 pixels	The forged regions sizes are varied from one image to another.
SATs-130	Consisted of 96 images divided into 48 tampered images and 48 originals.	Between 1024 × 683 and 3264 × 2448 pixels	The forged regions sizes are varied from one image to another.







Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:
  - Datasets:

Ten different combinations of geometric transformations applied to the original patch for the MICC-F220 dataset [25]

Attack	θ °	s_x	s_y
A	0	1	1
B	10	1	1
C	20	1	1
D	30	1	1
E	40	1	1

Attack	θ °	s_x	s_y
F	0	1.2	1.2
G	0	1.3	1.3
H	0	1.4	1.2
I	10	1.2	1.2
J	20	1.4	1.2

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:
  - Datasets:

Fourteen different combinations of geometric transformations applied to the original patch for the MICC-F2000 dataset [25]

Attack	θ °	s_x	s_y
a	0	1	1
b	0	0.5	0.5
c	0	0.7	0.7
d	0	1.2	1.2
e	0	1.6	1.6
f	0	2	2
g	0	1.6	1.2

Attack	θ °	s_x	s_y
h	0	1.2	1.6
i	5	1	1
j	30	1	1
l	70	1	1
m	90	1	1
n	40	1.1	1.6
o	30	0.7	0.9

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:
  - Datasets:

For dataset MICC-F600, 448 original image and 152the forged images

38 images	Forged by copying one patched region, apply transition, and then move.
38 images	Forged by copying two or three patched regions, apply transition, and then move.
38 images	Forged by copying one patched region, rotated by 30 degrees, and then move.
38 images	Forged by copying one patched region, rotated by 30 degrees, scale by 120%, and then move.

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:

➢ Testing Metrics:

$$TPR = \frac{T_P}{(T_P + F_N)} = (1 - FNR)$$

$$FPR = \frac{F_P}{(F_P + T_N)} = (1 - TNR)$$

$$FNR = \frac{F_N}{(F_N + Tp)}$$

$$TNR = \frac{T_N}{(T_N + F_P)}$$

➢ True Positive (T_P)
➢ False Positive (F_P)
➢ False Negative (F_N)
➢ True Negative (T_N)

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Experimental Results:

A) Metric parameters values after applying **high-pass filter** and applying SIFT algorithm & forgery detection

	MICC-F220	MICC-F600	MICC-F2000	SATS-130
TPR %	99.09	89.24	95.1	76.2
FPR %	9.01	7.13	7.2	11.33
TNR %	90.99	92.87	92.8	88.67
FNR %	0.91	10.76	4.9	23.8

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

B) Metric parameters values after applying **low-pass Gaussian filter** and applying SIFT algorithm & forgery detection with variable values of cutoff frequency

	MICC-F220				MICC-F600			
	TPR %	**FPR %**	**TNR %**	**FNR %**	**TPR %**	**FPR %**	**TNR %**	**FNR %**
***fc*=160**	98.18	19.09	80.91	1.82	80.2	22.03	77.97	19.8
***fc*=180**	97.87	14.55	85.45	2.13	87.5	16.1	83.9	12.5
***fc*=200**	98.18	19.09	80.91	1.82	85.1	18.02	81.98	14.9
***fc*=220**	96.01	13.55	86.45	3.99	82.7	20.13	79.87	17.3

	MICC-F2000				SATS-130			
	TPR %	**FPR %**	**TNR %**	**FNR %**	**TPR %**	**FPR %**	**TNR %**	**FNR %**
***fc*=160**	89.3	17.6	82.4	10.7	71.73	16.83	83.17	28.27
***fc*=180**	94.8	12.1	87.9	5.2	79.32	27.51	8473.	20.68
***fc*=200**	91.2	16.1	83.9	8.8	74.8	14.2	85.8	25.11
***fc*=220**	87.2	21.01	78.99	12.8	72.3	11.75	88.25	27.7

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

C) Metric parameter values from applying Butterworth low pass filter and applying SIFT algorithm & forgery detection with different values of cutoff frequency

	MICC-F220				MICC-F600			
	TPR %	FPR %	TNR %	FNR %	TPR %	FPR %	TNR %	FNR %
fc=160	99.09	13.64	86.36	0.91	79.38	9.35	90.64	20.62
fc=180	100	5.05	94.95	0	85.5	2.7	97.3	14.5
fc=200	99.09	9.09	90.91	0.91	88.75	12.68	87.32	11.25
fc=220	95.45	4.54	95.46	4.55	86.25	16.18	83.82	13.75
	MICC-F2000				**SATS-130**			
	TPR %	FPR %	TNR %	FNR %	TPR %	FPR %	TNR %	FNR %
fc=160	94.9	12.11	87.89	5.1	76.2	21.31	78.69	23.8
fc=180	96.71	8.76	91.24	3.29	81.25	20.83	79.17	18.75
fc=200	94.95	11.15	88.85	8.05	79.17	16.67	83.33	20.83
fc=220	91.3	17.87	82.13	8.7	79.17	21.75	78.25	20.83

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

D) Metric parameter values after applying high pass filter first then applying Butterworth low pass filter with different values of cutoff frequencies and complete SIFT algorithm & forgery detection

	MICC-F220				MICC-F600			
	TPR %	**FPR %**	**TNR %**	**FNR %**	**TPR %**	**FPR %**	**TNR %**	**FNR %**
***fc*=160**	94.30	10.73	89.27	5.7	81.13	12.15	87.85	18.87
***fc*=180**	100	4.54	95.46	0.02	87.76	5.63	94.37	12.24
***fc*=200**	97.27	6.36	93.64	2.73	91.49	9.37	90.63	8.52
***fc*=220**	99.09	8.18	91.82	0.91	89.64	10.2	89.8	10.36
	MICC-F2000				**SATS-130**			
	TPR %	**FPR %**	**TNR %**	**FNR %**	**TPR %**	**FPR %**	**TNR %**	**FNR %**
***fc*=160**	95.2	11.83	88.17	4.8	77.53	20.15	79.85	22.47
***fc*=180**	97.18	7.65	92.35	2.82	83.18	16.72	83.28	16.82
***fc*=200**	95.29	10.89	89.11	4.71	80.27	15.86	84.14	19.73
***fc*=220**	94.13	14.76	85.24	5.87	80.39	20.57	79.43	19.61

Enhanced Filter-based SIFT Approach for CMFD

Comparison between the proposal and traditional methods results

	MICC-F220				MICC-F600			
	TPR %	FPR %	TNR %	FNR %	TPR %	FPR %	TNR %	FNR %
The proposal	100	4.54	95.46	0	91.49	9.37	90.63	8.52
Amerini et al. [22]	100	8	92	0	69.2	12.5	87.5	30.8
Amerini et al. [23]	N/A	N/A	N/A	N/A	81.6	7.27	92.73	18.4
Christlein et al. [24]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	MICC-F2000				**SATS-130**			
	TPR %	**FPR %**	**TNR %**	**FNR %**	**TPR %**	**FPR %**	**TNR %**	**FNR %**
The proposal	97.18	7.65	92.35	2.82	83.18	16.72	83.28	16.82
Amerini et al. [22]	93.42	11.61	88.39	6.58	N/A	N/A	N/A	N/A
Amerini et al. [23]	94.86	9.15	90.85	5.14	N/A	N/A	N/A	N/A
Christlein et al. [24]	N/A	N/A	N/A	N/A	79.17	11.63	88.37	20.83

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

Comparison between the proposed method and Amerini et al. [25] performance against different values of JPEG compression

JPEG Quality Factor	The proposal		Amerini et al. [25]	
	TPR%	FPR%	TPR%	FPR%
100	97.18	7.65	93.42	11.61
75	97.15	7.65	93.72	12.07
50	97.09	7.47	93.16	11.15
40	97.83	7.30	92.14	11.13
20	97.31	6.89	87.15	10.46

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

Comparison between the proposed method and Amerini et al. [25] performance against values of Gaussian noise SNR (db) applied on whole images

SNR (db)	The proposal		Amerini et al. [22]	
	TPR%	FPR%	TPR%	FPR%
50	97.18	7.65	93.71	11.46
40	97.15	7.65	94.14	11.69
30	95.37	7.21	92.00	11.46
20	93.13	6.78	82.42	8.15

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Combined Attacks Tests
  - Gaussian noise adding with SNR = 50, and then Gamma correction with value 0.7.
  - Gaussian noise adding with SNR = 50, and then JPEG compression with quality 50.
  - Gamma correction with value 0.7, and then JPEG compression with quality 50.
  - Gaussian noise with SNR = 50, then Gamma correction with value 0.7, and then JPEG compression with quality 50.

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

- Combined Attacks Tests

Geometric transformations that can be applied sequentially on the tampered patched areas before pasting to the original images

Attack No.	Θ	s_x	s_y	Attack No.	Θ	s_x	s_y
1	0	1	1	7	5	1	1
2	0	0.5	0.5	8	20	1	1
3	0	0.7	0.7	9	30	1	1
4	0	1.2	1.2	10	50	1	1
5	0	1.6	1.6	11	70	1	1
6	0	2	2	12	90	1.5	1.5

Enhanced Filter-based SIFT Approach for CMFD (First algorithm)

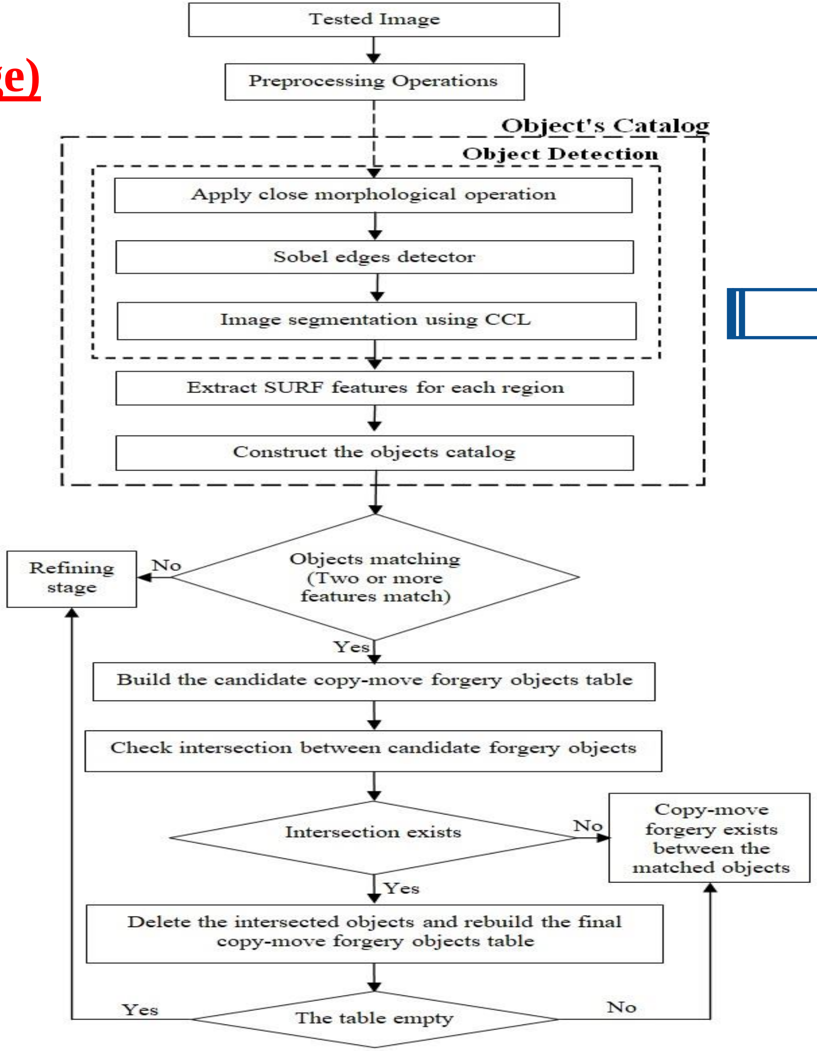
Comparison between the proposed method and Amerini et al. [25] performance against different types of combined attacks applied on patched areas only

Combined Attack Type	Algorithm	TPR%	FPR%
Gaussian Noise with Gamma correction attack	Amerini et al. [25]	85.71	14.29
	The Proposal	100	7.14
Gaussian Noise with JPEG compression attack	Amerini et al. [25]	86.75	14.80
	The Proposal	95.06	18.30
Gamma correction with JPEG compression attack	Amerini et al. [25]	87.5	12.4
	The Proposal	93.5	14.1
Gaussian Noise with Gamma correction with JPEG compression attack	Amerini et al. [25]	87.5	12.4
	The Proposal	91.3	14.1

Two Stages Object Recognition Based CMFD Algorithm (Second Algorithm)

- We developed a two stages CMFD approach:
  - ➢ The first stage is responsible for detecting the copy-move forged images and the images that candidate to be original (Matching Stage).
  - ➢ The second stage is applied on the candidate categorized to be original image, either to ensure their integrity or to detect a copy-move forgery within this candidate (Refine Matching Stage).

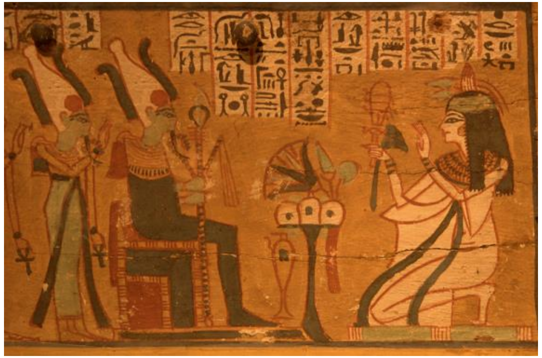
First Stage (Matching Stage)



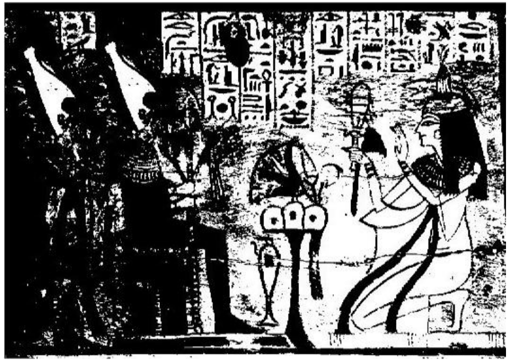
Object Catalog

Object No.	Object four corner points	SURF features
Object 1	$(x_1, y_1), (x_1, y_2),$ $(x_2, y_1), (x_2, y_2)$	Object 1 SURF features
Object 2	$(x_1, y_1), (x_1, y_2),$ $(x_2, y_1), (x_2, y_2)$	Object 2 SURF features
. . .	. . .	. . .
Object n	$(x_1, y_1), (x_1, y_2),$ $(x_2, y_1), (x_2, y_2)$	Object n SURF features

Tested Image

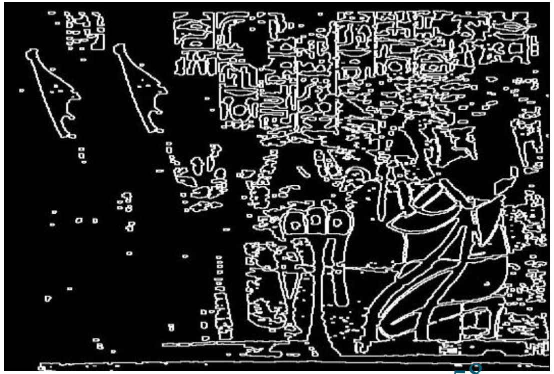


Binary Image

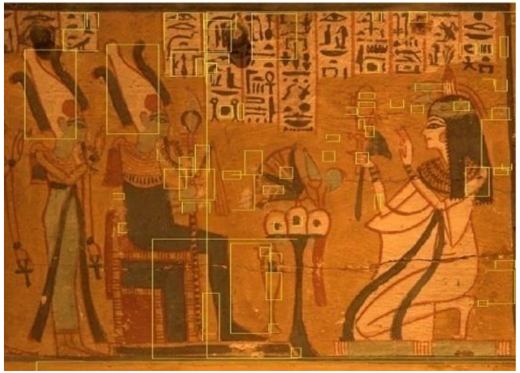


Closed morphological image

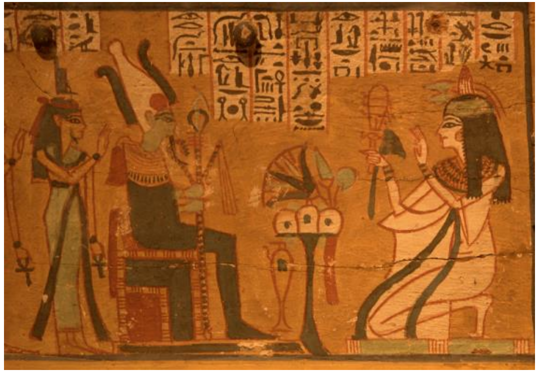
Edge detected image



Objects localization image



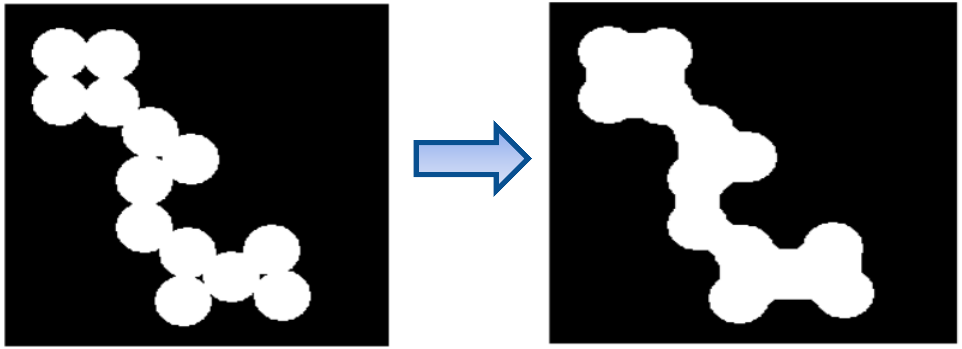
Original image



Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- **Object Detection:**

A) close morphological operation:



- Removes small holes resulted from projections and connects small cracks in its boundaries.
- Exhibits object outlines by growing the foreground pixels and detect boundaries or contours of that object.
- Shrinks the background holes or points belonging to these regions for the distinctness of region’s borders.

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- **Object detection:**

A) <u>close morphological operation</u>:

VS

Close Morphological operation

Open Morphological operation

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- **Object detection:**

B) Edge detection:

- Using Sobel operator
  - Noise reduction
  - Edge enhancement
  - Edge localization

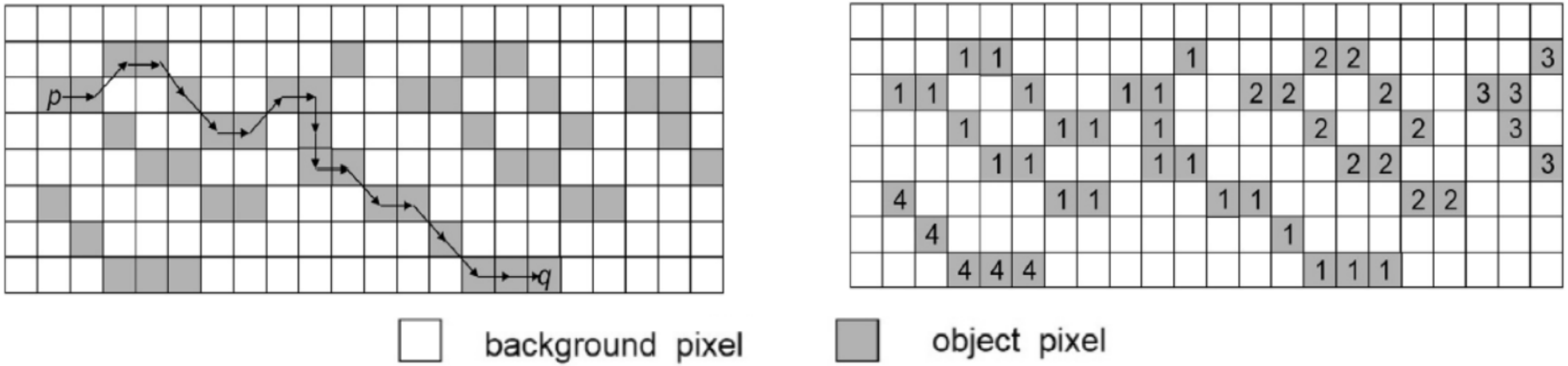
Other types that we trying:

1) Canny operator. 2) Roberts operators. 3) Prewitt operator. 4) Laplacian operator.

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

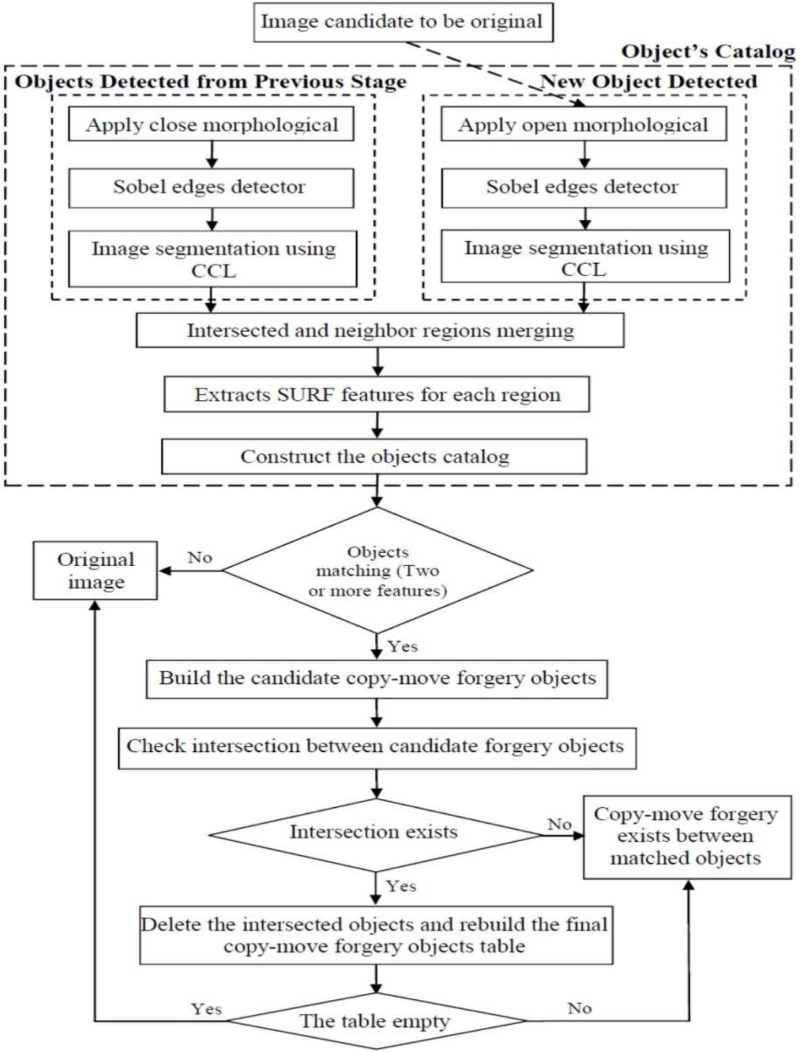
- **Object Detection:**

C) Image segmentation:



➢Scanning the edge detected, pixel by pixel, from top to bottom and left to right to find the connected pixel regions based on blobs.
➢Each pixel takes a label, being either foreground or background, according to its intensity value.
➢After assigning each pixel to a specific foreground object or a background region, objects bounding boxes are created.

Second Stage
(Refine Matching Stage)



Candidate original image and categorized as forgery image after refine matching stage

Image candidate to be original from matching stage

Binary Image

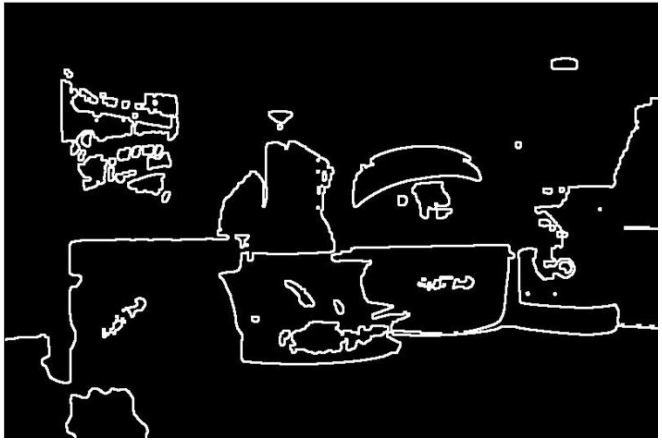
Candidate original image and categorized as forgery image after refine matching stage

Closed morphological image

Opened morphological image

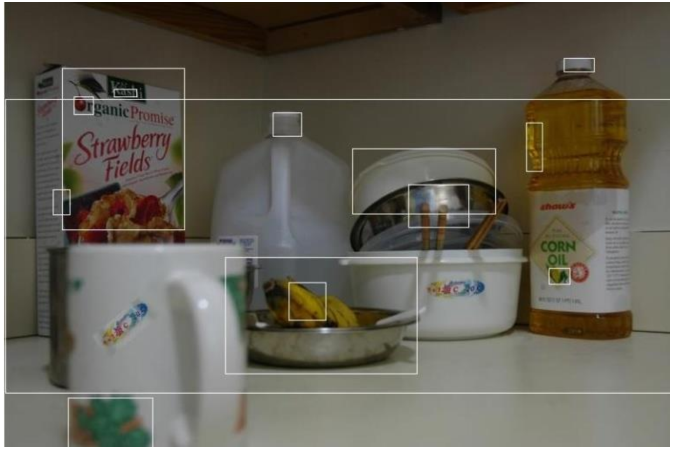
Edge detected image

Edge detected image

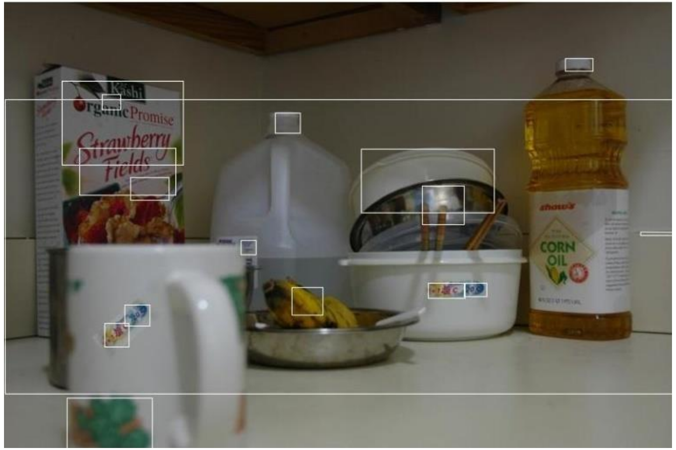


Candidate original image and categorized as forgery image after refine matching stage

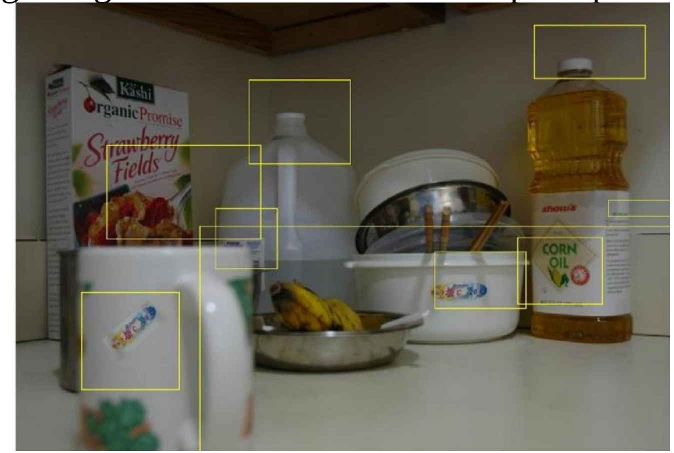
Regions resulted



Regions resulted



Merged regions from both close and open operations



Candidate original image and categorized as forgery image after refine matching stage

Original image

Candidate original image and categorized as original image again after refine matching stage

Image candidate to be original from matching stage

Binary Image

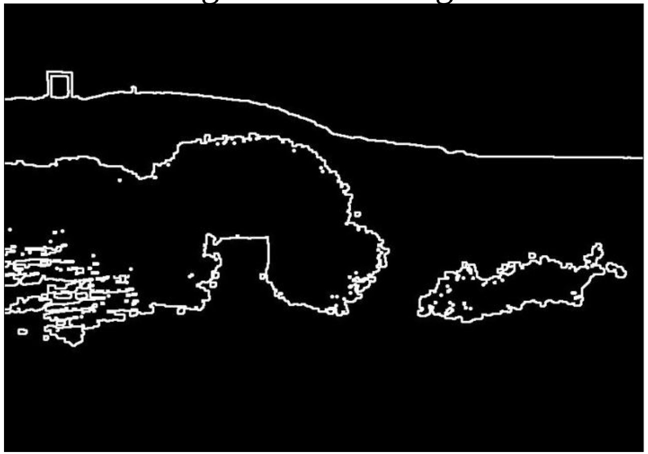
Candidate original image and categorized as original image again after refine matching stage

Closed morphological image

Opened morphological image

Edge detected image

Edge detected image

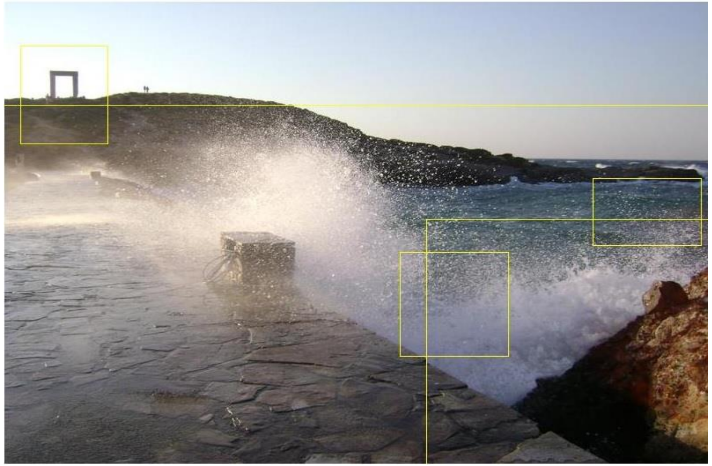


Candidate original image and categorized as original image again after refine matching stage

Regions resulted

Regions resulted

Merged regions from both close and open operations



Candidate original image and categorized as original image again after refine matching stage

Original image

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:
  - Datasets:

Dataset	Composition	Size of Images	Size of Forged Region
MICC-F220	Consisted of 220 images divided into 110 tampered images and 110 originals.	Between 722 × 480 and 800 × 600 pixels	The forged region represents 1.2% of the whole image.
MICC-F2000	Consisted of 2000 images divided into700 tampered images and1300 originals.	2048 × 1536 pixels	The forged region represents 1.12% of the whole image.
MICC-F600	Consisted of 600 images divided into 152 tampered images and 448 originals.	Between 800 × 532 and 3888 × 2592 pixels	The forged regions sizes are varied from one image to another.
SATs-130	Consisted of 96 images divided into 48 tampered images and 48 originals.	Between 1024 × 683 and 3264 × 2448 pixels	The forged regions sizes are varied from one image to another.

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Testing Metrics:

$$TPR = \frac{T_P}{(T_P + F_N)} = (1 - FNR)$$

$$FPR = \frac{F_P}{(F_P + T_N)} = (1 - TNR)$$

$$FNR = \frac{F_N}{(F_N + Tp)}$$

$$TNR = \frac{T_N}{(T_N + F_P)}$$

$$ACC = \frac{(T_N + T_{P)}}{(T_P + F_P + T_N + F_N)} \times 100$$

$$MCC = \frac{(T_P \times T_N) - (F_P \times F_N)}{\sqrt{((T_P + F_{P)} \times (T_P + F_N) \times (T_N + F_P) \times (T_N + F_N))}} \times 100$$

CT = Computational Time

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➢ Results of applying the proposed matching stage only

Datasets / Metrics	MICC-F220	MICC-F2000	MICC-F600	SATS-130
TPR	89.09%	87.40%	82.34%	80.47%
FPR	8.18%	12.35%	29.09%	21.28%
FNR	10.91	12.6%	17.66%	19.53%
TNR	91.82%	87.35%	70.91%	78.72%
ACC	90.45%	84.23%	70.79	69.89%
MCC	80.94%	72.34%	58.18%	56.26%
CT (mm:ss)	2:12	30:58	14:30	3:20

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

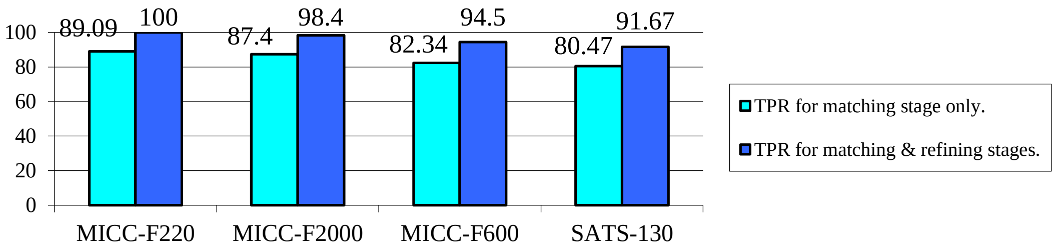
➢ Results of applying the proposed two-stage CMFD algorithm

Datasets / Metrics	MICC-F220	MICC-F2000	MICC-F600	SATS-130
TPR	100%	98.40%	94.50%	91.67%
FPR	1.80%	6.35%	11.35%	20.83%
FNR	0%	1.60%	5.50%	8.33%
TNR	98.20%	93.65%	88.65%	79.17%
ACC	99.09%	93.55%	91.05%	85.42%
MCC	98.20%	83.39%	80.79%	71.39%
CT (mm:ss)	2:48	46:58	17:37	7:24

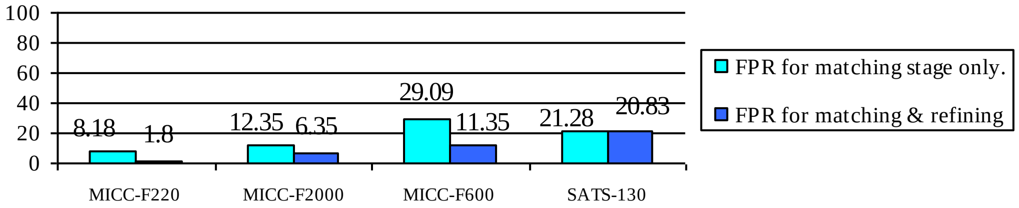
Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➢ TPR values for matching stage only Vs. TPR values for matching & refining stages.



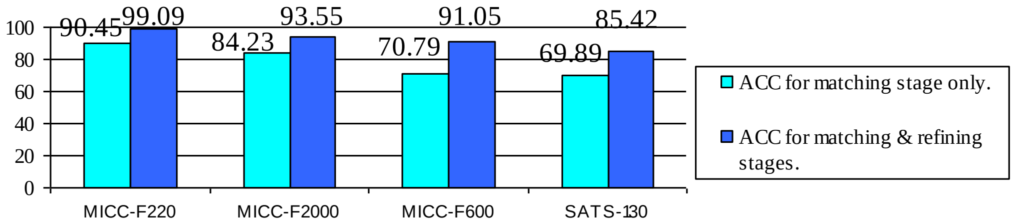
➢ FPR values for matching stage only Vs. FPR values for matching & refining stages.



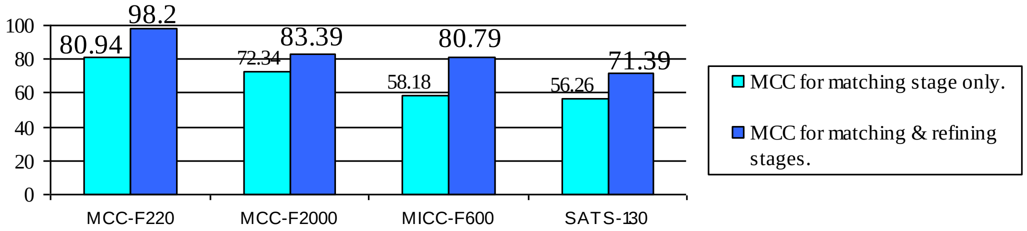
Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➤ ACC values for matching stage only Vs. ACC values for matching & refining stages.



➤ MCC values for matching stage only Vs. MCC values for matching & refining stages.



Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➢ Comparison between proposed algorithm and previously reported methods on MICC-F220.

	The Proposed Algorithm	Amerini et al. [25]	Amerini et al. [26]	Mishra et al. [28]	Kaur et al. [29]
TPR	100 %	100 %	100%	73.64 %	97.27 %
FPR	1.80%	8%	6%	3.64 %	7.27 %
FNR	0%	0%	0%	26.36 %	2.73 %
TNR	98.20%	92%	94%	96.36 %	92.73 %
CT (mm:ss)	2:48	24:13	17:05	0:2.85	N/A

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➢ Comparison between proposed algorithm and previously reported methods on MICC-F2000 dataset.

	The Proposed Algorithm	Amerini et al. [25]	Amerini et al. [26]
TPR	98.40 %	93.42 %	94.86 %
FPR	6.35 %	11.61 %	9.15 %
FNR	1.60 %	6.58 %	5.14 %
TNR	93.65 %	88.39 %	90.85 %
CT (mm:ss)	46:58	312:18	180:15

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:
  - Comparison between proposed algorithm and previously reported methods on MICC-F600 dataset.

	The Proposed Algorithm	Amerini et al. [25]	Amerini et al. [26]
TPR	94.50 %	69.20 %	81.60 %
FPR	11.35 %	12.50 %	7.27 %
FNR	5.50 %	30.80 %	18.40 %
TNR	88.65 %	87.50 %	92.73 %
CT (mm:ss)	17:37	115:00	76:21

Two Stages Object Recognition Based CMFD Algorithm (Second algorithm)

- Experimental Results:

➢ Comparison between proposed algorithm and previously reported methods on SATS-130 dataset.

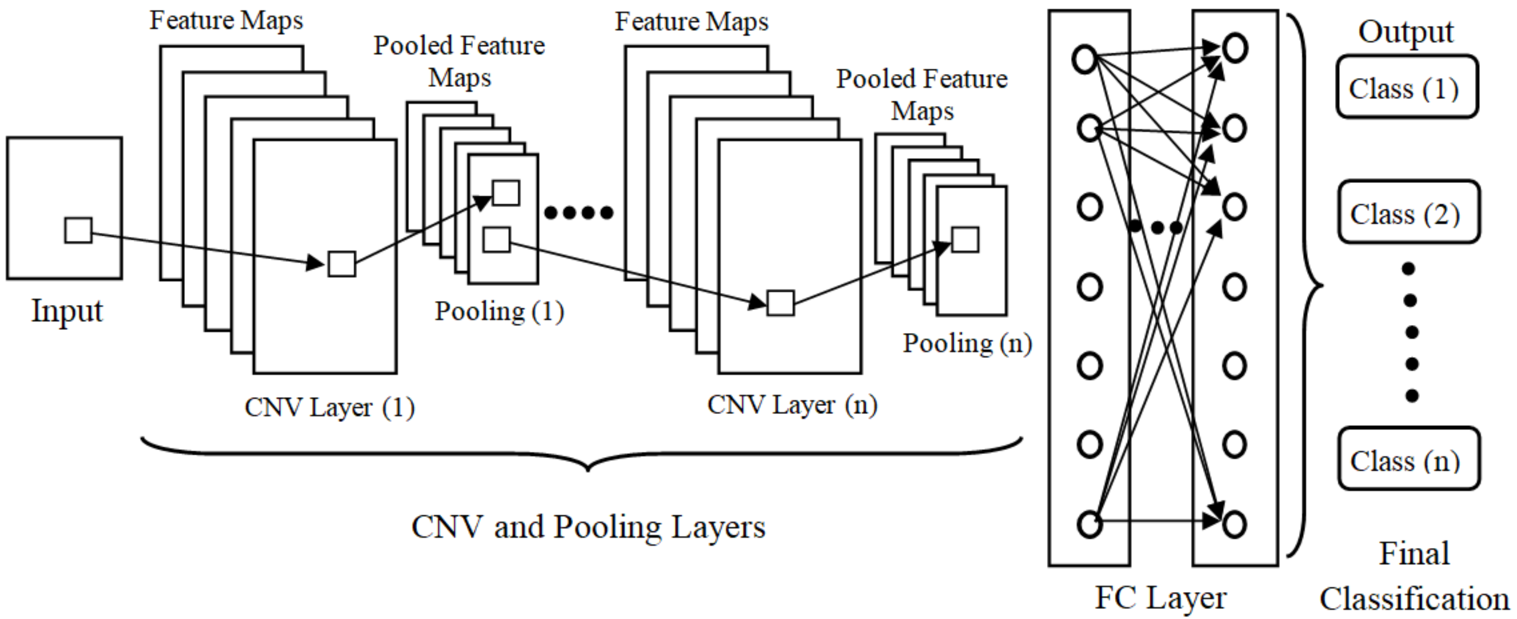
	The Proposed Algorithm	Amerini et al. [25]	Christlein et al. [27]	Amerini et al. [26]
TPR	91.67 %	67.13 %	79.17 %	79.35 %
FPR	20.83 %	11.89 %	11.63 %	14.51 %
FNR	8.33 %	32.87 %	20.83 %	20.65 %
TNR	79.17 %	88.11 %	88.37 %	85.49 %
CT (mm:ss)	7:24	47:00	N/A	35:31

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Developing a novel deep learning framework for CMFD approach (develop a fast and efficient algorithm by:)
  1) Achieve higher performance
     - Increasing detection accuracy.
     - Decreasing the loss values or the misclassification values of CMFD.
  2) Speeding up the forgery detection process by decreasing the computational time and computational cost.

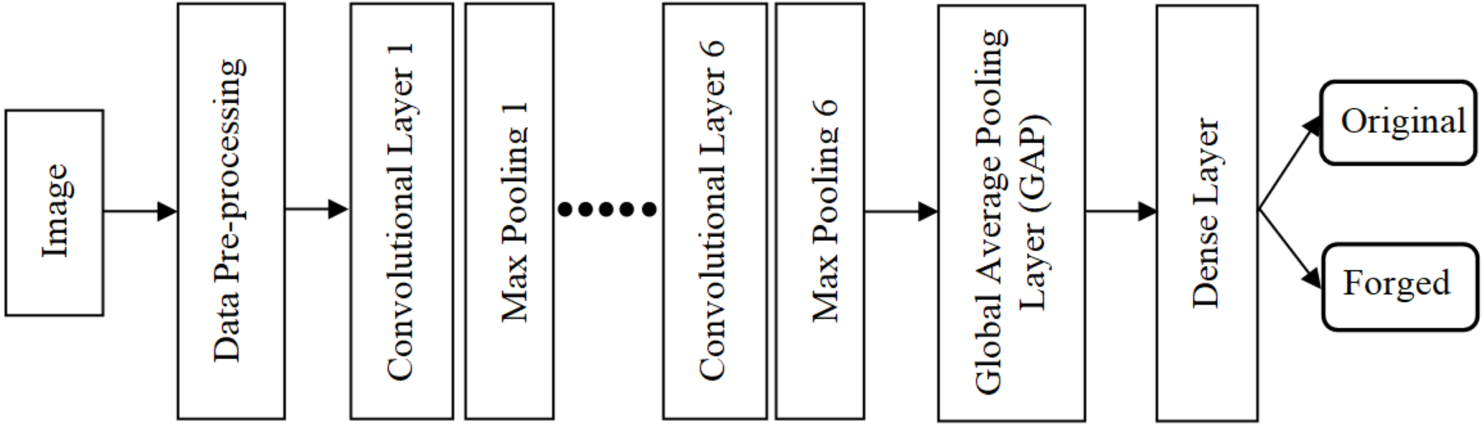
Building a high performance classification system using Convolutional Neural Network (CNN).

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The CNN structure.

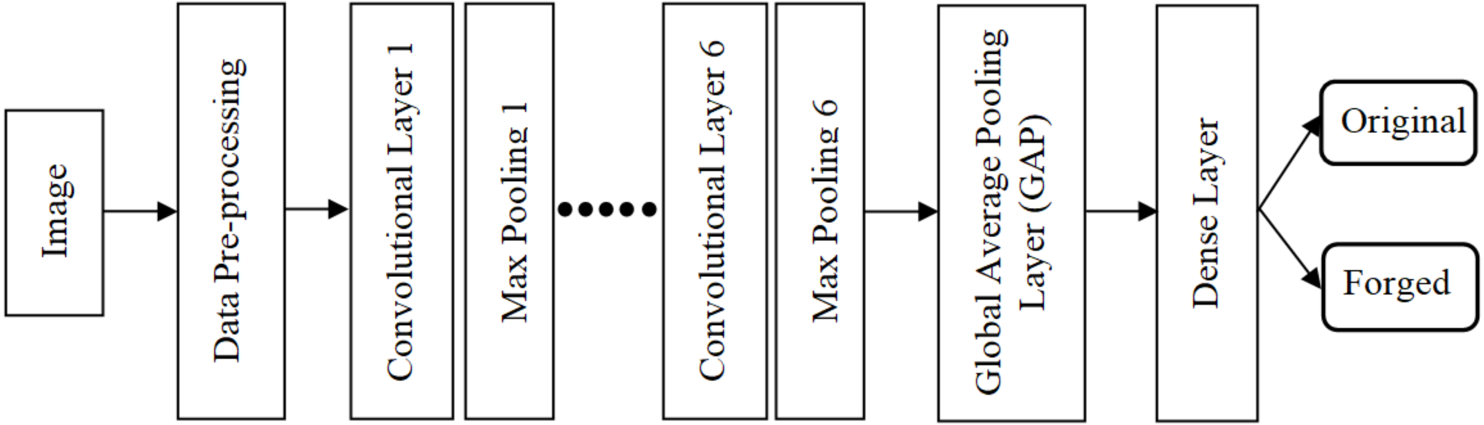
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The structure of the novel deep learning framework

- Deep CMFD system is presented in three phases: the pre-processing phase, the feature extraction phase, and the classification phase.

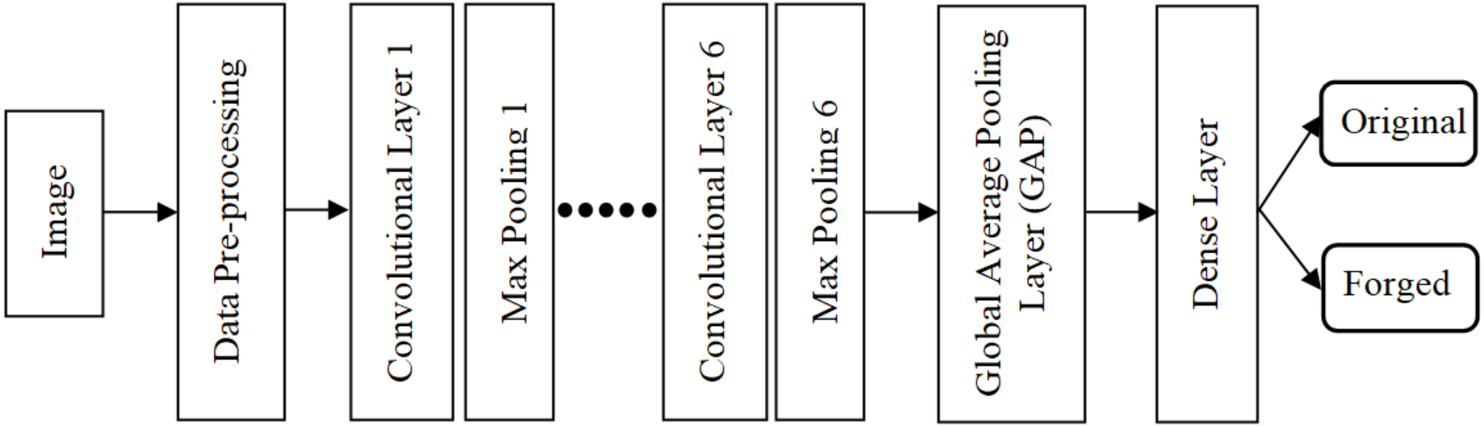
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The structure of the novel deep learning framework

- <u>Pre-processing stage:</u>
  - The input images are resized to the size that is specified in the input layer (input images is 224 × 224).

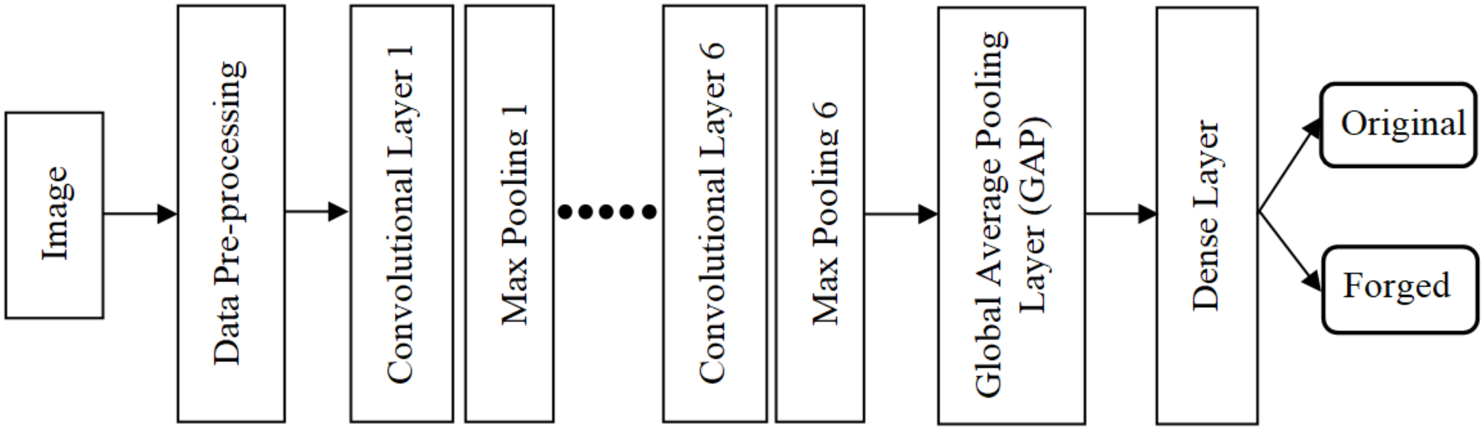
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The structure of the novel deep learning framework

- <u>The feature extraction stage:</u>
  - Consists of six Convolution (CNV) layers and each CNV layer is followed by a max pooling layer.

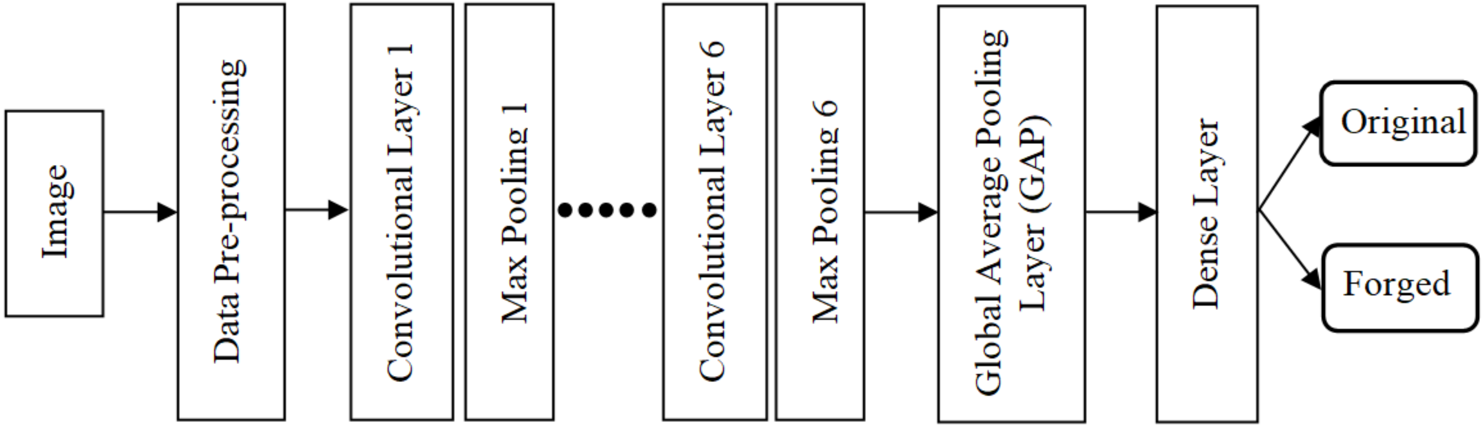
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The structure of the novel deep learning framework

- <u>Global Average Pooling Layer (GAP):</u>
  - Last max pooling layer output are vectorized and inserted into the GAP layer.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)



The structure of the novel deep learning framework

- <u>Dense layer:</u>
  - The GAP and Dense layers are used as a fully connected layer

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>The feature extraction stage:</u>
  - Consists of six Convolution (CNV) layers that its input parameters are arranged in 4 dimensions as:

[No. of samples, Input image width, Input image height, No. of filters used in each layer]

  - CNV layers act as features extractors [each CNV layer applies its specific number of filters and produces its feature maps].
  - No. of 2-D filters implemented for each layer are 16, 32, 64, 128, 256, and 512 for the CNV layers 1, 2, 3, 4, 5, and 6, respectively.
  - Max pooling layer produces a resized pooled feature maps which act as input to the next CNV layer.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- CNV and pooling layers summary

[No. of samples, Input image width, Input image height, No. of filters used in each layer]

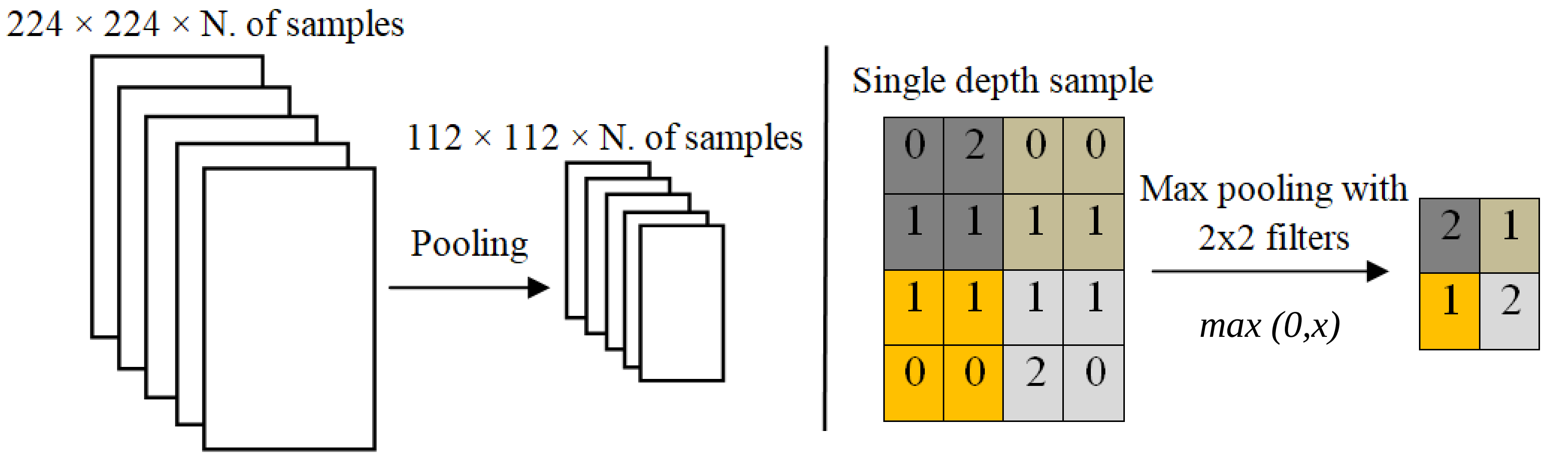
Pooling: removing some distortion edges in the input of the next layer.

Layer Type	Output Shape
CNV 1	(N. of samples, 224, 224, 16)
Pooling 1	(N. of samples, 112, 112, 16)
CNV 2	(N. of samples, 110, 110, 32)
Pooling 2	(N. of samples, 55, 55, 32)
CNV 3	(N. of samples, 53, 53, 64)
Pooling 3	(N. of samples, 26, 26, 64)
CNV 4	(N. of samples, 24, 24, 128)
Pooling 4	(N. of samples, 12, 12, 128)
CNV 5	(N. of samples, 10, 10, 256)
Pooling 5	(N. of samples, 5, 5, 256)
CNV 6	(N. of samples, 3, 3, 512)
Pooling 6	(N. of samples, 1, 1, 512)
Global Average Layer	(N. of samples, 512)
Dense	(N. of samples, 2)

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

➢ Max pooling layer:

- ➢ Produces a resized pooled feature maps which act as input to the next CNV layer.

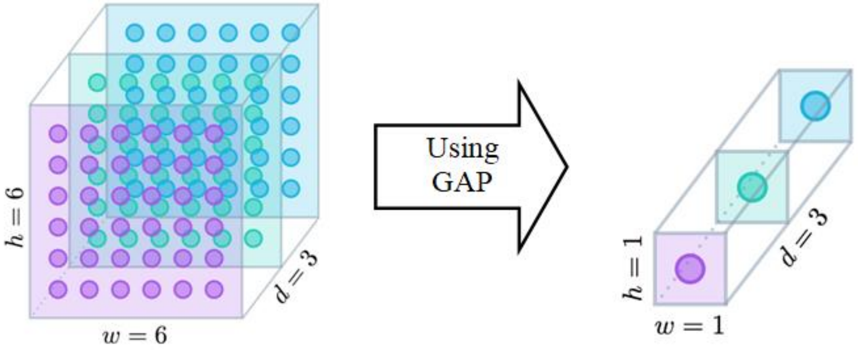


To reduce spatial information to 1) decreasing computational cost.
2) decrease chances of overfitting.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

GAP layer:

- Detecting correspondences between feature maps and demanded categories.
- Reduces overfitting probability by minimizing the total number of parameters utilized in the layer structure.
- Compatibility of data with the convolution structure.



A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Dense layer:
  - Used in the classification decision. The dense layer has a soft-max activation function and a class for each possible category (original or forged).
  - GAP layer and dense layer are used as fully connected layer.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - Datasets:

Dataset	Composition	Size of Images	Size of Forged Region
MICC-F220	Consisted of 220 images divided into 110 tampered images and 110 originals.	Between 722 × 480 and 800 × 600 pixels	The forged region represents 1.2% of the whole image.
MICC-F2000	Consisted of 2000 images divided into700 tampered images and1300 originals.	2048 × 1536 pixels	The forged region represents 1.12% of the whole image.
MICC-F600	Consisted of 600 images divided into 152 tampered images and 448 originals.	Between 800 × 532 and 3888 × 2592 pixels	The forged regions sizes are varied from one image to another.
SATs-130	Consisted of 96 images divided into 48 tampered images and 48 originals.	Between 1024 × 683 and 3264 × 2448 pixels	The forged regions sizes are varied from one image to another.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- **Experimental Results:**
  - <u>Datasets:</u>

✓ SATs-130 is a small dataset (96 images), thus training the CNN with such small dataset causes overfitting.

✓ we merged the four datasets (MICC-F220, MICC-F2000, MICC-F600, and SATs-130) to create an extensive dataset as a datasets combination to test SATs-130 dataset in between.

✓ The benefit of integrating various datasets extends beyond simply increasing the dataset size, to generalize the evaluation process of the proposed algorithm.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - Testing Metrics: In addition to Testing Time (*TT*)

$$TPR = \frac{T_P}{(T_P + F_N)} = (1 - FNR)$$

$$FPR = \frac{F_P}{(F_P + T_N)} = (1 - TNR)$$

$$FNR = \frac{F_N}{(F_N + Tp)}$$

$$TNR = \frac{T_N}{(T_N + F_P)}$$

$$ACC = \frac{(T_N + T_{P)}}{(T_P + F_P + T_N + F_N)} \times 100$$

$$LogLoss = 1 - ACC$$

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - <u>Evaluation Method:</u>

- Evaluated using the k-fold cross validation technique.
- Randomly dividing the dataset into (k) groups (folds) of approximately equal size. The proposed system is trained by (k-1) groups, and the remaining composes the test set.
- The learning process is repeated (k) times to achieve the diversity between the tested images and accomplish a strong evaluation by testing the datasets completely.

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

	Testing Folds (K-Folds) K=5				
Complete Dataset	**Fold 1**	**Fold 2**	**Fold 3**	**Fold 4**	**Fold 5**
	Testing	Training	Training	Training	Training
	Training	Testing	Training	Training	Training
	Training	Training	Testing	Training	Training
	Training	Training	Training	Testing	Training
	Training	Training	Training	Training	Testing

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - Results of performing the proposed algorithm on MICC-F220 dataset.

Metrics / No. of Epochs	Accuracy %	Log Loss %	*TPR %*	*FPR %*	*FNR %*	*TNR %*	*TT (sec)*
15 Epochs	92.18	7.82	86.67	Zero	13.33	100	16.43
25 Epochs	96.15	3.85	92.86	Zero	7.14	100	17.95
35 Epochs	97.62	2.38	95.45	Zero	4.55	100	15.29
50 Epochs	100	Zero	100	Zero	Zero	100	13.96
75 Epochs	100	Zero	100	Zero	Zero	100	14.63
100 Epochs	100	Zero	100	Zero%	Zero	100	17.76

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - The results of performing the proposed algorithm on MICC-F2000 dataset.

Metrics / No. of Epochs	Accuracy %	Log Loss %	*TPR %*	*FPR %*	*FNR %*	*TNR %*	*TT (sec)*
15 Epochs	92.16	7.84	93.18	9.72	6.82	90.28	108.4
25 Epochs	95.1	4.99	96.88	7.89	3.13	92.11	116.6
35 Epochs	98	2	97.73	1.39	2.27	98.61	119.4
50 Epochs	100	Zero	100	Zero	Zero	100	78.6
75 Epochs	100	Zero	100	Zero	Zero	100	93.8
100 Epochs	99.51	0.49	99.24	Zero	0.76	100	90.1

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - The results of performing the proposed algorithm on MICC-F600 dataset.

Metrics / No. of Epochs	Accuracy %	Log Loss %	*TPR %*	*FPR %*	*FNR %*	*TNR %*	*TT (sec)*
15 Epochs	92.1569	7.8431	90.91	5.56	9.09	94.44	32.41
25 Epochs	94.1176	5.8824	93.75	5.26	6.25	94.73	33.07
35 Epochs	96.0784	3.9216	96.77	5.00	3.23	95.00	32.30
50 Epochs	100	Zero	100	Zero	Zero	100	23.97
75 Epochs	100	Zero	100	Zero	Zero	100	25.75
100 Epochs	100	Zero	100	Zero	Zero	100	25.53

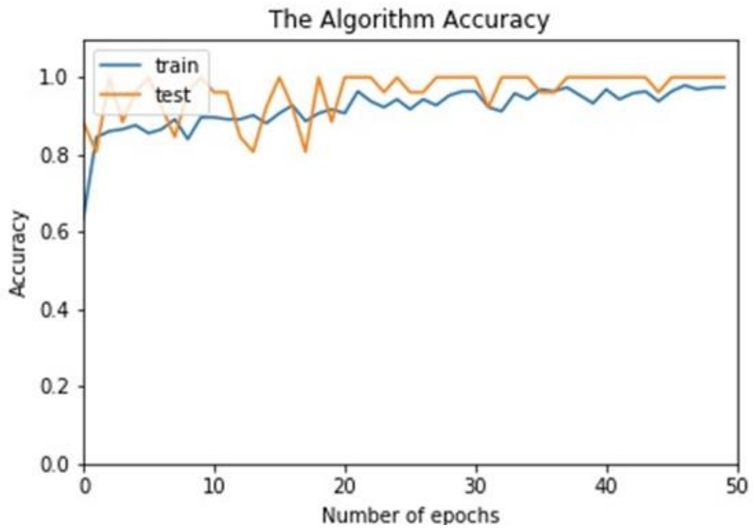
Enhanced Filter-based SIFT Approach for CMFD

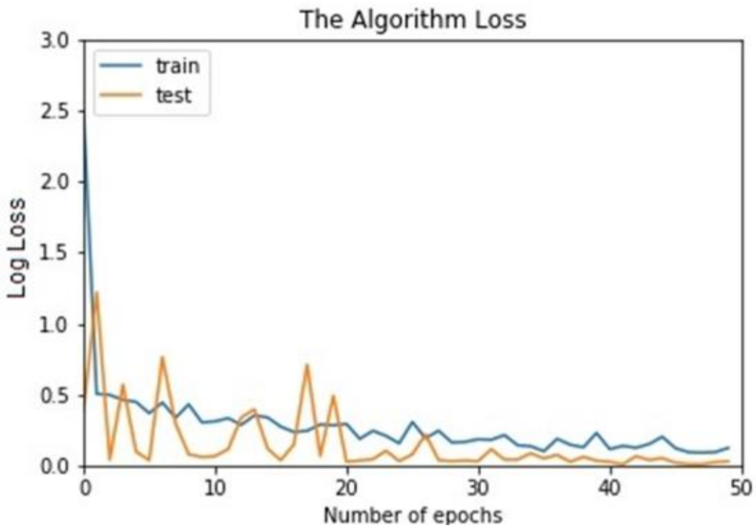
- <u>Experimental Results:</u>
  - The results of performing the proposed algorithm on datasets combination.

Metrics / No. of Epochs	Accuracy %	Log Loss %	*TPR %*	*FPR %*	*FNR %*	*TNR %*	*TT (sec)*
15 Epochs	93.57	6.43	94.20	7.04	5.80	92.96	112.82
25 Epochs	95.00	5.00	95.65	5.63	4.35	94.37	114.98
35 Epochs	97.86	2.14	100	4.11	Zero	95.89	117.73
50 Epochs	98.57	1.43	100	2.78	Zero	97.22	112.47
75 Epochs	100	Zero	100	Zero	Zero	100	110.1
100 Epochs	100	Zero	100	Zero	Zero	100	125.39

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

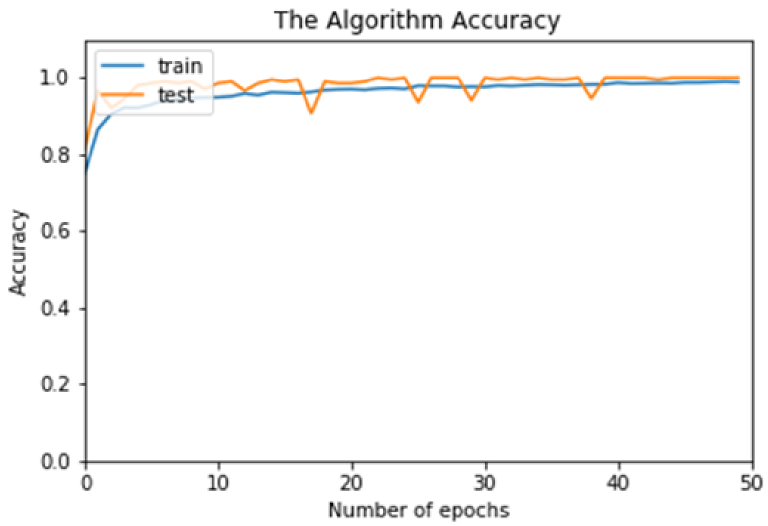
- <u>Experimental Results:</u>
  - The proposed algorithm accuracy & log loss for dataset MICC-F220 at No. of epochs equal to 50.

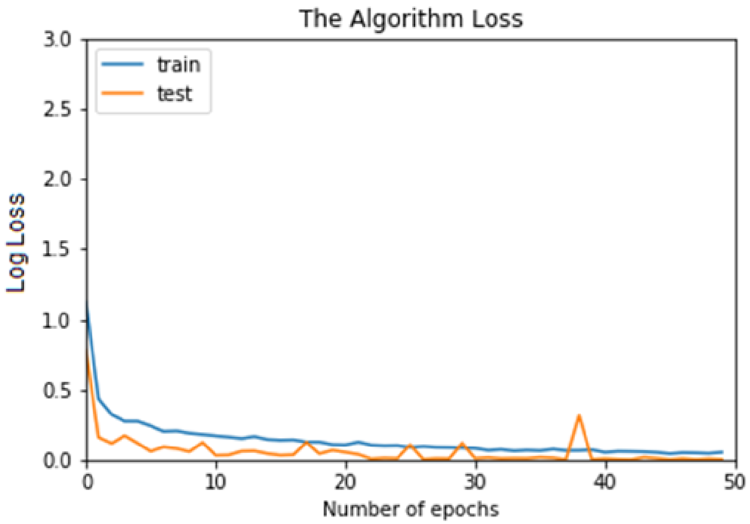




A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

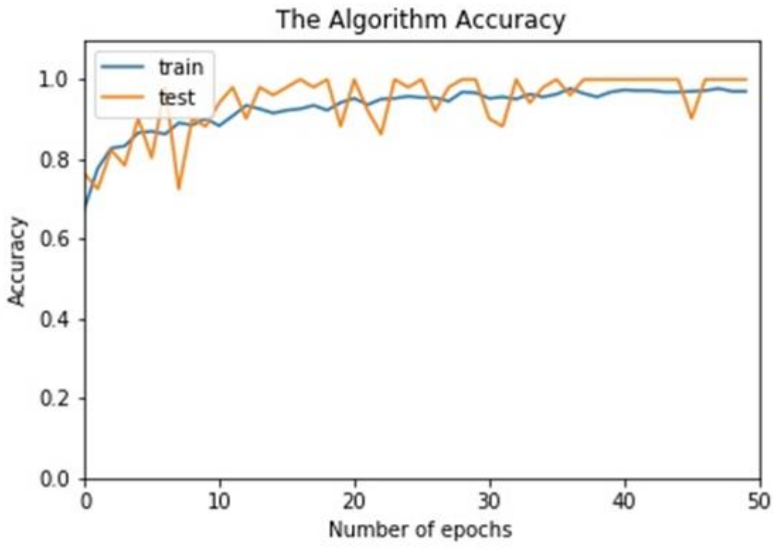
- <u>Experimental Results:</u>
  - ➢ The proposed algorithm accuracy & log loss for dataset MICC-F2000 at No. of epochs equal to 50.

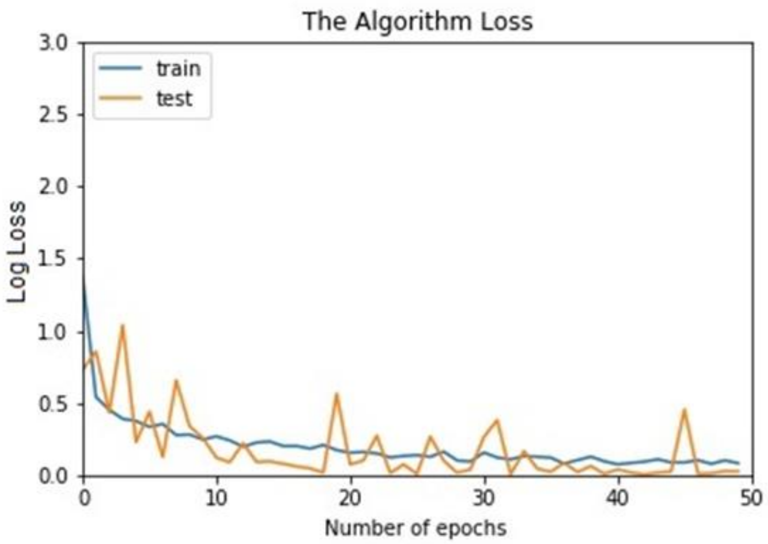




A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

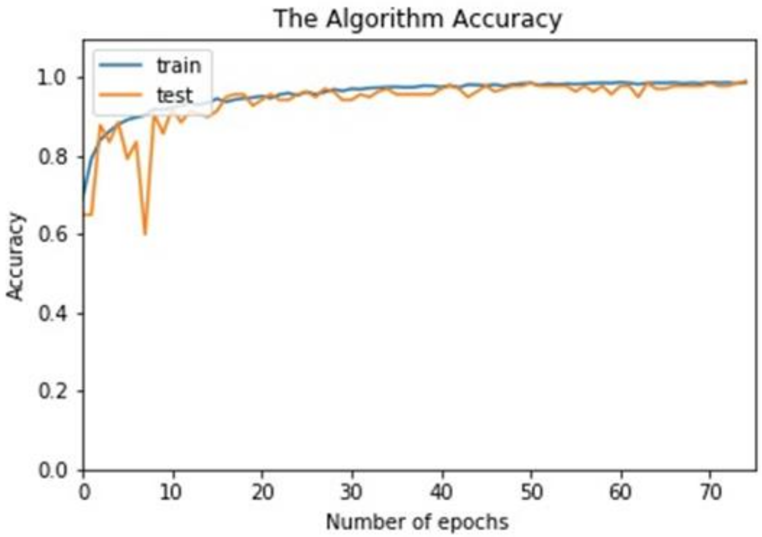
- <u>Experimental Results:</u>
  - The proposed algorithm accuracy & log loss for dataset MICC-F600 at No. of epochs equal to 50.

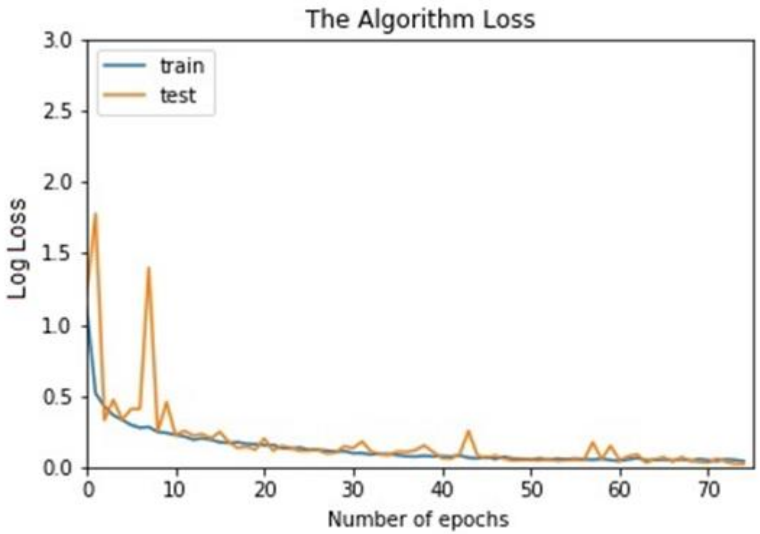




A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

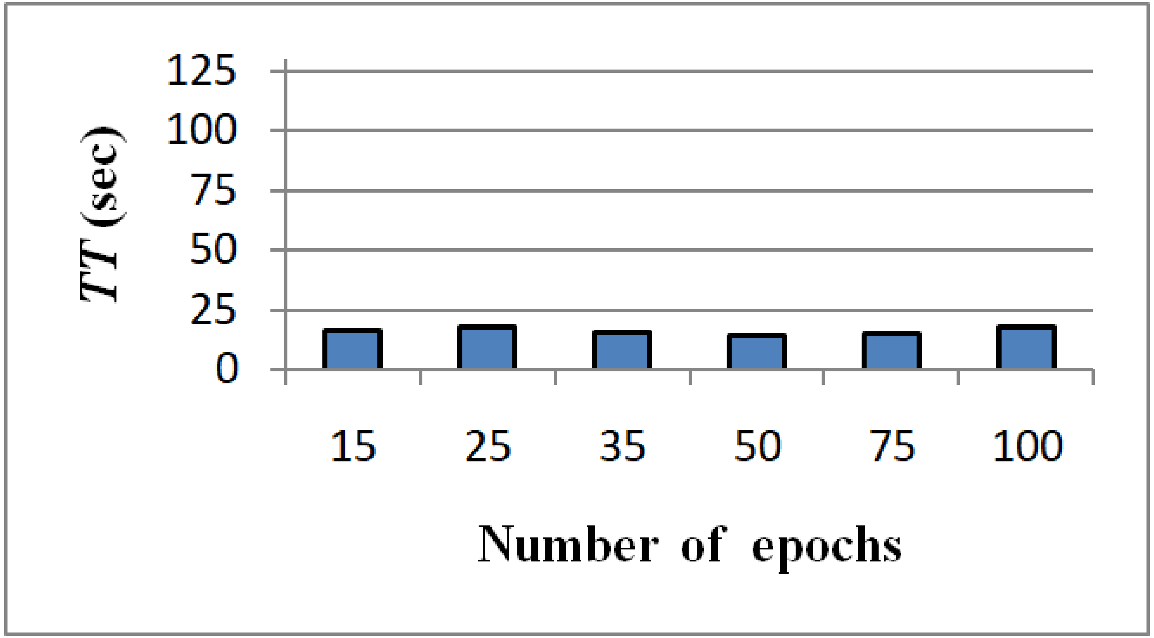
- <u>Experimental Results:</u>
  - The proposed algorithm accuracy & log loss for datasets combination at No. of epochs equal to 75.





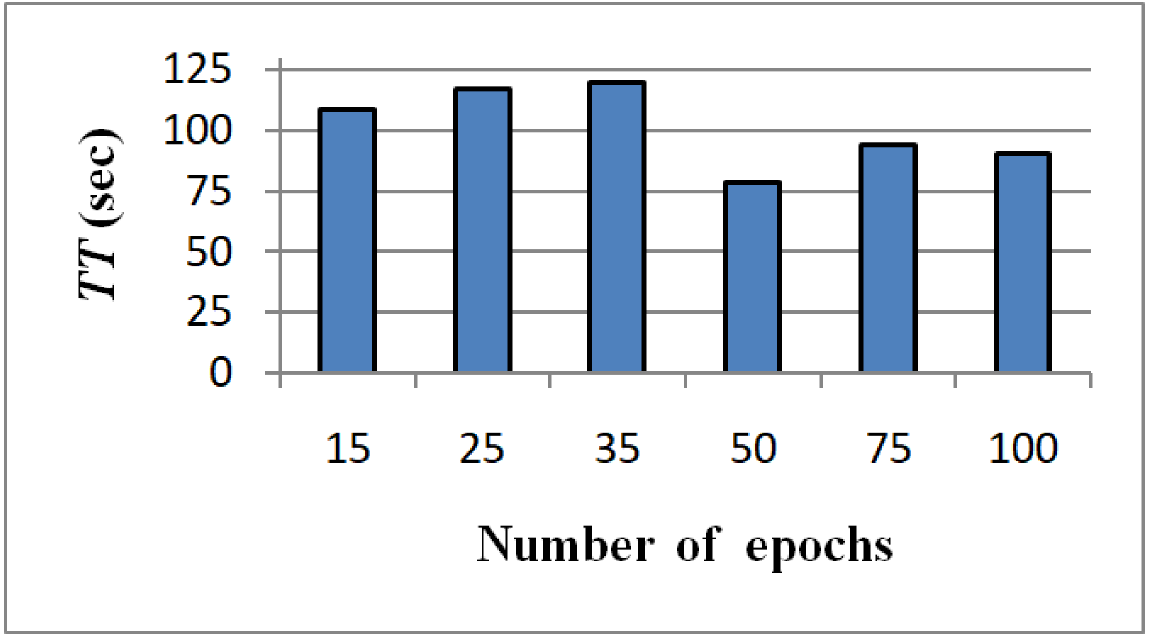
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - Number of epochs vs. *TT* for dataset MICC-F220.



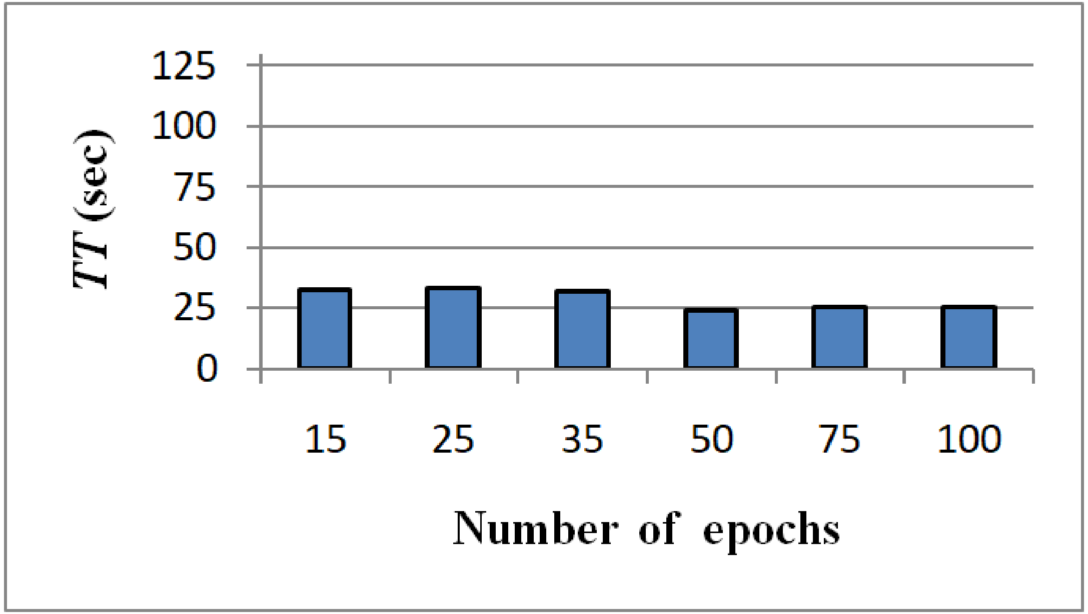
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - Number of epochs vs. *TT* for dataset MICC-F2000.



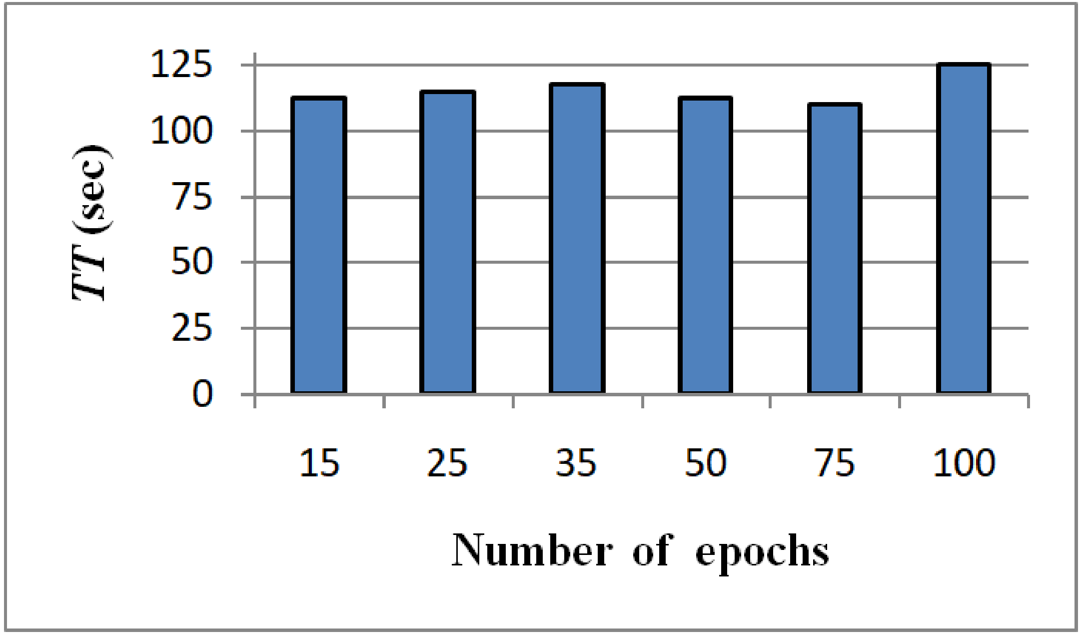
A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - ➢ Number of epochs vs. *TT* for dataset MICC-F600.



A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - ➢ Number of epochs vs. *TT* for datasets combination.



A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- Experimental Results:
  - Comparison between proposed algorithm and previously reported methods on MICC-F220 dataset.

	The Proposed Algorithm	Amerini et al. [22]	Amerini et al. [25]	Mishra et al. [30]	Kaur et al. [31]	Elaskily et al. [32]
TPR %	100	100	100	73.64	97.27	100
FPR %	Zero	8	6	3.64	7.27	1.80
FNR %	Zero	Zero	Zero	26.36	2.73	Zero
TNR %	100	92	94	96.36	92.73	98.20
TT (mm:ss)	0:14	24:13	17:05	0:2.85	N/A	2:48

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - Comparison between proposed algorithm and previously reported methods on MICC-F2000 dataset.

	The Proposed Algorithm	Amerini et al. [26]	Amerini et al. [25]	Elaskily et al. [32]
TPR %	100	93.42	94.86	98.40
FPR %	Zero	11.61	9.15	6.35
FNR %	Zero	6.58	5.14	1.60
TNR %	100	88.39	90.85	93.65
TT (mm:ss)	01:19	312:18	180:15	46:58

A Novel Deep Learning Framework for Copy-Move Forgery Detection (Third algorithm)

- <u>Experimental Results:</u>
  - ➢ Comparison between proposed algorithm and previously reported methods on MICC-F600 dataset.

	The Proposed Algorithm	Amerini et al. [22]	Amerini et al. [25]	Elaskily et al. [32]
TPR %	100	69.20	81.60	94.50
FPR %	Zero	12.50	7.27	11.35
FNR %	Zero	30.80	18.40	5.5
TNR %	100	87.50	92.73	88.65
TT (mm:ss)	0:24	115:00	76:21	17:37

Research Outputs

- Mohamed A. Elaskily, Heba K. Aslan, Fathi E. Abd El-Samie, Osama A. Elshakankiry, Osama S. Faragallah, Mohamed M. Dessouky, "Comparative Study of Copy-Move Forgery Detection Techniques", **Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & Intl Conf on New Paradigms in Electronics & Information Technology (PEIT),** Alexandria, Egypt, 2017.

- Mohamed A. Elaskily, Heba K. Aslan, Fathi E. Abd El-Samie, Osama A. Elshakankiry, Osama S. Faragallah, Mohamed M. Dessouky, "Performance Evaluation of Some Algorithms for Copy-Move Forgery Detection", **Journal of Electrical Systems and Information Technology, Elsevier**, accepted for publication.

- Mohamed A. Elaskily, Heba K. Aslan, Mohamed M. Dessouky, Fathi E. Abd El-Samie, Osama S. Faragallah, Osama A. Elshakankiry, "Enhanced Filter-based SIFT Approach for Copy-Move Forgery Detection", **Menoufia Journal of Electronic Engineering Research (MJEER),** Vol. 28, No. 1, Jan. 2019.

- Mohamed A. Elaskily, Heba A. Elnemr, Mohamed M. Dessouky, Osama S. Faragallah, "Two Stages Object Recognition Based Copy-Move Forgery Detection Algorithm", **Multimedia Tools and Applications,** DOI :10.1007/s11042-018-6891-7, 30, Nov. 2018.

- Mohamed A. Elaskily, Heba A. Elnemr, Ahmed Seddik, Mohamed M. Dessouky, Osama Elshakankiry, Heba K. Aslan, Osama S. Faragallah, Fathi E. Abd El-Samie, "A Novel Deep Learning Framework for Copy-Move Forgery Detection", **Multimedia Tools and Applications**, Vol. 79, No. 6, March 2020.

Research Outputs

- Mohamed A. Elaskily, Haider Alkinani, Ahmed Seddik, Mohamed M. Dessouky, "Deep learning based algorithm (ConvLSTM) for Copy Move Forgery Detection", **Journal of Intelligent and Fuzzy Systems**, Vol. 40, No. 3, PP. 4385-4405, March 2021.

Research Project: "Digital multimedia Forensics Investigations"

Fund: Sapienza University of Rome, Faculty of Computer Science and Artificial Intelligence, Jeddah University, Saudi Arabia kingdom.

Members:

- Prof. Dr. Prof. Irene Amerini, Sapienza University of Rome, Italy.
- Dr. Mohamed A. Elaskily, Electronic Research Institute (ERI), Egypt.
- Dr. Mohamed M. Dessouky, Faculty of Electronic Engineering, Egypt.
- Dr. Ahmed Sedik, Faculty of Artificial Intelligence, Kafrelsheikh University, Egypt.

Conclusion

- Copy-move forgery is the most difficult type to detect between all digital image forgeries.
- Copy-move forgery detection algorithms which is based on image invariant keypoints are the most efficient algorithms.
- Invariant keypoints based algorithms are characterized by their efficiency against intermediate processes such as rotation, scaling, reflection, translation, and against other post-processing operations such as JPEG compression, blurring, and Gaussian noise.
- Enhanced Filter-based SIFT Approach for CMFD able to give efficient results against different types of attacks which used for hiding copy-move forgeries.

Conclusion

- Enhanced Filter-based SIFT Approach for CMFD using SIFT features to give efficient forgery detection speed and results.
- Enhanced Filter-based SIFT Approach for CMFD show efficiency against rotation, scaling, reflection, translation, and against other post-processing operations such as blurring, Gaussian noise adding, JPEG compression, and Gamma correlation.
- Two Stages Object Recognition Based CMFD Algorithm presents a novel CMFD methodology that is based on segmenting the target image into different objects, and exploring the similarity among these objects.
- This method based on two consecutive stages; matching stage and refinement stage.

Conclusion

- In the matching stage, the candidate image is categorized into forged or original, while the refinement stage aims to certify the originality of the image that is classified as original in the matching stage.
- Two Stages Object Recognition Based CMFD Algorithm shows effectiveness with different datasets under different cloning conditions whether single or multiple cloning.
- Experimental results confirm that the proposed algorithm offers very low computational time comparing with other existing algorithms.
- This low computational time results from using SURF algorithm in addition to build the objects' catalog, which contains all the objects in the tested image, facilitates the matching process.

Conclusion

- demonstrates a novel CMFD methodology based on deep learning approaches.
- Another contribution is the development of a CNN classification system to classify the candidate images for two classes original or tamper.
- The CNN system extracts image features and builds feature maps. Then, the CNN uses the average of the produced feature maps and automatically searches for the features correspondences and dependencies.
- After training the CNN, the system is ready to test and classify the images to detect the copy-move forgery.
- The experimental results prove that the proposed algorithm offers a very low *TT* comparing with other algorithms.
- The overall result indicates that the deep learning-based proposed algorithm extensively outperforms the reported algorithms according to its performance and *TT*.

Future Work

- In the future work, CNN modification may be performed to further speed up the proposed algorithm.
- Searching for more challenged datasets may be fulfilled to test the suggested technique. Moreover, deep learning techniques may be applied to detect other types of digital image forgeries.
- Mobile-based and Web-based CMFD algorithm may be developed.
- Video forensics is a big new challenge will be breaking in.

References

[1] Prints & Photographs Division Library of Congress. Photo tampering throughout history. URL http://www.fourandsix.com/photo-tampering-history/.

[2] Eric Kee, Hany Farid, ”Exposing Digital Forgeries from 3-D Lighting Environments", IEEE WIFS’2010, 978-1-4244-9080 6/10, Seattle, USA, December 12-15, 2010.

[3] Osamah M. Al-Qershi , Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art ", Forensic Science International, 284–295, 3 July 2013.

[4] Alessandro Piva, "An Overview on Image Forensics", ISRN Signal Processing, Volume 2013, Article ID 496701, 2013.

[5] Judith A. Redi, Wiem Taktak, Jean-Luc Dugelay, "Digital image forensics: a booklet for beginners", Multimedia Tools Appl. 51, 133–162, (1) (2011).

[6] SALAM A.THAJEEL, GHAZALI SULONG, "A SURVEY OF COPYMOVE FORGERY DETECTION TECHNIQUES", Journal of Theoretical and Applied Information Technology, Vol.70 No.1, 10th December 2014.

[7] Image forgery and security. URL http://www.slideshare.net/ahlamansari/image-forgery-and-security.

[8] M. Ali Qureshi, M.Deriche, "A Review on Copy-moveImage Forgery Detection Techniques", Multi-Conference on Systems, Signals & Devices (SSD), 11-14 February 2014.

[9] http://www.wikipedia.org/wiki/morphing.

[10] Tu K.Huynh, Thuong Le-Tien, Khoa V.Huynh, Sy C.Nguyen, "A Survey on Image Forgery Detection Techniques", The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), 71-76, 25-28 Jan. 2015.

[11] J. Fridrich, D. Soukal, J. Luka´ s, "Detection of copy-move forgery in digital images", Proceedings of DFRWS 2003, Cleveland, USA, 2003.

[12] Michael Zimba, Sun Xingming, "Fast and Robust Image Cloning Detection using Block Characteristics of DWT Coefficients", International Journal of Digital Content Technology and its Applications. Volume 5, Number 7, July 2011.

References

[13] Guangjie Liua, Junwen Wanga, Shiguo Lianb, Zhiquan Wanga, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications , Volume 34, Issue 5, 1557–1565, 2010.

[14] Linda G. Shapiro and George C. Stockman, Computer Vision, Upper Saddle River: Prentice–Hall, 2001.

[15] Muhammad Hussain, Sahar Q. Saleh, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, "Comparison between WLD and LBP Descriptors for Non-intrusive Image Forgery Detection", IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA) Proceedings, 197-204, Alberobello, 23-25 June 2014.

[16] David G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints", international Journal of Computer Vision, Volume 60, Issue 2, pp 91-110, November 2004.

[17] Bo Liu, Chi-Man Pun, "A SIFT and Local Features Based Integrated Method for Copy-Move Attack Detection in Digital Image", IEEE International Conference on Information and Automation (ICIA), 865 - 869, Yinchuan, 26-28 Aug. 2013.

[18] Hussein Soleimani, Mohammadali Khosravifard, "Mutual Information- Based Image Template Matching with Small Template Size", 7th Iranian Machine Vision and Image Processing (MVIP), 1 - 5, Tehran, 16-17 Nov. 2011.

[19] Rohini.A.Maind, Alka Khade, D.K.Chitre, "Image Copy-moveForgery Detection using Block Representing Method", International Journal of Soft Computing and Engineering (IJSCE), 2231-2307, Volume-4, Issue-2, May 2014.

[20] Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 8, 1355 – 1370, AUGUST 2013.

[21] Surbhi Sharma, Umesh Ghanekar, "A rotationally invariant texture descriptor to detect copy-moveforgery in medical images", IEEE International Conference on Computational Intelligence & Communication Technology, 795-798, Ghaziabad, 13-14 Feb. 2015.

[22] Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni, " Forensic Analysis of SIFT Keypoint Removal and Injection", IEEE Transactions on Information Forensics and Security, Volume: 9, Issue: 9, 1450 - 1464, Sept. 2014.

References

[22] Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni, " Forensic Analysis of SIFT Keypoint Removal and Injection", IEEE Transactions on Information Forensics and Security, Volume: 9, Issue: 9, 1450 - 1464, Sept. 2014.

[23] Somnath Chakraborty, "Copy-moveImage Forgery Detection Using Mutual Information", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 1 - 4, Tiruchengode, 4-6 July 2013.

[24] Jie Zhao, Jichang Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Forensic Science International 233, 158 - 166, September 2013.

[25] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo,G. Serra, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 6(3), pp. 1099-1110, 2011.

[26] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-Move Forgery Detection and Localization by Means of Robust Clustering with J-Linkage", Signal Processing: Image Communication, vol. 28(6), pp. 659-669, 2013.

[27] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou: "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, vol. 7(6), pp. 1841-1854, 2012.

[28] Parul Mishra, Nishchol Mishra, Sanjeev Sharma, Ravindra Patel, "Region Duplication Forgery Detection Technique Based on SURF and HAC", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2013.

[29] Harpreet Kaur, Jyoti Saxena, Sukhjinder Singh, "Simulative Comparison of Copy- Move Forgery Detection Methods for Digital Images", International Journal of Electronics, Electrical and Computational System IJEECS, ISSN 2348-117X, Volume 4, September 2015.

References

[30] Mishra P, Mishra N, Sharma S, Patel R (2013) Region duplication forgery detection technique based on SURF and HAC. Hindawi Publishing Corporation. Sci World J.

[31] Kaur R (2016) Image forgery and detection of copy move forgery in digital images: a survey of recent forgery detection techniques. Int J Comput Appl 139(5)

[32] Elaskily MA, Aslan HK, Abd El-Samie FE, Elshakankiry OA, Faragallah OS, Dessouky MM (2017) Comparative study of copy-move forgery detection techniques. Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & Intl Conf on New Paradigms in Electronics & Information Technology (PEIT),
Alexandria, Egypt

Thank you