Image Hash Minimization for Tamper Detection

Authors: Subhajit Maity & Ram Kumar Karsh

Presented by,

Subhajit Maity

Department of ECE, Jalpaiguri Govt. Engg. College

Paper ID : 46, ICAPR 2017, 28th -30th December, 2017, Bangalore, India

Outline

- **Introduction**
  - *What is Image Tampering*
  - *Why do we need to detect Image Tampering*
  - *Different methods for Image Tampering & Detection*
- **Concept of the proposed method**
  - *How did we do it*
  - *What's new about us*
- **Resources used**
- **Results & Comparison**
  - *Our Findings*
  - *How Better are we from the previous works*
- **Conclusion & Discussion**
  - *Looking into the future*

Introduction

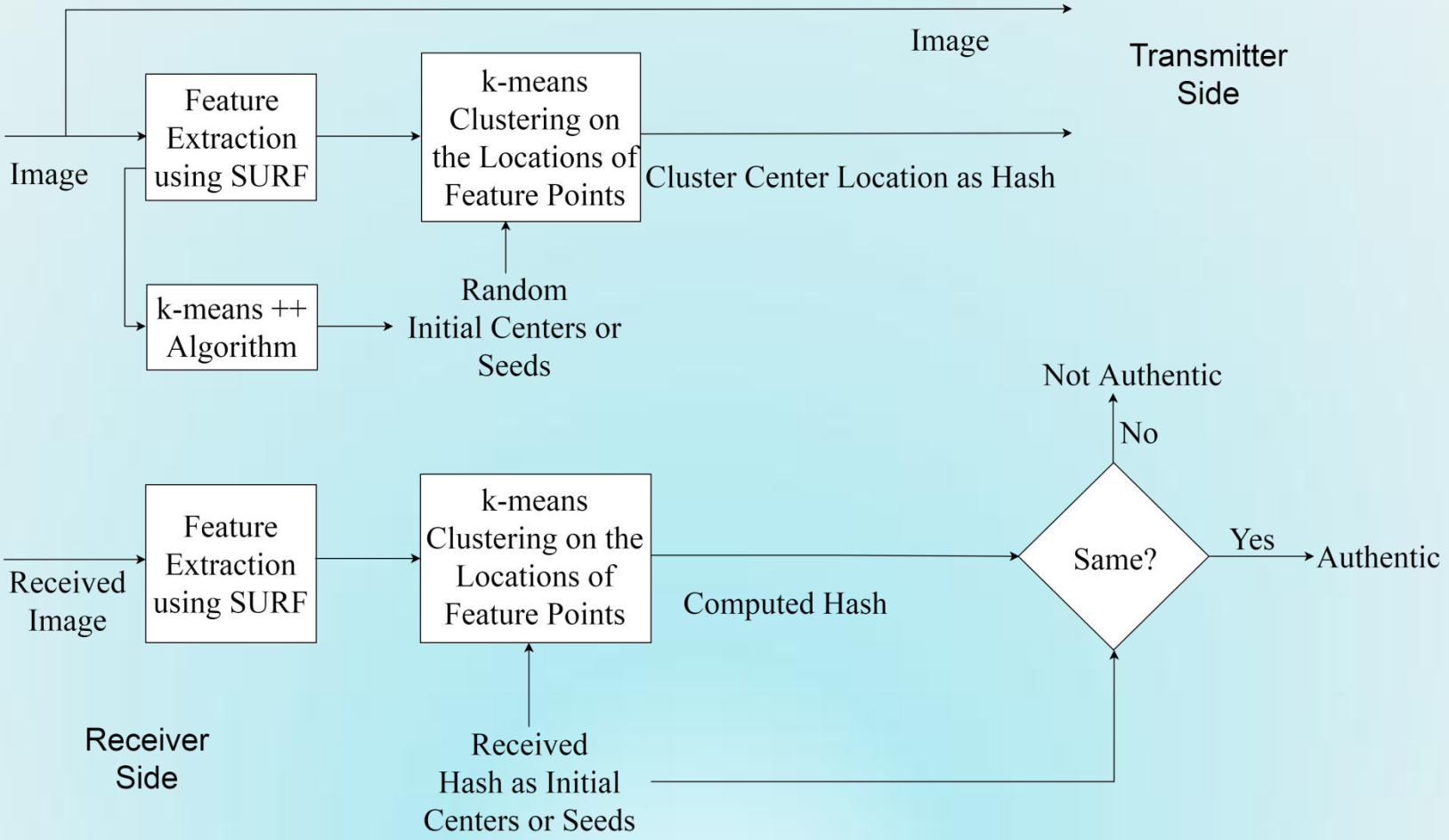
- Where all these started at the very beginning
  - *How **Artificial Intelligence (AI)** changed our life*
  - *The **problem of Classification** in AI*
  - *The solution of **Clustering in Machine Learning***
  - *Concept of Clustering in **Object Detection***

- How does it fit in the bigger picture
- What is **Image Tampering**
- Detection of Image Tampering
  - *Significance*
  - *Role in Data Protection & Security*

Introduction contd.

- **Different types of Image Tampering & Detection**
  - *Copy – Move Forgery*
  - *Copied Window Detection*
  - *Random Tampering*
  - *Concept of Image Hashing*
- Reason behind Popularity of Image Hashing
- Importance of Hash Minimization
- **Motivation behind the Work**
  - *Most of the previous works emphasized the detection techniques while none considers to optimization of the expense in resources.*
  - *Generally some low level features are excluded to define a hash length which degrades the detection accuracy.*

Proposed Method



How the Algorithm works

Proposed Method contd.

Comparison of Image Hashes

1. The hashes are nothing but the location of the cluster centers. The cluster center locations (hash) received from the sender is used as the initial center location while performing clustering on detected key-points from the received image.
2. The centers calculated at the receiver side is compared to the hash received if they remains same.

3. If the location of the centers change, the no. of objects or the location of objects changed. And we can say the image is tampered.

Proposed Method contd.

4. The detected key-points change due to several content preserving operations performed. So it is unjustified to determine if an image is tampered or not based only on the exact match of the image hashes.

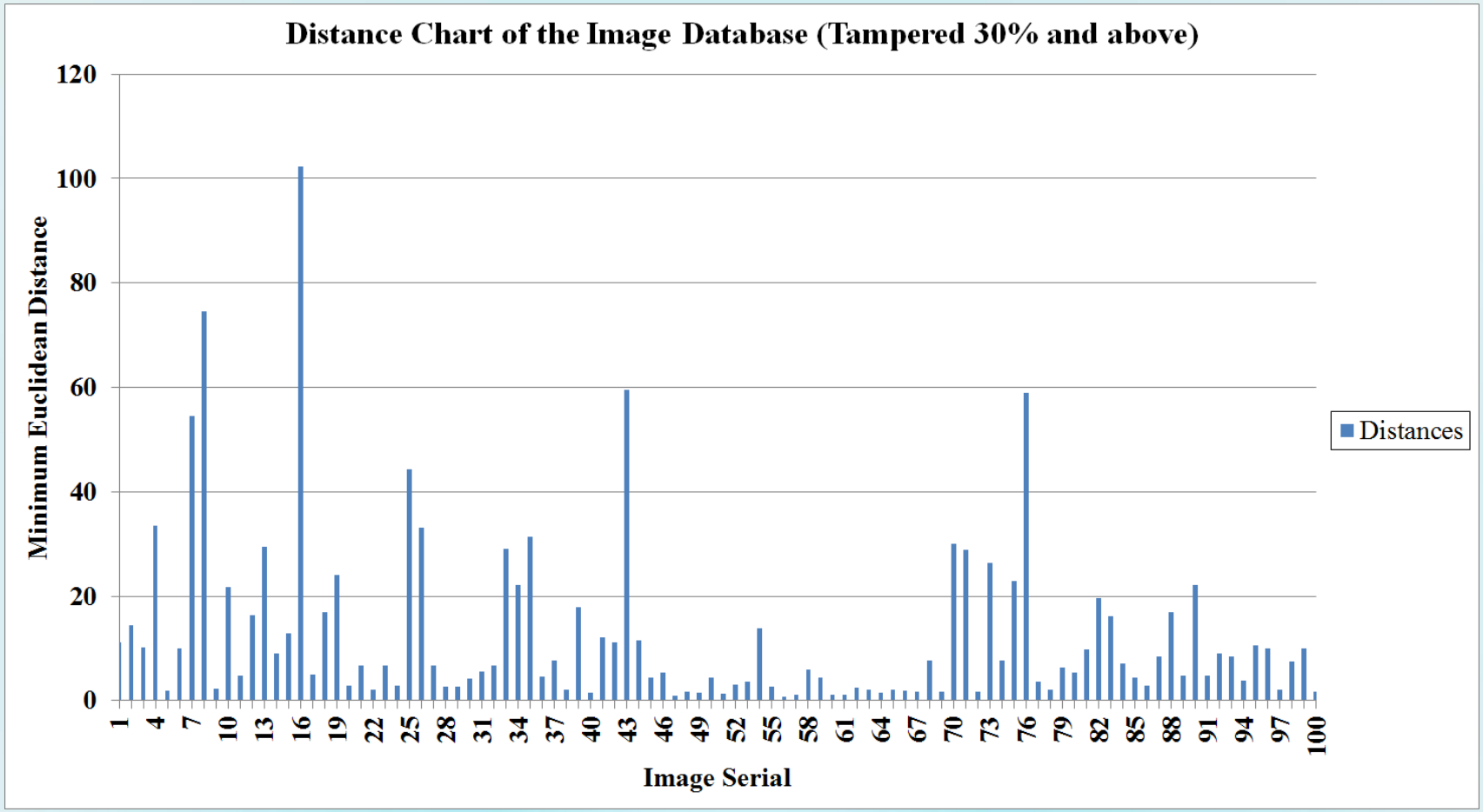
5. The comparison is done using the **minimum of the Euclidean distance measured between locations of the calculated cluster centers of the received images and the cluster centers received as hash**. This defines the closeness of the images.

Resources Used

- **Standard benchmark images** from SIPI image database for detection of not-tampered images
- We used **CASIA v2.0 Tampered image detection evaluation database** for all standard tamper detection experimentation where the **tampered area is at least 30% of the image.**

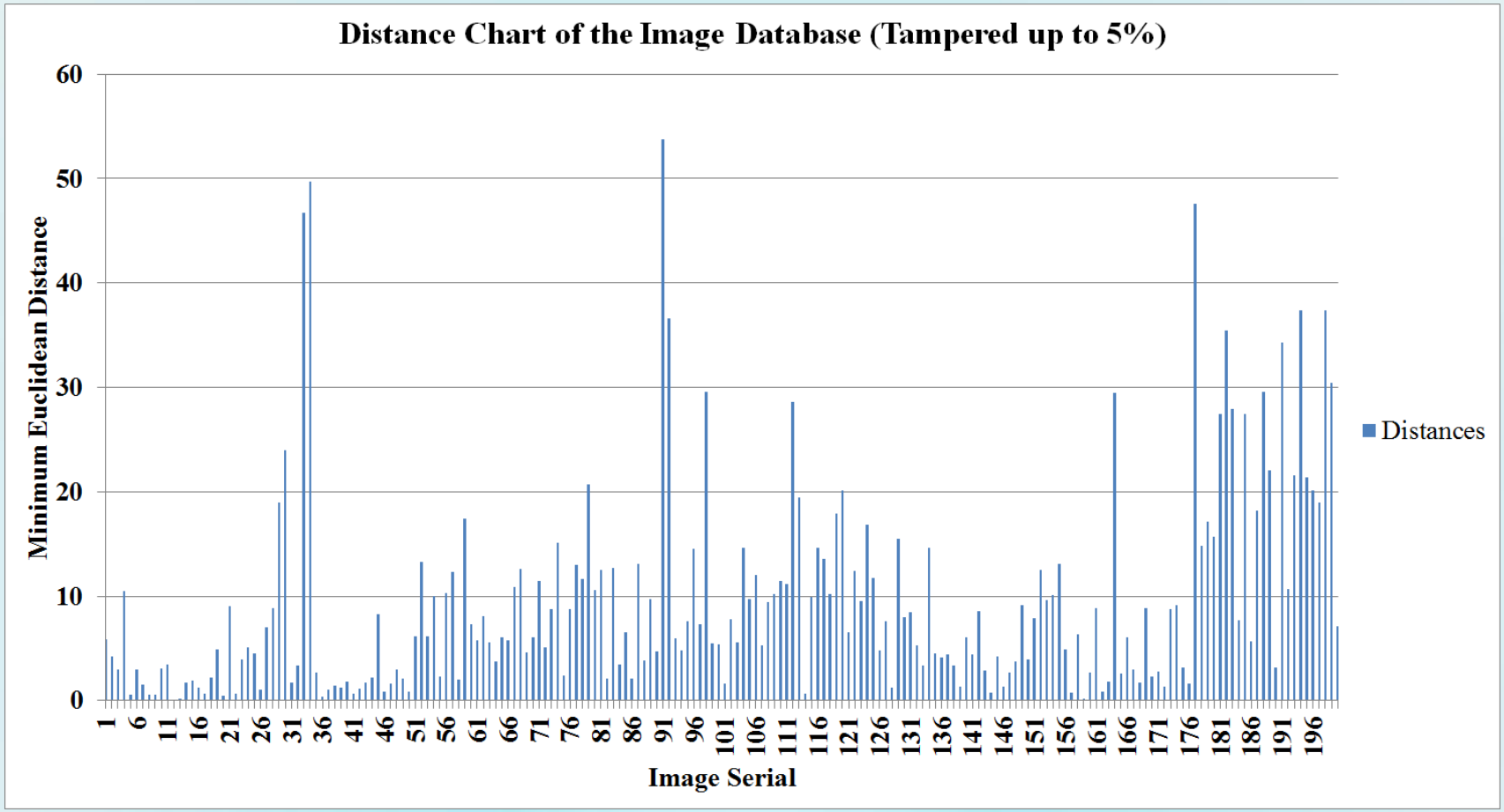
- Another database is used where **200 images** were taken from free to use web sources and **tampered at an area of 5% or less** with respect to the image area. We used this database of images where the tampered area is maximum 5% of the image.

Results & Comparison



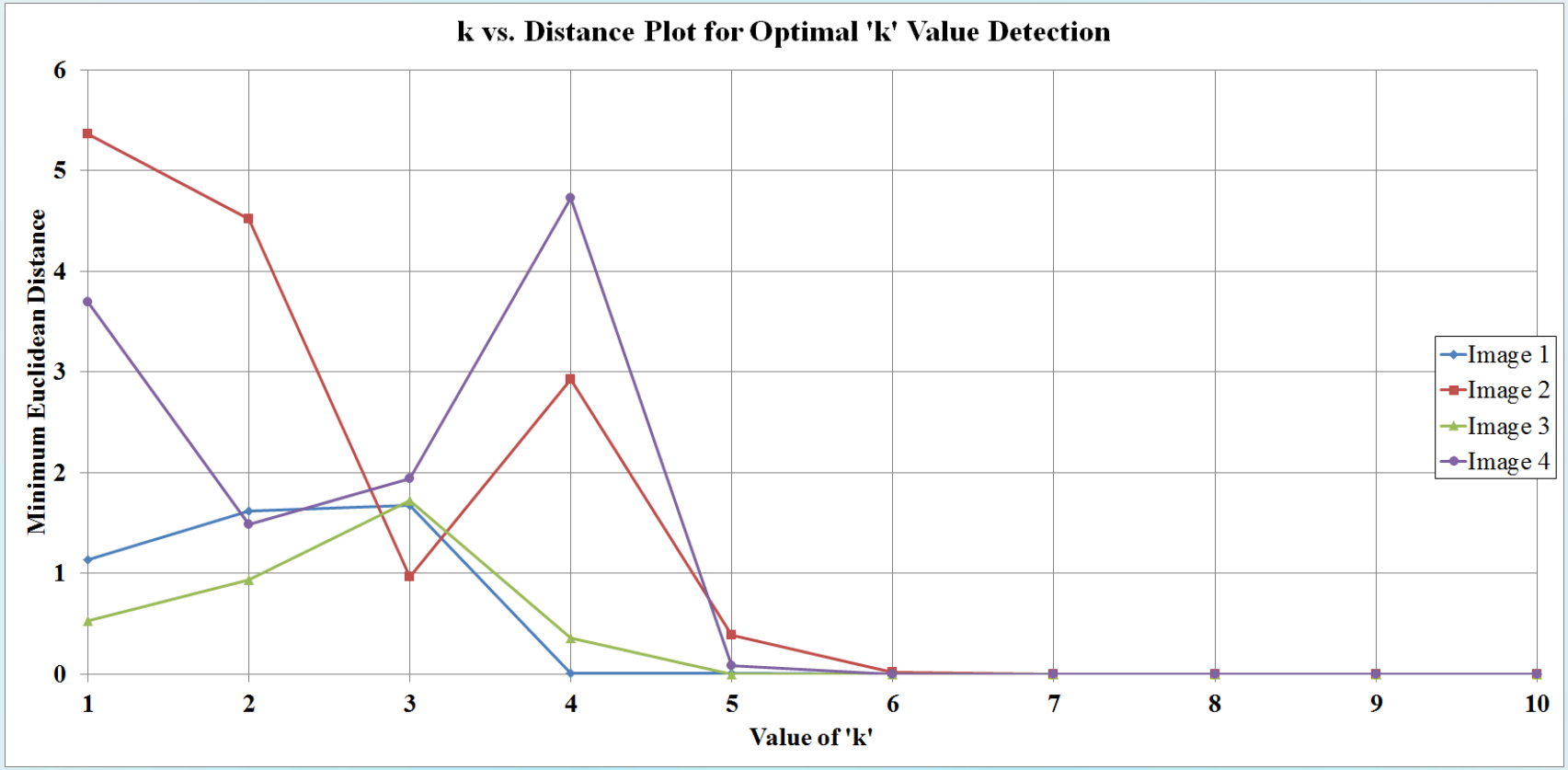
Distance bar chart for tampered area of minimum 30%

Results & Comparison contd.



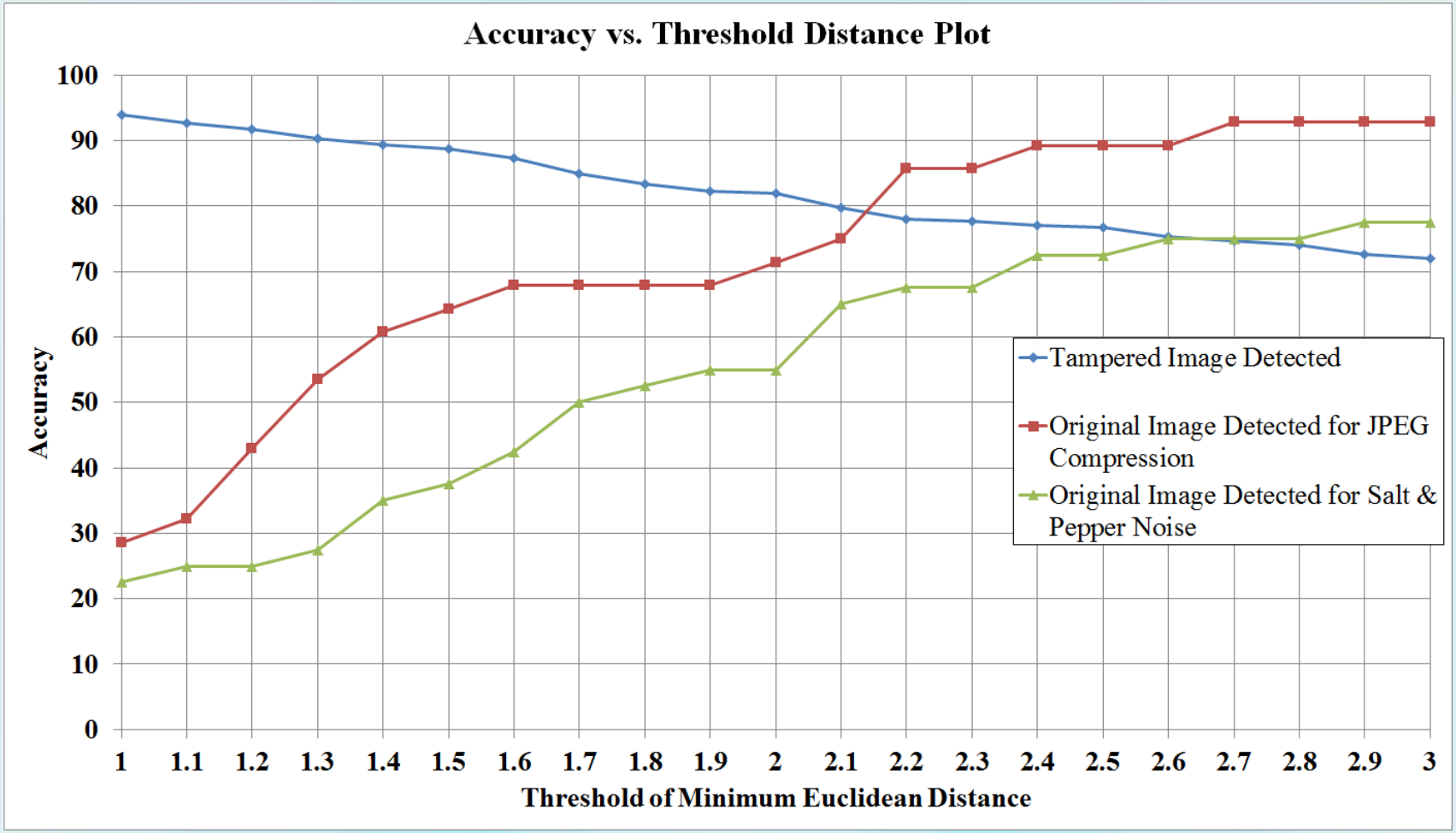
Distance bar chart for tampered area of maximum 5%

Results & Comparison contd.



'k' vs. Distance plot for detection of optimal no. of cluster centers. The highest average shows the optimal value.

Results & Comparison contd.



Detection Accuracy vs. Threshold Distance plot

Results & Comparison contd.

- The optimally detected Threshold of minimum of the Euclidean distance for tamper detection is **2.3922** and the optimally detected **value of 'k' is 1**. At these values the detection accuracy of both tampered and not-tampered images is **77%**.
- **Comparison with State-of-the-Art method**

Parameters	Yan et al. [2017] *	Proposed Method
Hash Length	634 digits	64 bits
Accuracy of Detection	60% (approximately)	77%

* *Yan et al. "Image Alignment-Based Multi-Region Matching for Object-Level Tampering Detection," IEEE Transactions on Information Forensics and Security, Feb. 2017, vol. 12, no. 2, pp. 377-391.*

Conclusion & Discussion

- The hash length minimization is achieved successfully and the detection accuracy improved as well. This is because none of the features is compromised for detection.
- We attempted to detect tampered area even less than 5% which is not done before.

- **Future Scopes of the work are as follows,**
  - *Unification of a developed algorithm for detection of any kind of tampering including Copy-Move forgery.*
  - *A step towards detection of image tampering using 'Zero Hash'.*

Thank You

Paper ID : 46, ICAPR 2017, 28th -30th December, 2017, Bangalore, India