I. J. Computer Network and Information Security, **2022, 5, 60-72**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.05.05

Image Hashing Through Spatio-triad Relationship

Sowmya K. N.
Department of ISE, JSS Academy of Technical Education, Bangalore, Karnataka, India
E-mail: kn_sowmya@rediffmail.com

H. R. Chennamma
Department of Computer Applications, JSS Science and Technology University, Mysuru, Karnataka, India
E-mail: hrchennamma@sjce.ac.in

Received: 17 March 2022; Revised: 25 May 2022; Accepted: 17 July 2022; Published: 08 October 2022

Abstract: Authenticating the content of the digital image has profound influence in legal matters and in court rooms. Image forensics plays an important role towards it. Proposed approach helps to authenticate the original image by generating a content based image signature that is a unique fingerprint for the image. Our novel approach establishes spatio triad relationship among features and finds the centre of gravity or centroid of the same after indexing. Topology of the triad relationship for the content based low level feature descriptors is preserved through aggregation until single key feature is deduced which is a 128 bit signature hash value and represented in decimal form. Density of feature keypoints influences the centre of gravity which acts as a unique signature for the given image. Manipulated image cannot contribute to restore / regenerate the same signature. We have verified our authentication approach for standard benchmark image dataset like MICC-F220, Columbia Image Splicing Evaluation dataset and Image manipulation dataset from Friedrich Alexander University and have found satisfactory results for the same. Content based image signature obtained is used to verify authenticity of image and for retrieval of video from database. Content based image fingerprint generated can also be considered for embedding as a watermark.

Index Terms: Spatio triad topology, Image Authentication, Digital Signature, Image Ttampering, Image Forensics, Content based Signature, Image Fingerprint.

1. Introduction

Traditional film cameras of the past are a history now. End user in those days had to approach a professional who had the dark room equipments and domain knowledge to process the films. Image forgeries of the past were hence performed by professionals most. Today in digital world, due to a lot of editing tools like Adobe's Photoshop, illustrator, Scissors, Acorn, handbrake, Pixlr, GIMP, Sefexa, Pixelmator, Photoplus, Coreldraw, Corel PaintShop Pro, Photoscape are soonavailable. Any layman or a professional can perform malicious manipulation through splicing, copy move or cloning, and object removal/insertion (cropping), etc to conceal information as well as to remove visual traces of tampering and it does not require any special environment. Nowadays most of the smart phone applications are available to provide these services at fingertips to the perpetrator fulfilling his/her fantasy. Such intentionally manipulated images are made available globally with the help of social media instantly. Computer graphics based synthetic images mock the original with high level of photorealism.

Main goal of image forensics/scientific investigators in forensic science is to see that the guilty should not escape and innocent must not suffer due to image tampering. Tampering means unauthorized alterations and cause damage to the original content of the image. Every digital image has unique fingerprint obtained through the acquisition device and is influenced by the lighting condition where it was taken. Image tampering identification methodologies assist to verify the integrity of the image by detecting global manipulations or localize the forgery by investigating the artefacts introduced due to tampering. Image forgery detection belongs to active or passive category depending on the approach adopted. In this paper, active forensic technique is applied for generating an image hash based on content. Entropy of information available in an image makes it robust and unique. We propose an algorithm to authenticate the content of an image based on key points. The proposed technique acts as a complete verification system that helps an investigating officer to verify whether the query image is original or forged. The paper is organized as follows. Section I gives the Introduction to the image forensics, Section II talks about related works in passive and active forensics. Section III presents the detailed description of our proposed approach. Section IV comprises the Numerical Research and Observations over the datasets considered. section V discusses the results and Section 6 highlights conclusions drawn and future scope.

2. Related Work

In passive approach espouse is blind forensics. Inherent features of the image are exploited to verify its genuineness. Availability of the reference image/original image does not exist in this case. Image acquiring device characteristics features like chromatic aberrations, colour filter arrays, camera response function, imaging sensors, compression and quantisation techniques adopted while saving the acquired raw image, statistical correlations etc are used to verify its genuineness. Imaging sensor imperfections found against the ideal supply a distinctive fingerprint in identification of the source camera. Source camera's components attribute to signal characteristics of the image. Sensors used in cameras are either CMOS or CCD based and imperfections in this sensors help to identify source camera. Kurosawa et al [1] have identified the source camera through fixed pattern noise that is distinct to each camera using dark images. Location of the non uniform magnitude of dark current on a CCD array is fixed for individual camera and acts as a fingerprint. Visible pixel defects like dead pixels, pixel traps, hot point defects and the cluster defects of low end camera were used by Geradts et al., [2] for source camera identification which was not in high end cameras. Sensor pattern noise (SPN) at various signal levels due to optical dust, interference in optical elements, Pixel Non Uniformity (PNU) in sensor manufacturing process acts as a natural feature to identify source camera models[3,4]. PRNU patterns have contributed to identify source camera [5-9]. Forgery localisation is achieved by abhishek et al., using semantic segmentation along with deep learning approach [10] Goel et al., used variant kernel size for dual branches to extract multiscale features that are later fused to obtain dominant features to assist classification of forged and authentic images [11]. 4 layer cnn is adopted with filter to detect splicing , copy-move [12]. Each pixel in an image is encoded using local directional pattern that effectively detect copy move forgery in [13]. Localisation of the forged region require manual effort. Saurabh et al., [14] used LPQ operator over the entropy filtered image to maintain invariant information that helps to detect forged images using SVM classifier. All forms of image forgeries and the deep-learning approaches adopted in recent years along with anti-forensic techniques have been discussed elaborately by Camacho et al., [15].

Active approach involves identifying image forgery by identifying the change in primary authentication like signature or watermark embedded in the image which is a known information/signal. Watermark can be fragile or semi fragile in nature and can be embedded spatially. DCT, DWT, QDCT, DFT coefficients are utilized in the literature for watermarking effectively [16-24]. Image watermarking assist content authentication [25]. In early times digital signatures were based on cryptographic functions. Soft-hashing was first proposed in [26] and [27] developed a soft hash based on visual content of the image as importance was given to content than the file. The data reduced message authentication code is then encrypted using cryptographic technique. Threshold chosen is robust to lossy compression. Boncelet et al., [28] iterate over the image repeatedly performing partition and computes cryptographic MAC for each block. Structural and pseudo random partitions (INTMAC) help to detect and localize forgery regions and background partition helps to detect number of errors. Similar to [28] DWT based variable length structural digital signature (SDS) utilizes multi scale parent-child pairs in [29] Inter scale relation of wavelet coefficients help to localize forged regions when statistical correlations vary. Monga et al., [30] developed a clustering approach to generate the variable length perceptual final hash for the intermediate hash generated using wavelet transform to the Morlet wavelet. Swaminathan et al., [31] hash algorithm has used Fourier Mellin transform outputs which are rotation invariants to detect malicious tampering and is robust to content preserving operations. Xiang et al., [32] have built a histogram oriented hash robust to geometric distortions which fails to exhibit local information completely and cannot detect/identify when different contents have same histogram. Monga et al., [33] used a dimension reduction oriented approach that fails to locate the regions forged since hash obtained is from the secondary image with NMF and fails to detect forgery when geometric transforms is large and brightness is varied. Similar dimension reduction approach is adopted by Tang et al., [34] where NMF is applied to the secondary sub images in order to generate a coarsely quantized coefficient matrix which is scrambled to create image hash. Wenjaun Lu et al., [35] have proposed a Forensic hash scheme – FASHION. Hash computed using Radon transforms and scale space theory helps to localize forgery regions and identify geometric transformations to locate forgery. Wenjun Lu et al., [36] constructed a forensic hash based on hybrid approach using SIFT and block based features for better tampering localisation than [35].Gaussian distribution of features has been assumed for virtual watermark based on decision theory and combined with pseudo randomly generated patterns to extract hash bits by Khelifi et al., [37]. Their approach detects change in content for relatively large area efficiently. Fouad et al., [38] identified the importance of initial key in NMF which can be uniquely/precisely assessed depending on the observations of image's hash pairs. F ahmed et al., [39] have proposed a robust wavelet based variable length hashing scheme based on the size of the image after random pixel modulation using secret key.Y lei et al., [40] have considered magnitude of the significant radon transforms and DFT is applied on these invariant moments. They are normalized and quantized to generate fixed length hash. Zhenjun Tang et al., [41] construct image hash using lexicographical framework. Dictionary consisting of words representing various features such as size, color, texture etc are considered to build sub dictionary to avoid duplications. NMF is used to generate words that form a intermediate hash in dictionary and the non overlapping blocks are captured through DCT. SSIM helps to find matched block in dictionary. Lv et al.,[42] embeds SIFT –Harris feature points into shape based context descriptors in order to compute a fixed length hash utilising radial shape context and angular shape context hashes. Tampering attacks of all types cannot be detected efficiently using their approach. Yan zhao et al., [43] approach has used local descriptors like texture,

position and global descriptors like Zernike moments that represent structure of the image to generate hash. Threshold distance helps to determine forgery, its type and location. Yuenan Li et al., [44] developed a locality sensitive hashing using PCT. Copy move forgery after rotation is detected accurately and perform better than Zernike moments based algorithms. Granty et al., [45] developed efficient copy-move forgery detection and image retrieval scheme by spectral hashing of invariant patterns represented through polar harmonic transforms PCT whose transform kernel is orthogonal in nature. Sparsification of laplacian features helps to reduce the computational time required. The binary code generated through spectral hashing for a query image is then evaluated with the training set images to aid retrieval of image if they are similar. Hamming distance helps to measure similarity and minimum distance between the binary values is a potential candidate to identify for forged region. [46] Key point based methods are influenced by the region of high entropy of information contained in the image.

3. Proposed Approach

We propose an algorithm to authenticate the content of an image based on signature technique. This technique acts as a complete verification system that verifies the query image as original or forged. Our key point based approach can use any scale invariant features like HARRIS[47], HOG[48], SIFT[49], SURF[50] and MSER[51] for the given image I. Malicious geometrical transformations like rotation, scaling, translation and cropping can be efficiently identified using our approach. The location of the key feature vectors are sorted based on lexicographical sorting or their Cartesian coordinates/polar coordinates and are spatially arranged in spatio triad relationship (STR). The spatio triad relationship connects the key points obtained among the extracted features. Our approach adopts STR and finds the midpoint or centroid of the same at each level. It preserves the topology of the new mid points thus obtained by repeating the STR until it deduces to a single point at the last level. If even number of key points is obtained at any level then the loop back process is adopted for the first key point in that level. If only two key points are obtained initially during feature extraction then the midpoint of the two is considered to be the centroid. The final centroid key points thus obtained acts as a distinctive signature for the given image. Depending upon the density of feature keypoint, we obtain the centre of gravity repreenting the content based image signature (CBIS) for the given image. Most likely the centroid lies where the density of keypoint is high.

In the verification phase, we verify whether the CBIS of pristine and query image is same or not. If it is different then we conclude that query image is forged/tampered one. If there is any forgery done on the image then the key point's location varies at level zero resulting in change in the fingerprint. Hence our technique can be adopted as evidence for alteration detection. Our CBIS approach is fragile to malicious modifications and can identify very small amount of change too in the image. Change in a single keypoint extracted also reflects the change in the signature. The CBIS thus obtained can be stored separately in decimal form for verification or can be embedded to the image as a watermark. The CBIS signature is represented in binary to calculate the hamming distance. Our experiments prove the efficiency of CBIS since the normalised hamming distance is around 0.5. The exact location of the spatial region modified is not identified in our work. CBIS registration phase ensures image integrity by generating 128 bit unique key at the time of acquiring evidence.

Content Based Spatio Triad Relationship Algorithm (CBSTR):

The proposed algorithm for CBIS registration and verification is as follows.

ALGORITHM: CBSTR

Input: Image I
Output: $CBIS_{(x,y)}$ for Image I.

Step 1: Extract and determine m keypoints for Image I
$m_i(x,y)$ i^{th} keypoint coordinates x and y of m features obtained

Step 2: Sort keypoint features and label them.

Step 3: Calculate level 'L' for Image 'I' based on m.
Initialisation:
Level L 0
Keypoints of an existing level lm m
While (*lm*> 1) do
Compute the count of keypoint for the next level
$lm \quad lm/2$
L L+1

Step 4: Compute Centre of gravity to generate CBIS

CBIS(I) function Centre of Gravity(m(x, y), L)

Centre of Gravity(m(x, y), L)
for j 1: L
{
Let i 1, k 1
while (i< m-2)
{
COG[k] = [m_i(x,y) + m_{i+1} (x,y) + m_{i+2} (x,y)] / 3
i i+2, k k+1
}
if (m%2==0)
COG[k] = [m_i(x,y) + m_{i+1} (x,y) + m_i(x,y)] / 3
else
COG[k] = [m_i(x,y) + m_{i+1} (x,y) + m_{i+2} (x,y)] / 3
m COG;
m k;
}

CBIS (I) m

Step 5: End

Time complexity of our CBSTR scheme is $\boldsymbol{O}(\log \boldsymbol{m})$ where *'m'* indicates the number of keypoints. Our content based image hashing approach always return a 128 bit message digest represented in decimal form CBIS($I_{x,y}$) where x and y are 64 bit each for the content based feature vector's centre coordinates x and y.

Content based image signature model Proposed:

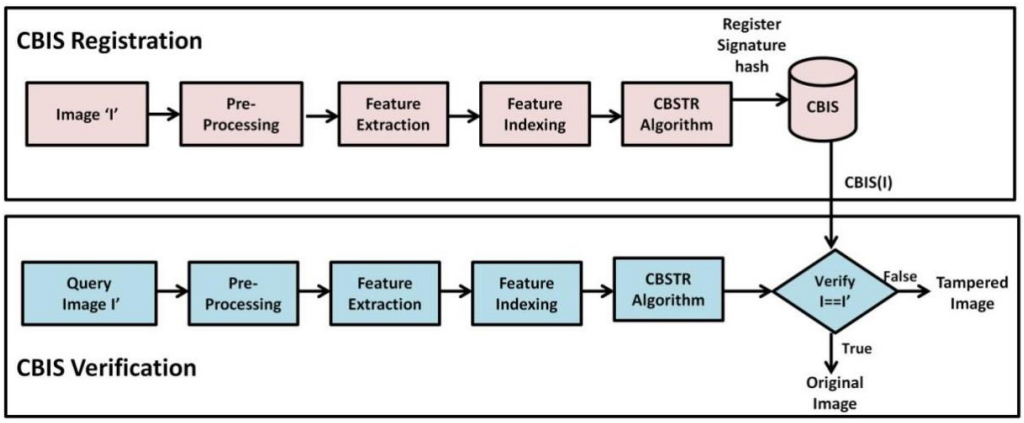


Fig.1. CBSTR signature generation and verification model

The CBIS model proposed is largely classified into CBIS Registration and Verification phase as depicted in Fig.1. During the ***CBIS registration phase***, CBIS signature is generated for the original image based on the features derived from the content of the image and stored to facilitate verification. During ***verification phase*** the query image is verified for its legitimacy by generating the signature for the same. CBIS of the query image is matched to the CBIS of original image; if there is a mismatch then it is identified as fake and tampered else original. The steps involved in CBIS generation are described below.

Step 1: Extract and Determine 'm' keypoints for the given image I.

Extract features for the given image 'I'. The features thus obtained are the low level descriptors of an image identified in terms of blobs. Any competent feature extraction method can be considered for feature extraction. We have considered SIFT, SURF, MSER, HOG and HARRIS in our work. For an Image 'I', P_n (x, y) epitomize the *x, y* coordinates of the keypoint for the 2D plane where n = 1, 2, 3**….**m. 'm' indicates the total keypoints obtained during feature extraction and are said to be at level '0'. These location attribute of the keypoints is considered for further processing.

Step 2: Sort keypoint features and label them.

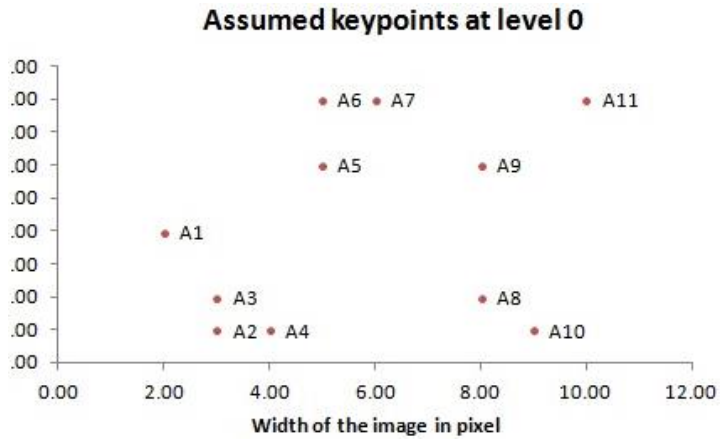


Fig.2. Indexed and labelled key points of an image

Sort the 'm' keypoints extracted based on their location and arrange them in the increasing order of 'x' and 'y' coordinates for the given image (Chennamma et al., [52]) in the 2D plane as shown in Fig.2., and label them.

Step 3: Calculate level 'L' for Image 'I' based on m.

The total number of level *'*L*'* required for CBIS generation is the least *'*L*'* and is represented in eqn (1).

$$m \leq 2^{L+1} - 1 \tag{1}$$

If '*m' key* points exist at level '0', then at level 1 $\left|\frac{m}{2}\right|$number of centroids are obtained. The process of centroid computation is repeated on these$\left|\frac{m}{2}\right|$key points and $\left|\frac{m}{4}\right|$ number of key points are obtained at the next level 2 (refer to Fig.3). At every consecutive level the features gets condensed by half.

Step 4: Compute Centre of gravity to generate CBIS for Image I.

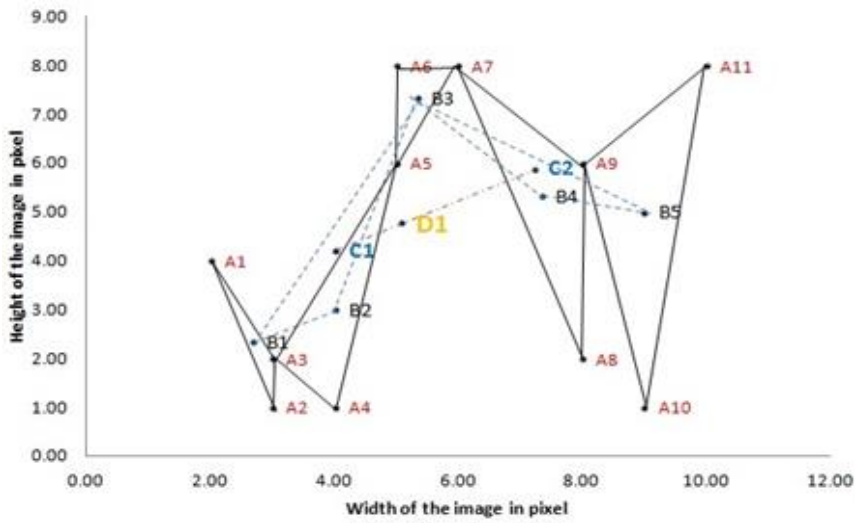


Fig.3. Illustration of CBIS (I) calculation process for a given image

The features extracted at level `0' and indexed for the given image 'I' are local descriptors in nature and plenty in general. In order to deduce the signature from these keypoints for hard authentication, the features '$P_n(x, y)$' for n=1,2,3 to m are grouped consecutively for every three key points with the last superimposed between successive sets and the midpoint of each such triplets are found at each level 'l'. Centroid computation is repeated until a single keypoint is generated at the last level which represents the fingerprint of the image. If two keypoints exists at level'0' then the mediocre of the two is the CBIS (I).The CBIS computation for a given image is demonstrated in Fig.3. Observe the new keypoints *B1*, B_2, B_3, B_4, B_5 that are formed at level 1from the centroid of sorted features of level 0 *{(A_1, A_2, A_3), (A_3, A_4, A_5), (A_5, A_6, A_7), (A_7, A_8, A_9), (A_9, A_{10}, A_{11})}* where $A_1$to A_{11} are the extracted keypoints for this particular case. The process of midpoint/centroid calculation is continued for all levels and the last level contains a deduced single centroid D_1 at level 3 representing the unique image representative (IR) for the given image.

Computation Of Content Based Image Signature (CBIS)

Let $\left(P_x^0(i), P_y^0(i)\right)$ represent the coordinates of i[th] keypoint in level 0.Using these keypoints that are extracted using suitable scale invariant approach the next level keypoints are computed:

$$P_x^1(k) = \frac{\sum_{i=2k-1}^{2k+1} P_y^0(i)}{3}, P_y^1(k) = \frac{\sum_{i=2k-1}^{2k+1} P_y^0(i)}{3} \quad (2)$$

Where $(P_x^1(k), P_y^1(k))$ indicate the k[th] key point at level 1.

Keypoints obtained by computing the centroids of level 1 are the new imaginary keypoints for level 2. They are used to compute the keypoints for the next level as in (3):

$$P_x^2(k) = \frac{\sum_{i=2k-1}^{2k+1} P_x^1(i)}{3}, P_y^2(k) = \frac{\sum_{i=2k-1}^{2k+1} P_x^1(i)}{3} \quad (3)$$

At every level, total keypoints get reduced by 50% of previous level. Centroid computation process is continued until last level. The general centroid computation for a given 'l [th]' level is represented as in (4):

$$P_x^l(k) = \frac{\sum_{i=2k-1}^{2k+1} P_x^{l-1}(i)}{3}, P_y^l(k) = \frac{\sum_{i=2k-1}^{2k+1} P_y^{l-1}(i)}{3} \quad (4)$$

Depending on the number of keypoints at a particular level, the last centroid computation process varies as in Fig.4. During the existence of even keypoints, the end centroid computation process is followed as in (5)

$$P_x^l(t) = \frac{P_x^l(m-1)+P_x^l(m)+P_x^l(1)}{3} \quad P_y^l(t) = \frac{P_y^l(m-1)+P_y^l(m)+P_y^l(1)}{3} \quad \text{Where } t=\left|\frac{m}{2}\right| \quad (5)$$

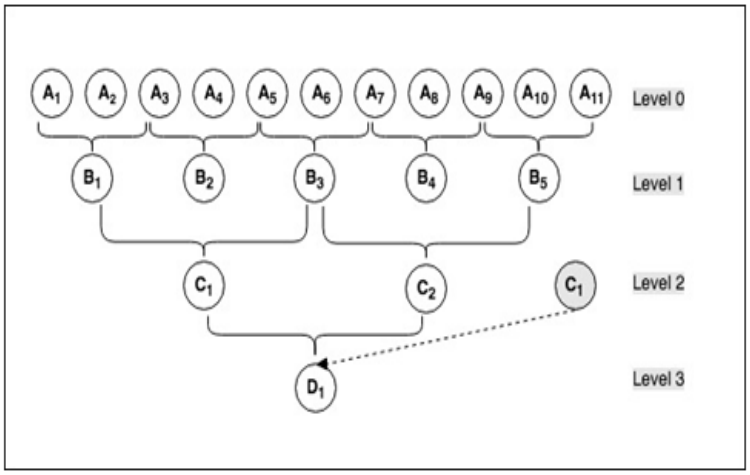


Fig.4. CBIS computation flow for odd number of keypoints at level 0

Consider an example, where the count of keypoints extracted is 11 as shown in Fig.4. Sort these keypoints as in Fig.2. Compute the levels and keypoints through centroids for subsequent levels. The new keypoints in subsequent levels are found to be 5, 3 and 1 respectively. Total levels are 3 that satisfy the inequality equation (1). Suppose the count of keypoints is 8 at level '0', then count of new keypoints at subsequent levels will be 4, 2 and 1 respectively. Total levels will be 3 that satisfy the inequality equation (1).

4. Numerical Research and Observations

In this section, the results of experimental study and efficacy of the proposed method is discussed. MatlabR2014b and Java IDE with JmatIO external library environment is used in this work. To examine quality analysis of the original and tampered images from the standard benchmark datasets available publicly for image tampering detection due to splicing, copy move forgery, object addition and deletion have been considered in our work. Semantic changes in the image due to forgery attacks will be reflected in the CBIS obtained retroactively. Low level local descriptors like] HARRIS[47], HOG[48], SIFT[49], SURF[50] and MSER [51] are used for feature extraction. The key features are indexed and the same is fed to the CBSTR scheme to generate fingerprint/signature as shown in Fig.1.

Proposed CBSTR algorithm efficiency, feasibility and accuracy are evaluated with the standard public dataset like MICC-F220 from image communication laboratory (ICL) [53], Columbia image splicing dataset [54] and Image Manipulation Dataset from Friedrich Alexander University [55] to determine the detection rate of tampered images.

Table 1. Content based image signature (CBIS) for images taken from MICC - F220 dataset

Image Name	HARRIS	SIFT	SURF	HOG	MSER
DSCN41_scale.jpg (Original Image)	x=406.33743322384356 y=452.96563246574414	x=445.0461906213484 y=409.30364832596655	x=386.1925662627509 y=463.2563952071114	x=314.0136759857855 y=499.2927925890129	x=411.06762550626104 y=468.9327284550271
DSCN41tamp1.jpg (Tampered Image)	x=406.57869576974196 y=453.16964813156454	x=443.0940161560738 y=411.15645514742	x=384.0035644671372 y=463.0652955399293	x=313.9635784532616 y=499.29506752306037	x=410.2126330585127 y=470.34594770983
DSCN41tamp25.jpg (Tampered Image)	x=412.7396804041805 y=455.4537417712156	x=450.94682348557967 y=414.25228674490677	x=383.94536504031794 y=458.61577860514325	x=313.7186050683946 y=498.7701553858701	x=408.04641958497456 y=469.8195838364245
DSCN41tamp27.jpg (Tampered Image)	x=408.022808247423 y=454.71139040119095	x=450.16117258547985 y=409.1961965486291	x=383.162644920762 y=459.55260780217026	x=312.2887206832695 y=500.2836837338304	x=409.9491674370599 y=470.5560301152912
DSCN41tamp37.jpg (Tampered Image)	x=407.8143567793452 y=455.30490963684593	x=450.18333214787725 y=408.2708430286711	x=386.0876577142135 y=456.8866741504271	x=313.0742262620931 y=499.22226486589784	x=410.3848234556594 y=469.965965911721
DSCN41tamp131.jpg (Tampered Image)	x=405.7301407754446 y=454.19762667731993	x=444.62922792934677 y=413.24395044793306	x=383.97551708718555 y=462.9555705901491	x=313.0412776362985 y=498.9551440161769	x=408.37358024101803 y=470.4573020033858
DSCN41tamp132.jpg (Tampered Image)	x=406.32947614913314 y=454.97850444287025	x=443.9393454588562 y=407.49078392521466	x=383.9743130638403 y=462.9545145777554	x=314.51965630314294 y=497.413787199909	x=408.8033795481029 y=467.0898517061526
DSCN41tamp133.jpg (Tampered Image)	x=406.9330196967526 y=453.7076882327464	x=444.1498123592271 y=415.56773188368976	x=384.43314380061423 y=461.3160678007094	x=315.16790796732545 y=496.84382093325206	x=407.6879966295705 y=467.5856990596176
DSCN41tamp134.jpg (Tampered Image)	x=406.5489407292603 y=454.9496786682855	x=444.17393893207344 y=409.2924533861708	x=385.0599006303398 y=462.5026393588623	x=315.02612089460314 y=497.0627412986435	x=403.45858575076414 y=468.08170807810376
DSCN41tamp176.jpg (Tampered Image)	x=406.6806498340197 y=453.9975344746354	x=450.94018340700103 y=408.0966754729124	x=384.03178994304216 y=463.4360724345811	x=315.09992333851 y=496.91658399338013	x=404.2798245181 y=467.2322592424958
DSCN41tamp237.jpg (Tampered Image)	x=408.08279374245416 y=454.8781186441222	x=450.3413771613405 y=415.7283727074125	x=382.79623508584183 y=460.01418831093696	x=313.13494982368394 y=497.81290058681935	x=408.1215393355372 y=468.72275550306216

Table 1 lists the results of all query images with their corresponding CBIS obtained. Our experiment was conducted on ground truth database MICC- F220 [53] consisting of 110 original and tampered images respectively. Fig.5. shows an original and its tampered images from the same. Copy move forgery attack is seen in the tampered images which has undergone translation, rotation and scaling. STTFR approach is able to identify these forgeries with different digital signatures for all of them.

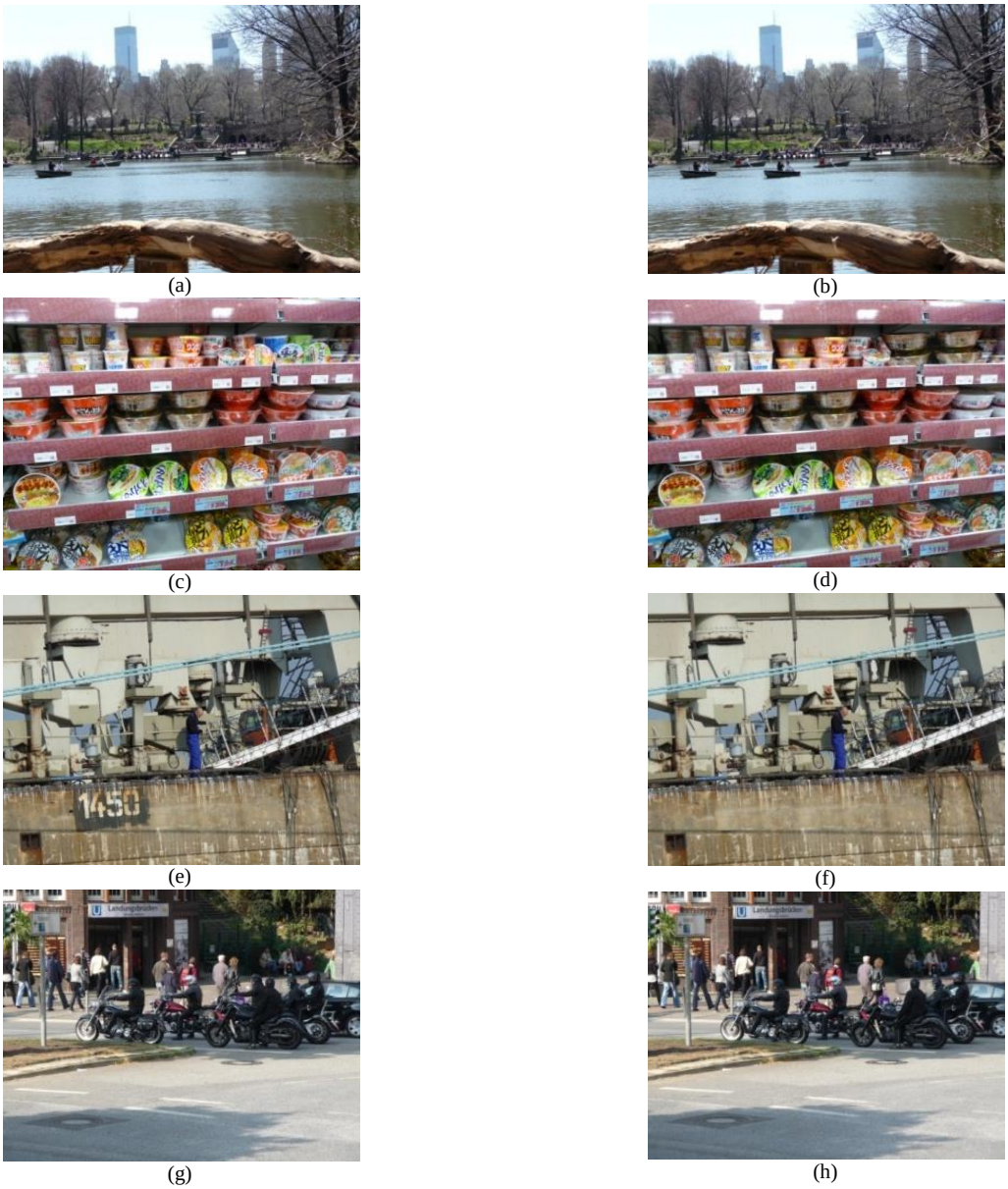
(a) (b) (c) (d) (e) (f) (g) (h) (i)

(j) (k)

Fig.5. DSCN41_scale Pristine and the tampered images from MICC-220 considered in Table 1. (a) Original image, (b)-(k) shows the copy move forged images with translation, rotation and scaling done.

Our method is efficient to detect copy move forgeries from MICC- 220 dataset efficiently and the signatures obtained in all cases are found to be different when forged.

The second benchmark dataset used was Image Manipulation Dataset from Freidrich Alexander university [55] It is used for benchmarking the image tampering artifacts like copy move forgery detection (CMFD). It includes 48 base images and artifacts introduced images based on various transformations, resampling and double JPEG compression. Few of the experimental images considered from the dataset and their results are shown in Table 2 and Fig.6. Copy move forged images have undergone geometrical transformations semantically to provide meaningful information.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

(i)

(j)

Fig.6. Pristine and forged images due to Copy-Move Forgery from Image Manipulation dataset. (a) central_park original image, (b) central_park _copy tampered image, (c) Supermarket original image, (d) Supermarket _copy tampered image, (e) ship_number original image, (f) ship_number_copy tampered image, (g) motorcycle original image, (h) motorcycle_copy tampered image, (i) red_tower original image, (j) red_tower_copy tampered image

Table 2. Content based image signature (CBIS) for images taken from Image Manipulation Dataset

Image Name	HARRIS	SURF	HOG	MSER
central_park	x=2025.472217403276 y=743.3809727729872	x=1909.8897788577842 y=1043.6357456216049	x=1973.217097797112 y=917.7899718654536	x=1883.8195547783496 y=1048.1864497123663
central_park_copy	x=2012.4598547828607 y=750.2624024457988	x=1853.02841594598 y=1064.6592471018084	x=1959.8958806725575 y=928.0546880296737	x=1874.037802034976 y=1048.2222208495584
Supermarket	x=1509.1098891948723 y=1572.8415033208757	x=1584.2811751051968 y=1509.1624709230418	x=1548.674033903527 y=1870.6601316861636	x=1511.6570162301493 y=1446.2281083342707
Supermarket_copy	x=1505.684382656544 y=1559.363778895641	x=1530.6591054468015 y=1528.5252676782593	x=1517.7596230724203 y=1893.6326079889689	x=1510.5813215110566 y=1448.6581888086357
Ship_number	x=1964.209252187563 y=1258.9444061335114	x=1755.9026349087308 y=1310.7973248347716	x=1966.2608793421757 y=1276.2884430573529	x=1881.5852237436384 y=1381.1249391293732
Ship_number_copy	x=1936.5440936017794 y=1244.0560974451166	x=1807.4255480195152 y=1282.1552430772451	x=2015.2346966927635 y=1239.1840455924896	x=1887.840770452595 y=1381.8313326094437
motorcycle	x=1205.8973822737958 y=868.8586066831737	x=1293.137381258514 y=856.8103256011236	x=829.0748941706115 y=811.5905985425946	x=1654.8457585143278 y=852.4957136585948
motorcycle_copy	x=1202.7997774350447 y=871.5554140132062	x=1292.0042759648334 y=859.0669513210186	x=828.2110693625897 y=810.7750224511882	x=1648.674476686437 y=855.6424826891379
red_tower	x=1695.9920983456543 y=638.4711699895676	x=1624.8266473651354 y=912.6517052368202	x=1957.841422613138 y=457.0927725628988	x=1630.8574006734768 y=977.6941918756708
red_tower_copy	x=1655.1490069538133 y=644.9606452596644	x=1613.914180142303 y=931.8244326064352	x=1907.7314773086298 y=461.6644809547311	x=1626.0921278017875 y=1001.5337181699174

Table 3. Content based image signature (CBIS) for Columbia Image Splicing Dataset Samples

Image Name	HARRIS	SURF	HOG	MSER	SIFT
AU_T_002.bmp	x=62.04492801501427 y=54.15210081226051	x=55.58188247157386 y=58.27551961828161	x=65.5576055527024 y=67.12312062828484	x=60.22517886475771 y=67.34489882989838	x=67.68474622770918 y=62.37554183813444
SP_T_002.bmp	x=45.21013399962698 y=60.45272033728036	x=51.283832888871395 y=63.50897743737911	x=61.875067342837546 y=67.98957785432106	x=58.98022427611227 y=67.325243533557	x=68.97012345679013 y=57.112331961591224
AU_T_082.bmp	x=53.70332059546263 y=63.55744420288357	x=78.91591389973958 y=60.15270890129937	x=66.1362207274923 y=60.51527148771351	x=54.32115680167377 y=61.219886943309554	x=59.267037037037035 y=54.16031550068586
SP_T_082.bmp	x=43.597692974310355 y=61.9191935582416	x=66.62932346485279 y=40.26481501261393	x=61.433026448525844 y=65.67011753914288	x=55.50660299927774 y=63.32273395692696	x=53.128175582990394 y=57.426104252400556
AU_T_028.bmp	x=56.994317562764344 y=67.27829659034194	x=56.09721189271276 y=62.94320399280438	x=57.8323388036441 y=66.40855688671571	x=60.13785366495287 y=64.5336649074476	x=57.818856881572934 y=60.70204846822131
SP_T_028.bmp	x=58.84984349855616 y=68.60121993774361	x=62.44617012400687 y=70.03048073411479	x=63.4177240250478 y=64.99728796478816	x=56.93705531762625 y=68.05015155480886	x=58.688949855205 y=61.12265965554031

We can observe from the results obtained in Table 2, that irrespective of the amount of forgery done over an image, our approach is able to detect tampering with change in signature for the forged images.

In our experimental study we have also considered Columbia image splicing detection evaluation dataset [54] from DVMM Laboratory of Columbia University for our study. Columbia dataset contains 1845 image blocks of diverse content containing 933 authentic images and 912 spliced images with size 128 X 128 pixels extracted from CalPhotos collection. The photomontage found in this dataset is found accurately in our work. Table 3 describes the results of the spliced and original images and Fig.7. represents the image samples.

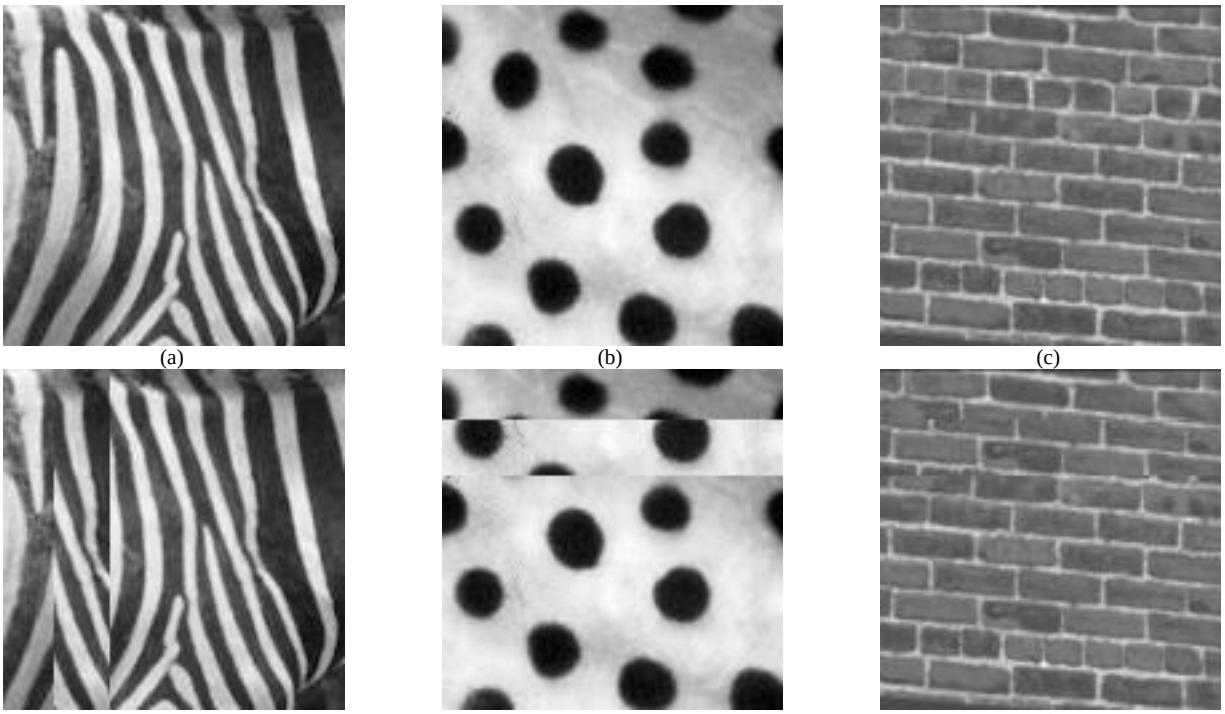


Fig.7. Original and spliced images from Columbia dataset. (a), (b), (c) are authentic category image blocks and (d), (e), (f) are spliced images of them respectively.

These authentic and spliced image blocks are having an entirely homogeneous textured region. Spliced region indicate the cover up done when any portion is cropped and the empty space is filled with homogeneous background. Experimental results from table 4 indicate the change in the signature when the original is forged

5. Discussion of Results

The proposed CBSTR algorithm for authentication is able to identify tampering of image visual content effectively. Performance of the CBSTR algorithm is assessed with public image forgery datasets containing variety of images and authentication results are accurate**.** Our CBSTR based scientific approach provides unique fingerprint of the test images considered irrespective of their size and type. Image integrity can be verified by re-generating the digital signature of the registered image when its credibility needs to be established and authenticated. Internal illustrations of CBIS hold on to IEEE754 floating point system. The CBIS depicted in decimal system helps to verify the image instantly and locate it in database while retrieval. The hash values obtained are purely depending on the pattern of keypoint distribution obtained during feature extraction stage. Most likely the centroid lies where the density of keypoint is high. High value indicates that the centroid obtained through triad relationship of the image lies in the right top portion of the Cartesian coordinate system. The same principle applies for the low value too. Here we verify whether the CBIS of the original and CBS of the query image is same or not. If it is different then we conclude that query image is tampered.

Verification process of Image authentication consists of:

- Generating Content based Image Signature using CBSTR approach.
- Extraction of attached or dissimulated CBIS from storage or image if embedded.
- Comparison of the two CBIS to authenticate whether query image is original or tampered.

The feature based digital signature approach is hierarchical in nature and sensitive to image manipulation due to splicing and copy move forgery. Any location based low level feature descriptors can be considered for feature extraction. CBSTR authentication system is sensitive to slightest manipulation of image content and is reflected in the changed CBIS obtained. It helps to protect against any falsification and detects efficiently. The CBIS of images can be stored in an index file for retrieving image files from database. It can also be stored separately for content verification, our main purpose. The CBIS key can be used for lock-in and unlock image files by investigating officers or agencies and can also be embedded as a watermark. 128-bit CBIS uniquely represent the image and establishes integrity of the image. It is stored in decimal format that helps in determining Just Noticeable Difference during verification. Significant changes for forgery detection can be observed in 5 precisions of decimal part only. The performance of CBSTR approach is evaluated with the hamming distance among 128 bit binary hash of the pristine and forged image represented by (6).

$$d(h_1(x,y),h_2(x,y)) = \frac{1}{w}\sum_{i=1}^{w} | h1(x,y) \otimes h2(x,y) | \quad (6)$$

Ideal hash generated for images with different visual content is dissimilar and their normalized hamming distance must be close to 0.5. Our experimental observation demonstrates the spliced and original images generate a hamming distance near to 0.5 that is agreeable and revealed in Table 4. The hamming distance of the content based image signatures for the images compared are maximally different for all type of feature extracted.

Table 4. Hamming distance for images considered in Fig.7. and results obtained in Table 3.

Images	SIFT	SURF	HOG	HARRIS	MSER
AU_T_002.bmp SP_T_002.bmp	0.36	0.41	0.45	0.31	0.35
AU_T_082.bmp SP_T_082.bmp	0.42	0.32	0.46	0.42	0.44
AU_T_028.bmp SP_T_028.bmp	0.44	0.40	0.42	0.35	0.42

Table 4 contains normalized hamming distance results for Table 3. The proposed CBSTR algorithm used to generate CBIS is fragile. The hard authentication system proposed will not locate the spatial region modified. CBIS based on centre of gravity acts as a unique trait of the image.

6. Conclusion and Future Scope

Scientific investigation approach in a systematic way helps the law agencies to accept or reject the digital evidence produced during trails. Authentication of the semantic visual content is a priority than the image itself. Evidence acquired during image acquisition can be preserved along with the hash value registration to verify its integrity during verification process. Malicious tampering of evidence during investigation or analysis can be verified effectively through our CBSTR algorithm. Our Key point based approach is influenced by the region of high entropy of information contained in the image. Our CBSTR hash function computes fixed size forensic signature that can be used for authentication and validation of the given image. The image signature can be used to identify image in a large database during search.

The distinguished signatures obtained have 100% identification of true positives for the dataset considered. Brightness and contrast increase are considered to be malicious from 10% onwards. It is highly improbable for two different images to generate the same message digest/hash value using our approach. The hash functions are random hash values that are statistically independent for two distinct images of different content. Security perspective of the hash obtained is strong since the entropy of content is considered for key features at level 0. Our hash function is secure since it is impractical for an adversary to maintain the same hash value while changing the underlying image content or to obtain the same. In extension to the current work, exact tampering localization with respect to copy move forgery can be detected using our approach if the image is divided into blocks and individual block signatures are stored separately to compare.

Acknowledgement

We wish to thank JSS Mahavidyapeetha for their constant support and encouragement in our work.

References

[1] Kurosawa, Kenji, Kenro Kuroki, and Naoki Saitoh. "CCD fingerprint method-identification of a video camera from videotaped images." In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, vol. 3, pp. 537-540. IEEE, 1999.

[2] Geradts, Zeno J., Jurrien Bijhold, Martijn Kieft, Kenji Kurosawa, Kenro Kuroki, and Naoki Saitoh. "Methods for identification of images acquired with digital cameras." In *Enabling technologies for law enforcement and security*, vol. 4232, pp. 505-513. International Society for Optics and Photonics, 2001.doi: 10.1117/12.417569

[3] Lukas Jan, Jessica Fridrich, and Miroslav Goljan. "Detecting digital image forgeries using sensor pattern noise." In *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, p. 60720Y. International Society for Optics and Photonics, 2006.

[4] Filler, Tomáš, Jessica Fridrich, and Miroslav Goljan. "Using sensor pattern noise for camera model identification." In *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*, pp. 1296-1299. IEEE, 2008. DOI:10.1109/ICIP.2008.4712000

[5] Alles, Erwin J., Zeno JMH Geradts, and Cor J. Veenman. "Source camera identification for low resolution heavily compressed images." In *Computational Sciences and Its Applications, 2008. ICCSA'08. International Conference on*, pp. 557-567. IEEE, 2008.

[6] Chen, Mo, Jessica Fridrich, Miroslav Goljan, and Jan Lukáš. "Determining image origin and integrity using sensor noise." *IEEE Transactions on Information Forensics and Security* 3, no. 1 (2008): 74-90.

[7] Chen, Mo, Jessica Fridrich, Jan Lukáš, and Miroslav Goljan. "Imaging sensor noise as digital x-ray for revealing forgeries." In *International Workshop on Information Hiding*, pp. 342-358. Springer, Berlin, Heidelberg, 2007.
[8] Li, Yue, and Chang-Tsun Li. "Decomposed photo response non-uniformity for digital forensic analysis." In *International Conference on Forensics in Telecommunications, Information, and Multimedia*, pp. 166-172. Springer, Berlin, Heidelberg, 2009.
[9] Rosenfeld, Kurt, and Husrev Taha Sencar. "A study of the robustness of prnu-based camera identification." In *Media Forensics and Security*, vol. 7254, p. 72540M. International Society for Optics and Photonics, 2009.
[10] Abhishek, Jindal, N. Copy move and splicing forgery detection using deep convolutional neural network, and semantic segmentation. *Multimed ToolsAppl* 80, 35713599(2021). https://doi.org/10.1007/s11042-020-09816-3
[11] Goel, N., Kaur, S., & Bala, R. (2021). Dual branch convolutional neural network for copy move forgery detection. *IET Image Processing*.
[12] Singhal, S., & Ranga, V. (2021). Passive authentication image forgery detection using multilayer cnn. In *Mobile Radio Communications and 5G Networks* (pp. 237-249). Springer, Singapore.
[13] Surbhi Sharma, Umesh Ghanekar, "Spliced Image Classification and Tampered Region Localization Using Local Directional Pattern", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.11, No.3, pp. 35-42, 2019. DOI:10.5815/ijigsp.2019.03.05
[14] Saurabh Agarwal, Satish Chand, "Image Forgery Detection using Multi Scale Entropy Filter and Local Phase Quantization", International Journal of Image, Graphics and Signal Processing(IJIGSP), vol.7, no.10, pp.78-85, 2015. DOI:10.5815/ijigsp.2015.10.08
[15] Castillo Camacho, I., & Wang, K. (2021). A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. *Journal of Imaging*, *7*(4), 69.
[16] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. "Secure spread spectrum watermarking for multimedia."*Image Processing, IEEE Transactions on* 6, no. 12 (1997): 1673-1687.
[17] Fridrich, J., Goljan, M., & Baldoza, A. C. (2000). New fragile authentication watermark for images. In *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)* (Vol. 1, pp. 446-449). IEEE.
[18] Maeno, K., Sun, Q., Chang, S. F., & Suto, M. (2006). New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization. *IEEE Transactions on Multimedia*, *8*(1), 32-45.
[19] Fei, C., Kundur, D., & Kwong, R. H. (2006). Analysis and design of secure watermark-based authentication systems. *IEEE transactions on information forensics and security*, *1*(1), 43-55.
[20] Mitrea, M., & Hasnaoui, M. (2013). Semi-fragile watermarking between theory and practice. *Proceedings of the Romanian Academy*, 328-327.
[21] Feng, G., & Huang, K. (2013, October). H. 264 video standard based zero watermarking technology. In *2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID)* (pp. 1-4). IEEE.
[22] Wang, J. T., Yang, W. H., Wang, P. C., & Chang, Y. T. (2014, June). A novel chaos sequence based 3d fragile watermarking scheme. In *2014 International Symposium on Computer, Consumer and Control* (pp. 745-748). IEEE.
[23] Kadam, B. D., & Metkar, S. P. (2014, December). Digital video watermarking based on dither modulation. In *2014 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.
[24] Fallahpour, M., Shirmohammadi, S., Semsarzadeh, M., & Zhao, J. (2014). Tampering detection in compressed digital video using watermarking. *IEEE Transactions on Instrumentation and Measurement*, *63*(5), 1057-1072.
[25] Anuja Dixit, Rahul Dixit, "A Review on Digital Image Watermarking Techniques", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.4, pp.56-66, 2017. DOI:10.5815/ijigsp.2017.04.07
[26] Schneider, M., & Chang, S. F. (1996, September). A robust content based digital signature for image authentication. In *Proceedings of 3rd IEEE International Conference on Image Processing* (Vol. 3, pp. 227-230). IEEE.
[27] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C John Wiley & Sons. *Inc., America*.
[28] Boncelet, C. (2005, September). Image authentication and tamperproofing for noisy channels. In *IEEE International Conference on Image Processing 2005* (Vol. 1, pp. I-677). IEEE.
[29] Lu, C. S., & Liao, H. Y. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme. *IEEE transactions on multimedia*, *5*(2), 161-173.
[30] Monga, V., Banerjee, A., & Evans, B. L. (2006). A clustering based approach to perceptual image hashing. *IEEE Transactions on Information Forensics and Security*, *1*(1), 68-79.
[31] Swaminathan, A., Mao, Y., & Wu, M. (2006). Robust and secure image hashing. *IEEE Transactions on Information Forensics and security*, *1*(2), 215-230.
[32] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.
[33] V. Monga and M. K. Mihcak, "Robust and secure image hashing via non-negative matrix factorizations," IEEE Trans. Inf. Forensics Security,vol. 2, no. 3, pp. 376–390, Sep. 2007.
[34] Z. Tang, S.Wang,X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.
[35] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE,Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.
[36] W. Lu and M.Wu, "Multimedia forensic hash based on visual words," in Proc. IEEE Conf. on Image Processing, Hong Kong, 2010, pp.989–992
[37] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection," IEEE Trans. Image Process., vol. 19, no. 4, pp.981–994, Apr. 2010.
[38] K. Fouad and J. Jianmin, "Analysis of the security of perceptual image hashing based on non-negative matrix factorization," IEEE Signal Process. Lett., vol. 17, no. 1, pp. 43–46, Jan. 2010.
[39] F. Ahmed, M. Y. Siyal, and V. U. Abbas, "A secure and robust hash based scheme for image authentication," Signal Process., vol. 90, no. 5, pp. 1456–1470, 2010.
[40] Y. Lei, Y.Wang, and J. Huang, "Robust image hash inRadon transform domain for authentication," Signal Process.: Image

Commun., vol. 26,no. 6, pp. 280–288, 2011.
[41] Z. Tang, S. Wang, X. Zhang, W. Wei, and Y. Zhao, "Lexicographical framework for image hashing with implementation based on DCT and NMF," Multimedia Tools Applicat., vol. 52, no. 2–3, pp. 325–345, 2011.
[42] X. Lv and Z. J. Wang, "Perceptual image hashing based on shape contexts and local feature points," IEEE Trans. Inf. Forensics Security, vol.7, no. 3, pp. 1081–1093, Jun. 2012.
[43] Robust Hashing for Image Authentication UsingZernike Moments and Local Features Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Member, IEEE
[44] Li Y. Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int. 2013; 224(1–3):59–67.
[45] Image Forgery Detection using Multidimensional Spectral Hashing based Polar Cosine Transform J. Granty Regina Elwin1* and G. Kousalya2
[46] Li P, Wang M, Cheng J, Xu C, Lu H. Spectral hashing with semantically consistent graph for image indexing. IEEE Trans Multimed. 2013 Jan; 15(1):141–52.
[47] Mikolajczyk, Krystian, and Cordelia Schmid. "Scale & affine invariant interest point detectors." *International journal of computer vision* 60, no. 1 (2004): 63-86. DOI:10.1023/B:VISI.0000027790.02288.f2
[48] Zhu,Qiang, Mei-Chen Yeh, Kwang- Ting Cheng, and Shai Avidan. "Fast human detection using a cascade of histograms of oriented gradients." In computer Vision and Pattern Recognition, 2006 IEEE Computer Society conference on,vol.2,pp.1491-1498.IEEE,2006
[49] SIFT (Lowe, 2004), SURF (Bay et al., 2006), HOG (Subramanyam and Emmanuel, 2012), Harris (Mikolajczyk and Schmid 2004) and MSER (Matas et al., 2004) Lowe, David G. "Distinctive image features from scale-invariant keypoints."*International journal of computer vision* 60.2 (2004): 91-110.DOI:https://doi.org/10.1023/B:VISI.0000029664.99615.94
[50] Bay, Herbert, Tinne Tuytelaars, and Luc Van Gool. "Surf: Speeded up robust features." In *European conference on computer vision*, pp. 404-417. Springer, Berlin, Heidelberg, 2006. DOI:DOI:https://doi.org/10.1007/11744023_32
[51] Matas, Jiri, Ondrej Chum, Martin Urban, and Tomás Pajdla. "Robust wide-baseline stereo from maximally stable extremal regions." *Image and vision computing* 22, no. 10 (2004): 761-767. DOI:10.1016/j.imavis.2004.02.006
[52] Chennamma, H. R., Lalitha Rangarajan, and M. S. Rao. "Robust near duplicate image matching for digital image forensics."*International Journal of Digital Crime and Forensics (IJDCF)* 1.3 (2009): 62-79.DOI: 10.4018/jdcf.2009070104
[53] I. Amerini,L Ballan,R.Caldelli, A. Del Bimbo, G. serra. "A SIFT based forensic method for copy move attack detection and transformation recovery", IEEE transaction for information forensics and Security, vol 6, issue 3, pp. 1099-1110,2011.
[54] http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm.
[55] V. Christlein, CRiess, J Jordan, C. Riess, E. Angelopoulou: "An Evaluation of popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, Vol. 7, no. 6, pp. 1841-1854,2012.

Authors' Profiles

Dr. Sowmya received her doctoral degree in "Faculty of computer and Information Sciences" in the year 2020 from Visvesvaraya Technological University, Belgaum, Karnataka, India. She is working as an Assistant professor in the Department of Information Science and Engineering at JSS Academy of Technical Education, Bangalore affiliated to Visvesvaraya technological university. Her area of research includes Video and Image Processing, Image Forensics, Video forensics & Machine learning.

Dr. Chennamma received her graduate degree in Computer Applications with distinction in the year 2003, Visvesvaraya Technological University, India and completed her Ph.D. in Computer Science from the University of Mysore in the area of Digital Image Forensics in 2011. Subsequently, she continued her Post Doctoral research in the Department of Computer Science and Engineering, University of North Texas, USA in 2012. Currently, she is an Associate Professor in the Department of Master of Computer Applications, JSS Science and Technology University, Mysuru, India. Previously, Chennamma served as a Senior Research Fellow (SRF) in National Computer Forensic Laboratory, Ministry of Home Affairs, Government of India, Hyderabad. She served as a Project Trainee for an year at the National Aerospace Laboratory (NAL), Bangalore and she also served as a software engineer for a year in a multinational software company, Bangalore. Chennamma is the recipient of two "Best Scientific Paper Awards" in the All India Forensic Science Conference, Kolkata, India in the year 2007 and another in National Cyber Safety and Security Standards Summit'17, Hyderabad, India. Her current research interests are Image Forensics, Pattern Recognition, Computer-Generated Image Forensics and Image Retrieval.

How to cite this paper: Sowmya K. N., H. R. Chennamma, "Image Hashing Through Spatio-triad Relationship", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.5, pp.60-72, 2022. DOI:10.5815/ijcnis.2022.05.05