# Robust Image Authentication Using Optimized Haralick Features Based on Genetic Algorithm

K.Alice[1]
{k_alice_suresh@yahoo.com[1]}

Department of IT, Bharath Institute of Higher Education and Research,
Selaiyur,Tambaram,Chennai, Tamilnadu, 600 073, India.[1]

**Abstract.** Recent development in multimedia data increases the role of digital images in many applications. As a result,content based image authentication with an aid of feature extraction techniques has a great impact. It suffers a serious drawback of increased computational complexity due to the availability of irrelevant and interdependent features, which contains no useful information about the image. In the proposed authentication system to decrease the complexity, not all haralick features are used but only the most influencing features that contain critical information about the image is used in hash generation. Feature selection based on chaotic genetic feature selection optimization algorithm is used to optimize the haralick features without compromising the accuracy of the system. A comparison on the system performance with all the features and with optimized features is performed. Experiment results shows resultsusing optimized features are similar to the results of using all the features..

**Keywords:** Genetic Algorithm, Optimized Haralick Feature, Chaotic Genetic Feature Selection optimization algorithm, Circular Blocks, Rotation invariance, Authentication system..

## 1 Introduction

The widespread use of digital images in multimedia data increased the need for image authentication which validates the uniqueness of image. For an image, it is enough to authenticate the content of the image rather than the image as a whole. Image authentication is highly essential in various applications like medical images, court evidence images, property documents, quality control images, military target images etc., where alteration in image cause severe damage.Schneider et al [17] used histogram as image features to generated hash code which suffered a drawback of long signatures. Nilesh et al [13] in his paper generated hash using fuzzy color histogram and it fails to detect color pixel manipulation. Another useful feature to represent image is edges as proposed by Canny [3] and it does not report recover of lost data. DCT,DWT and wavelet transform Storck et al[19], Wu et al[23], Lin et al[10],Sun et al[20]are also used to represent image content but it cannot recover lost data. In Kailasanathan et al [8] uses statistical measurese to generate lengthy hash code. Moments are global descriptors [9] are set of values that represent the information contained in the image.

Two or more hash generation techniques are mixed up in hash code generation process. Seyedamir [18] uses strict and selective authentication using AMAC. Tri.H.Nguyen et al[21] combines SVD and DWT to generate watermark but problem of localization and tamper recover was addressed. Lima Sebastian et al [9] and Yan Zhao et al[24] use global and local features to produce hash and does not address image recover in case of even accidental loss of data.Obaid et al [14] generated a watermark usinginformation of spatial and frequency domain also partial recovery of lost content is addressed using RS codes. M.F.Hashmi at el [11], combines SVM and HMM classifiers to calssify the image as authentic or not.

The basic requirement of a good authentication system can be given as follows [2]: Robustness- The system should tolerate content preserving transformations. Security- The system should be able to protect the data from malicious attack. Sensitivity- The system should detect any content modifications or manipulations. Localization - The system should be able to locate the area of tampering. Recovery- The system should be able to reconstruct the tampered regions. Complexity - The system must be neither complex nor slow. Portability- The system should be able to hold image and its signature together.Features are used to describe the content of an image. Not all the features contain useful information about the image. Feature selection [7] is an optimization process that reduces the dimensionalities in the underlying feature space. Suppose there are n numbers of features then there will be $2^n$ possible subsets for that feature set.

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308648

Feature selection is the process of selecting k < n features from that feature subset that are most influencing features and that best describe the image without compromising the accuracy of the system. Feature selection process removes irrelevant and interdependent features, thereby reducing the time complexity in features analysis and training. Also it reduces the overall computational model.

Optimization problem is a mathematical term that is used to either maximize or minimize any given objective function. Objective function is problem specific. Many optimization algorithms are widely used now a day; which include both local and global optimization. Unlike local optimization which uses a single design point, global optimization uses a set of design points to find an optimum solution. Global optimization algorithms are much preferred since they provide a global optimal solution rather than converging to a local optimal solution. The most commonly used global optimization algorithm [6] includes

- Genetic algorithm
- Particle swarm optimization
- Colony optimization
- Harmony search
- DIRECT deterministic algorithm
- Tabu search
- Evolutionary programming
- Genetic programming etc.

Out of the above mentioned algorithm, each having its own advantages and limitations, Genetic algorithm is the most commonly used algorithm because it is a probabilistic, robust and heuristic search algorithm that depends on natural selection. It is a transparent algorithm that always provides a sub optimal solution. It can be applied to any search space in any domain. Premature convergence is a major problem of genetic algorithm that increases the number of iterations in achieving global optimal solution.Many advanced versions of genetic algorithm are also introduced by researchers to eliminate the problem of premature convergence.Chaotic Genetic optimization algorithm is one such advanced algorithm that has the potential to provide global optimal solution by introducing chaotic variables in GA processes thereby eliminating local convergence.

The paper is organized as follows: Section II gives a brief description about Genetic Algorithm and Chaotic Genetic algorithm. Section III explains our proposed work. Section IV provides a performance analysis based on the requirement of authentication system. Section V concludes the paper.

## 2 Methods and Materials

**Genetic Algorithm (GA)**

Genetic Algorithm is a bio inspired optimization algorithm that works on the principle of survival of the fittest. The basic idea of GA is borrowed from the biological process of survival and adaptation. GA is different from classical search algorithms in the following ways: There is no limitation in the search space;it uses natural selection criteria, parallel computation of the population of solutions.GA uses a simple chromosome like data structures and applies techniques inspired from natural evolution like selection, mutation and crossover to these data structures so as to retain the critical information.

The general steps in genetic algorithm are as shown in Figure 1.

Step 1: Randomly create initial population

Step 2: The population is ranked based on fitness function

Step 3: Parents are randomly selected for reproduction. While selecting the parents higher ranked individuals are given preference usually

Step 4: Create children by randomly mixing the selected parents by process called crossover and mutation.

Step 5: Calculate the fitness function for the children and check whether desired solution is obtained. Otherwise if children fitness is better than parent remove parent from the population and add children

Step 6: Repeat steps 3 and 4 with the newly generated population until optimal solution is reached.

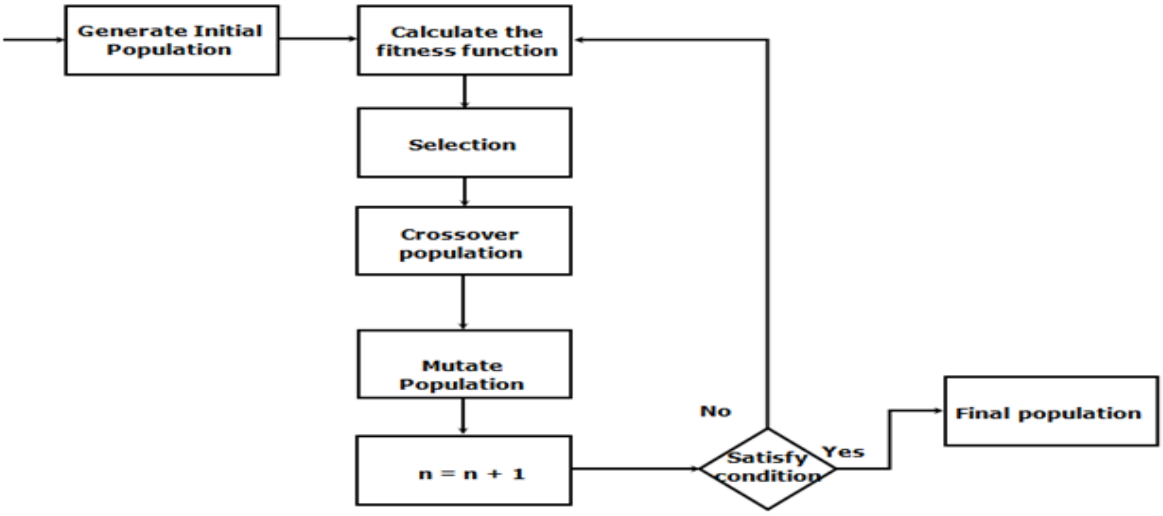



**Figure 1: Basic Block diagram of Genetic Algorithm**

If Pc (probability of crossover) is too large, then the genetic pattern is damaged easily and individual structures with high fitness value will be destroyed soon [12]. If Pc is very small, the convergence becomes slow. If Pm (probability of mutation) is too large, GA becomes similar to random search algorithm. if Pm is too small, it will be very difficult to produce new individual structures. If the population size is increased, this will reduce the number of iterations required for global optimum.GA is probabilistic and not deterministic. It is evolved into a better and better solution in each iteration. It works with the coding of solution and not with solutions themselves. The presence of a feature in a feature subset is encoded as 1 it is encoded otherwise as 0. Genetic algorithm suffers a serious drawback of converging to either local maxima or local minima. Due to this drawback of premature convergence the number of iterations for global optimal solution is also increased. This problem of premature convergence can be avoided by using advanced genetic algorithm like chaotic genetic algorithm which introduces chaotic variables to create diversity in population so as to avoid local convergence.

**Chaotic genetic Algorithm (CGA)**

Chaos is a confusing behavior of a nonlinear dynamic system that depends on initial conditions and is described using deterministic algorithm. Chaos feature is very important that improves the efficiency of Genetic Algorithm. The three main properties [15] of chaotic behavior are Ergodicity, Randomness, and high sensitive to initial condition. Ergodicity property allows the chaotic variables to travel in all states without repetition in a certain range of space and hence avoid falling into local minimum solution in optimization problems. Sensitivity to initial condition maintains population diversity, that is, no two identical new populations are very close.

Chaotic genetic algorithm is similar to ordinary genetic algorithm but to introduce chaotic behavior instead of random sequence used for crossover and mutation, logistic map output sequences is used for crossover and mutation. The basic steps in CGA are as shown in figure 2. And by comparing figure 1 and figure 2 the difference shows that the chaotic behavior in CGA is implemented using logistic chaotic function. The logistic chaotic function provides the necessary chaotic behavior that maintains population diversity, Randomness, and Ergodicity and has the potential to produce global optimal solution.

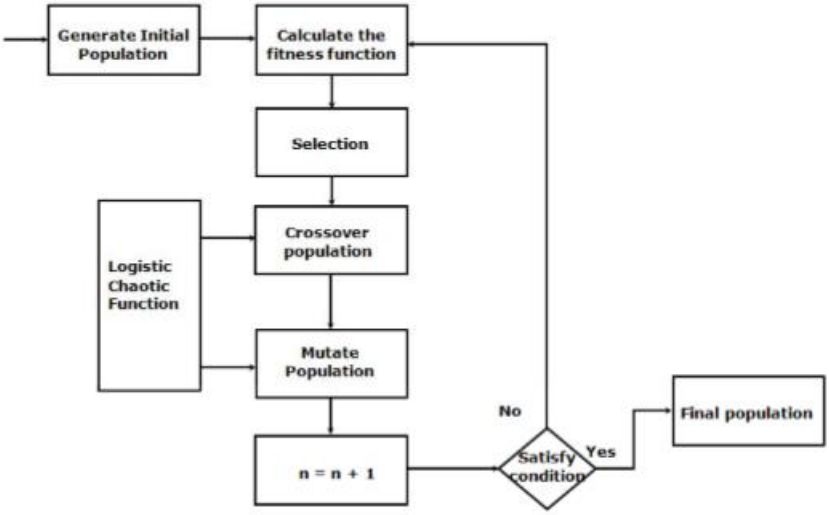



**Figure 2: Basic Block Diagram of Chaotic Genetic Algorithm**

**Logistic Chaotic Function**

The simplest form of chaotic map is the logistic map [7]. This map is a polynomial mapping of degree 2 given as

$$Z_{n+1} = r\, Z_n(1-Z_n) \quad \text{where } Z_n \in \{0,1\}$$

Here 'r' should take values between 0 and 4. If r € {0,3}, the behavior is convergent. If r € {3,3.5}, then periodic. If r € {3.5 ,4}, it represents chaotic behavior. So to ensure chaotic behavior r should be taken as 4.

## 3 Proposed Image Authentication System

**Pre-processing**

In preprocessing stage the image is converted to a standard 512 X 512 square image using bilinear interpolation which is done to reduce computational complexity. Since color information is not an important discriminating parameter, the image is converted to gray scale image. Then a low pass Gaussian filter is applied to remove any unnecessary additive noise. The size of the image is fixed to have uniform complexity in handling all images.

Next the preprocessed image is subjected to image division to generate local features. Instead of dividing the image into square blocks to achieve rotation invariance the image is divided into equal area circular blocks. The division of blocks algorithm is [25]as shown below

**Step 1:** The center ($x_c$,yc) for the set of circular blocks is given as where m=512 is the size of image

$$if\ m = even \begin{cases} x_c = \dfrac{m}{2} + 0.5 \\ y_c = \dfrac{m}{2} + 0.5 \end{cases} \quad if\ m = odd \begin{cases} x_c = \dfrac{(m+1)}{2} \\ y_c = \dfrac{(m+1)}{2} \end{cases}$$

**Step 2:**The radius $r_k$(k=1,2,3,….n) of each concentric circle from the center is given as where n is the number of rings and is 64

$r_1$-radius of the inner circle = $\sqrt{\frac{\mu_A}{\pi}}$. Where $\mu_A$is the average area of each ring and is given as A/n

$r_n$-radius of the outer circle=floor(m/2).

$r_k$ - radius of the intermediate circle $r_k$(k=2,3,….n-1) = $\sqrt{\frac{\mu_A + \pi(r_{k-1})^2}{\pi}}$.

**Step 3:** The distance from $q_{ij}(x_i,y_j)$ to the image center $x_c,y_c$can be measured using Euclidean distance

$d_{ij} = \sqrt{(x_i - x_c)^2 + (y_j - y_c)^2}$.

The set of pixels that form each ring block can be obtained using

$R_1=\{q_{ij}|d_{ij} \leq r_1\}$and $R_k=\{q_{ij}|r_{k-1} < d_{ij} \leq r_1\}$ where k={2,3…n}

Now each $R_k$ for k= {1,2,3….n} will contain the set of pixels of the circular blocks of equal area that forms the image .

First the center of the image is calculated in step 1. Then the radius if n concentric circular blocks are calculated in step 2 and then the collection of pixels that form a specific circular block is identified based on the distance of radius in step 3. The result of this algorithm is a group of 64 blocks of pixels grouped together to form 64 circular block

**Feature Extraction**

The image features are extracted using first 13 Haralick features [16] as listed in Table 2. Haralick features are texture features that best represent the content of the image. They have proven to provide good results in literature. The Maximal Correlation Coefficient feature is not used in feature representation to reduce computational complexity.

Table 1: Haralick Features

| Sl | Haralick Features | | |
|---|---|---|---|
| 1 | Angular ond Moment | 8 | Sum Entropy |
| 2. | Contrast | 9 | Entropy |
| 3 | Correlation | 10 | Difference variance |
| 4 | Sum of ares: Variance | 11 | Difference Entropy |
| 5 | Inverse ference ment | 12 | Information Measures correlation 1 |
| 6 | Sum Average | 13 | Information Measures correlation 2 |
| 7 | Sum of iance | 14 | Maximum Correlation efficient |

The proposed system combines these haralick features with circular blocks to improve the hash performance. For an image, 13 haralick features are extracted. But always, not all features will contain the critical information. So the most influencing feature that contains the critical information about a particular image has to be selected using a proper feature selection algorithm.

**Feature Selection**

Features are used to describe the content of an image. Feature selection is also called as attribute selection [7] is an optimization algorithm.The "Curse of Dimensionality" is the common term used to refer the more large number of features available in the dataset and makes the methods or algorithms to struggle in clustering or classification. Feature selection is a way to filter the irrelevant and redundant features available in the data without compromising the accuracy of actual feature representation. Feature selection is a problem of finding a reduced feature subset while retaining the accuracy in representing the original features. Genetic algorithm is the most commonly used feature selection algorithm. Many advanced versions of genetic algorithm is introduced by researchers to eliminate the problem of permeating convergence. Chaotic Genetic Feature selection optimization (CGFSO) algorithm [7] is one such algorithm that has the potential to provide global optimal solution thereby eliminating local convergence by introducing chaotic variables in GA processes.

**Chaos Genetic Feature selection optimization (CGFSO) Algorithm**

The input will be a set of all 13 Haralick features. Features will not be used directly by the algorithm instead coding of feature subset is given as input. Each individual is represented as ($a_1,a_2,a_3,\ldots a_n$) where each $a_i$corresponds to the ith feature. If $a_i$=1, feature is selected; else $a_i$=0. For each individual, fitness function will be evaluated. The two key factors used in designing the fitness function are classification accuracy and feature cost.

Individual with high classification accuracy and low feature cost has the high probability to be in the next generation. Fitness function [6] identifies the suitability of the solution. Fitness function is given as follows.

$$f(x) = \sqrt{Precision(x)^2 + Recall(x)^2} - \lambda \times \frac{\delta(x) \times cost(x)}{Precision(x) + Recall(x) + 1} + cost_{max}$$

Where Precision (x) - test precision ratio
Recall (x) - test recall ratio
Cost(x) - sum of measurement cost of the feature subset represented by x
$\lambda$ - the weighing factor ranges from 0 to 1.
$Cost_{max}$ - the sum of all outcomes measured with all 14 features and is the upper bound value.
$\delta(x) = 1$ then x feature is included otherwise 0.

The search in the feature space, CGFSO algorithm works as follows. By taking a single image at a time, the following operations were done:

**Algorithm**

- Input to algorithm is set of 13 Haralick Features, $P_m$ (Probability of mutation)and $P_c$(Probability of crossover)
- Step-1 Initial Population P(0) is a non-empty subset of all Haralick features and iteration K=0
- Step-2 Evaluate the fitness function f(x) for the population
- Step-3 Select $1/3^{rd}$ of population that has top most fitness value and let his be P(k+1)
- Step-4 Perform logistic chaotic crossover operation for P(k) to produce C(k) and perform logistic chaotic mutation operation to C(k) to produce M(k)
- Step-5 Calculate the fitness value of M(k) and if fitness value is improving then the next population is P(k+1)=C(k) U M(k)
- Step-6 if the fitness value is reached the desired level or number of iterations the current population is returned as feature set otherwise increment k and proceed to Step-2.

The output of this algorithm is a set of k <13 most influencingfeatures that best describe the image.

### 1.1 Hash Code Generation

From the result of CGFSO algorithm the result of most useful K features are selected for each circular block of image and mean is calculated for each block and is represented as a row vector of size [1 X 64] and is stored in HF. Then the hash code is generated using the formulaH1= (HF + K1) mod 256 with a randomly generated key K1 containing values on range of 0-255

**Hash Verification Phase**

The hash code of trusted image H1 and the Hash code of received image H2 are compared to check for similarity using correlation coefficient measure. The image is authentic as far the content of the image is preserved.so pixel by pixel verification is not required. If correlation coefficient is greater than .95 it is authentic.

## 4 Experimental Set Up

Table 2: Experimental set up for CGFSO

| S.No | Parameter | Value |
|---|---|---|
| 1. | Population size | $2^{13}$-1 |
| 2. | Length of chromosome | 13 |
| 3. | Pc | 0.7 |

| | | |
|---|---|---|
| 4. | Pm | 0.2 |
| 5. | Subset Selection Method | Rank method |
| 6. | Number of subset selected in each iteration | 1/3rd of the population size |
| 7. | Encoding | Binary |
| 8. | Number of Iterations | 100 |
| 9. | Desired fitness value | 0.1 |
| 10. | Weighing factor | 0.3 |

The result is measured by precision, recall, accuracy, sensitivity, specificity, and F measure.

## 5 Results and Discussion

A data set of 2000 image is utilized in performance measure. These images are downloaded from the web and for 50 unique image content preserving transformation like scaling, turn, watermark inserting, contrast change, Gamma remedy and zero mean Gaussian function are applied as recorded in Table 3. Thus, for each image 40 variations of images arises. The images are assaulted utilizing adobe Photoshop and MATLAB. The performance of the system is analyzed based on the requirements of a good authentication system.

For experiments two different datasets are used. First set contains 2000 images with all Haralick features and the second dataset contains 2000 images with 4 most influencing Haralick features obtained as a result of optimization being used.The results of Accuracy, sensitivity, specificity and F measure is as shown in Table.4.

Table 4: Result Summary

| Criterion | Number of Features | |
|---|---|---|
| | All haralick Features | Optimized Haralick features |
| Classification accuracy | 0.9625 | 0.9600 |
| Sensitivity | 0.9629 | 0.9737 |
| Specificity | 0.9629 | 0.9737 |
| F Measure | 0.9578 | 0.9689 |

Table 3: List of Content Preserving Manipulations

| Content Preserving manipulation | Luminance | Geometric Distribution | | | Additive Noise | Watermarking |
|---|---|---|---|---|---|---|
| | Brightness and Contrast | Rotation | Scaling | Gamma Correction | Zero mean Gaussian noise | Text watermarking of length 10 |
| Measured in ranges | Scale [+10,-10,+20,-20] | Degree [1 to 300] | % [0.5 to 2.5] | % [0.75 to 1.25] | Variance [0.3 to 0.9] | Opacity [10 to 100] |
| Number of Images | 4 | 14 | 4 | 4 | 4 | 10 |

Figure 3 – 6 show the graphs for results shown in Table 4.After performing all the steps in CGFSO for all images, the most selected features are listed.The feature selection gives that energy homogeneity, correlation, contrast and entropy are most influencing features. It is observed that more than 96% of all the hash pairs have a correlation coefficient value of above .95. This result is similar to the results of using all features [1].

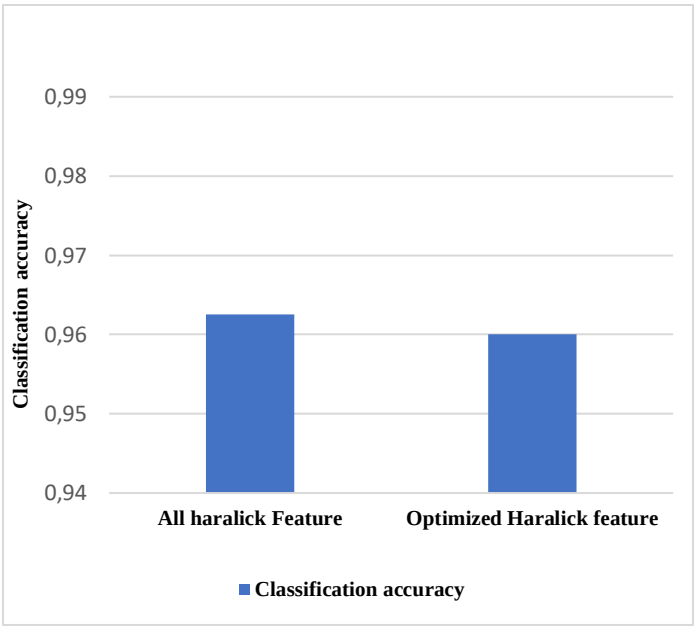



**Figure 3: Accuracy of the proposed System**

From Figure 3, it is clear that the proposed system using all Haralick features has higher classification accuracy by 0.25% compared to the system that uses optimized Haralick feature.

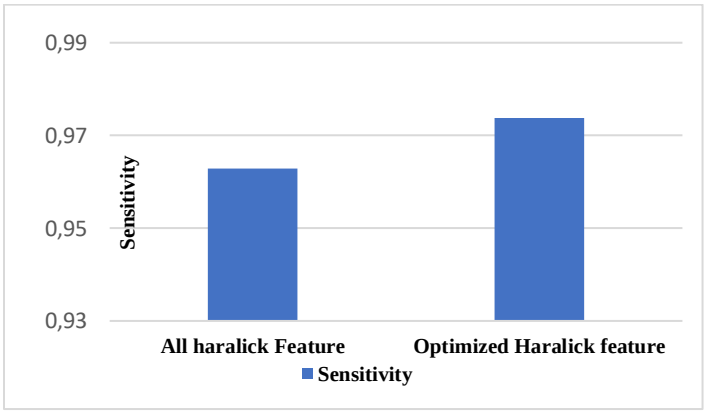



**Figure 4: Sensitivity of the proposed System**

From Figure 4, it is clear that the proposed system using optimized Haralick feature has higher sensitivity by 1.08 % compared to the system that uses all Haralickfeatures.

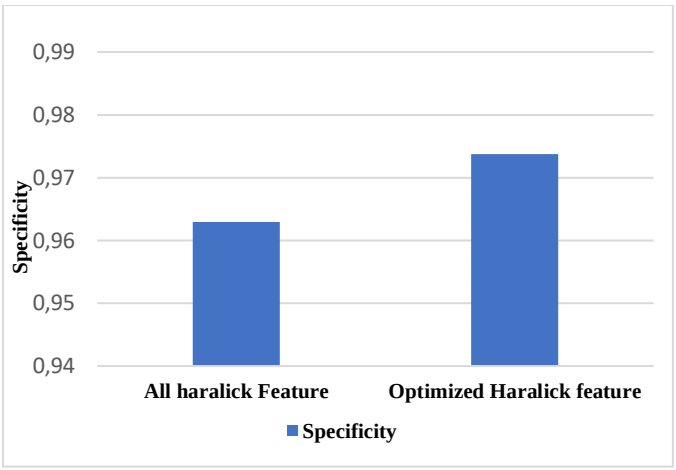



**Figure 5: Specificity of the proposed System**

From Figure 5, it is clear that the proposed system using optimized Haralick feature has higher specificity by 1.08 % compared to the system that uses all Haralick features.

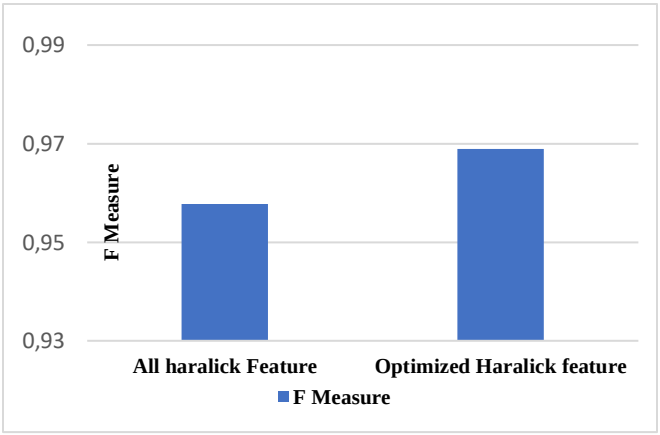



**Figure 6: F Measure of the proposed System**

From figure 6, it is clear that the proposed system using optimized Haralick feature has higher F measure by 1.11 % compared to the system that uses all Haralick features.

### 1.2 Robustness

Robustness is a measure of tolerance of the authentication system to content preserving manipulation. To measure the robustness of the proposed system a set of 5 standard images as shown in Figure 7 is taken.The result of Correlation Coefficient for various attacks for a set of 5 standard image processing images is graphically shown in Fig 8(a) -(f) and a comparison for the same with system using all Haralick features [1] is also shown. It is observed that the Correlation Coefficient S is above .95 for all types of attack listed in Table 2 except for rotation which is above .93.

### 1.3 Sensitivity

It refers to the ability of system to correctly specify forged image as forged. Our system correctly classifies images as authentic and forged. We observe that more than 96 % of all the hash pairs using reduced feature set have a correlation coefficient value of above 0.95.

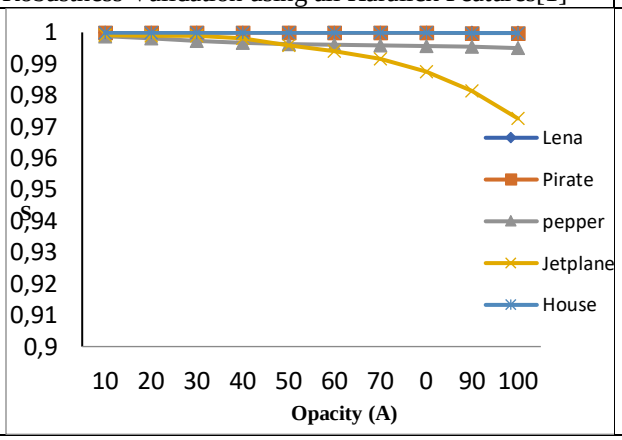
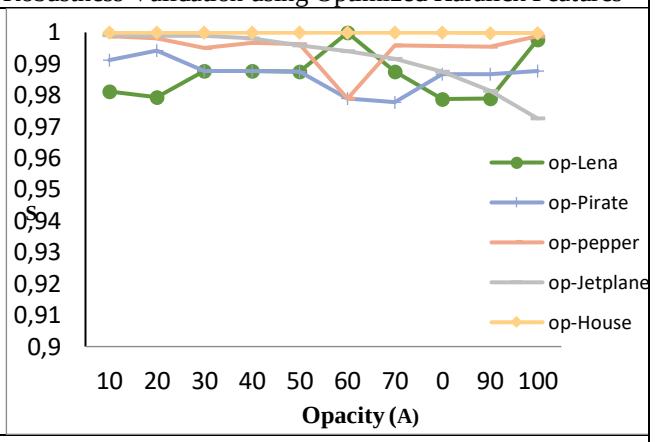
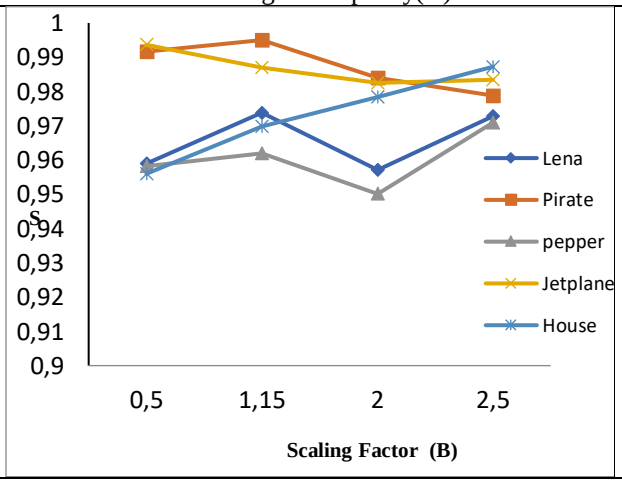
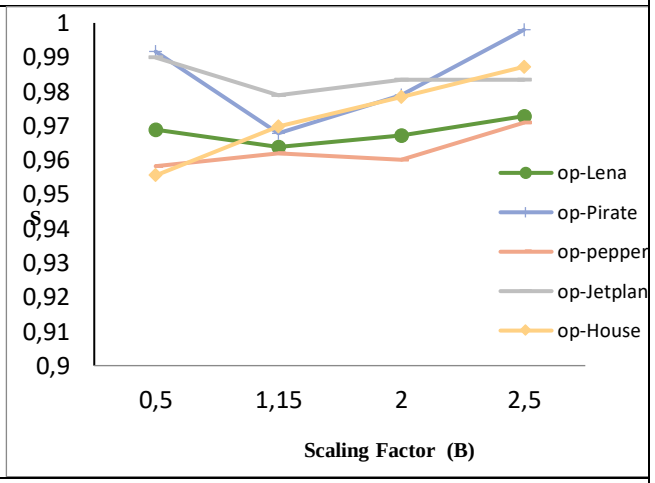
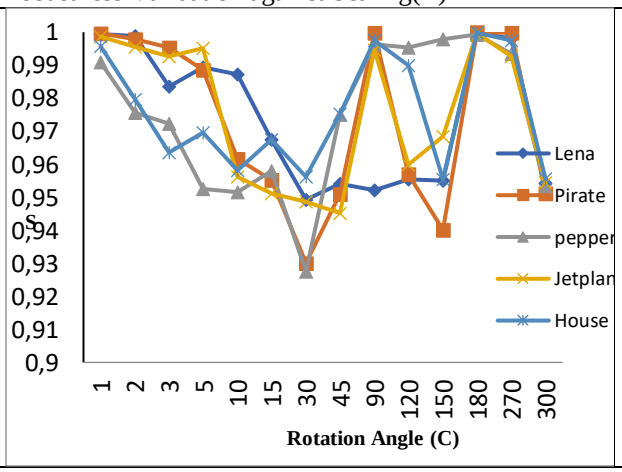
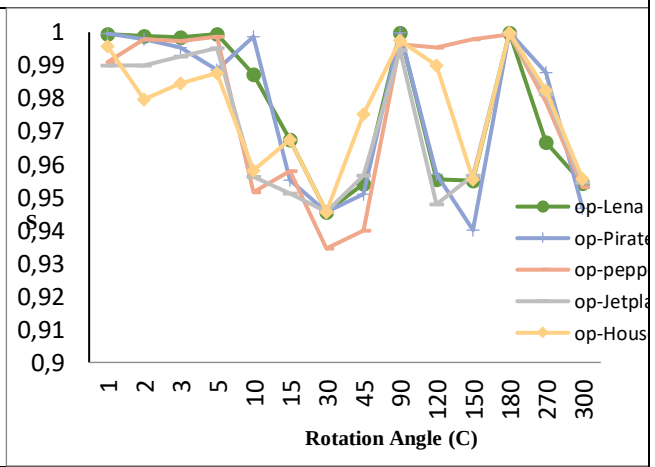
**Figure 7: Set of 5 Standard Images taken for Robustness validation (a) House (b) Lena (c) Pepper (d) Pirate (e) Plane**

Table 5: Comparison of Hash Performance

| | Features Used | Hash Length | Robustness validation against | | | | Ability to detect small area forgery | Ability to locate forged area |
|---|---|---|---|---|---|---|---|---|
| | | | additive Noise | slight cropping | small angle rotation | large angle rotation | | |
| VWD method of [4] | Local | 250 bits | Yes | Yes | Yes | No | No | No |
| NMF-NMF method of [22] | Local | 64 – floating point numbers | Yes | Yes | No | No | Yes | No |
| Wavelet based method of [5] | Local | 7168 bits | Yes | No | No | No | Yes | Yes |
| Proposed method | Local | 320 bits | Yes | Yes | Yes | Yes | Yes | Yes |

The purpose behind this lack is principally because of rotation, since it normally looks unusual when turned to bigger points. Since the rotated image has a critical extension and a few regions might be padded with dark or white pixels, so only the central part of the image of size 403 x 403 is considered for hash code.

The Classification performance is visualized using Receiver operating characteristic (ROC) curve where true positive rate and false positive rate are measure of robustness and sensitivity respectively. ROC curve is shown in Figure 9. Table.5 compares the proposed system with [4], [5], [22] all of these system uses local features for hash generation. This comparison reveals that our results outperforms in tolerating rotation to larger angles retaining tolerance to other content preserving transformation.

| Robustness Validation using all Haralick Features[1] | Robustness Validation using Optimized Haralick Features |
|---|---|
|  |  |
| Robustness Validation against Opacity(A) | |
|  |  |
| Robustness Validation against Scaling(B) | |
|  |  |
| Robustness Validation against Rotation(C) | |

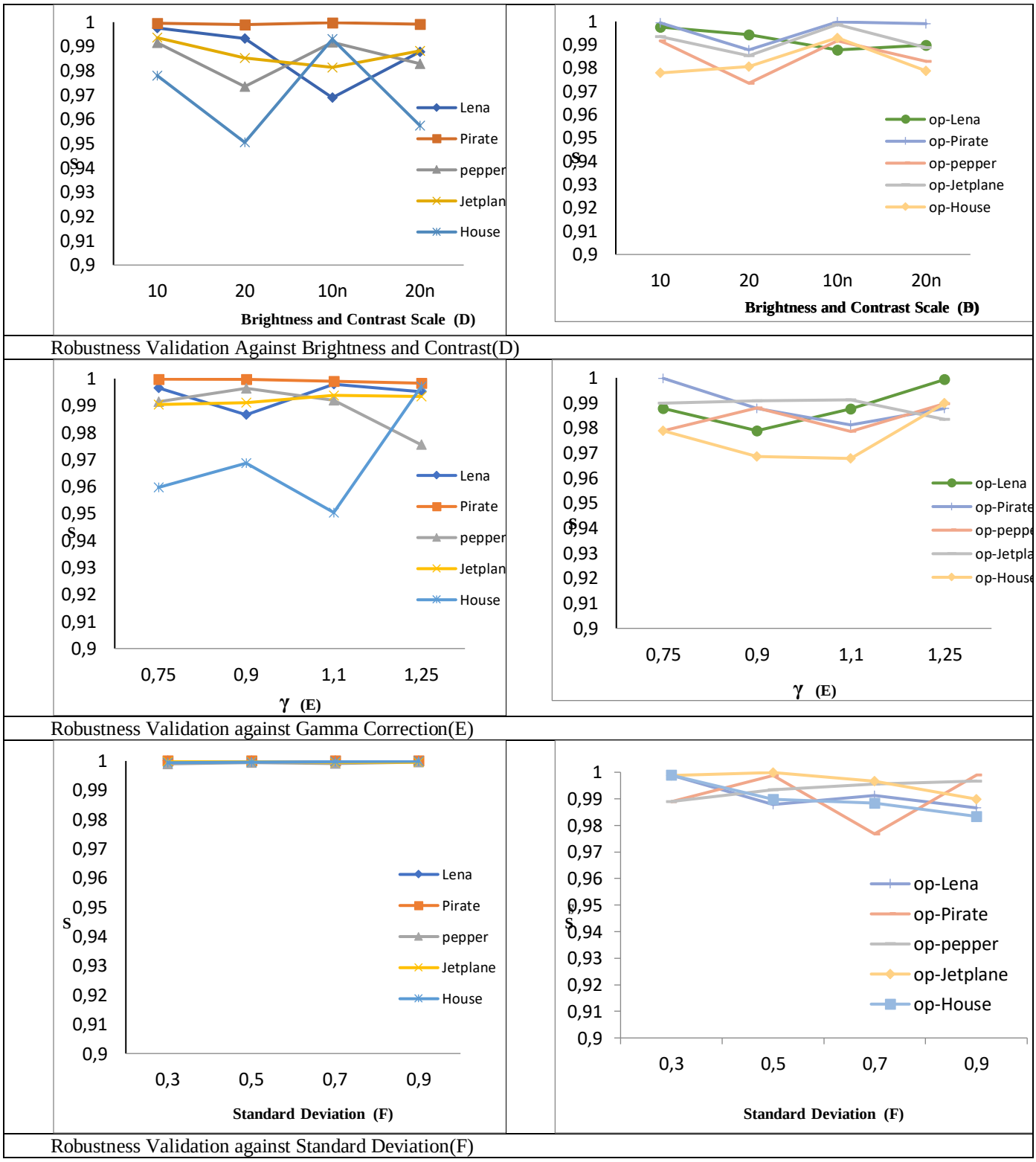



**Figure 8: Robustness Validations against (a). Opacity (b).Scaling (c).Rotation (d).Brightness and Contrast (e).Gamma Correction (f). Standard Deviation**

**Tamper detection and localization**

The proposed system has a 100 % achievement rate in localization and tamper detection. The threshold τ is taken as 0.95.The tampered circular block can be detected by from change in position of the hash code and by comparing the values of $R_k$ of circular block we can locate the change in pixel value and from its corresponding $d_{ij}$ we can locate the exact location of change in pixel value. From this we can locate the tampered regions successfully.

Table 6: Comparison of Average Time and Hash length

| Algorithm | Average time (s) | Hash Length |
|---|---|---|
| [22] | 1.153 | 64 decimal digits |
| [25] | *0.437* | 64 decimal digits |
| [26] | 1.429 | 42 decimal digits |
| [1] | 2.563 | *320 bits* |
| Proposed System | *0.739* | *320 bits* |

The average run time required to generate hash code for 200 different images is compared with [22], [25], [26] and is shown in Table 6. The bold text in Table 6 represents optimum results.The average run time of [25] is 0.437optimum as it uses only one low complexity entropy as feature for describing images and for ours it is 0.739.The average run time of optimized Haralick features isimproved over all Haralick features [1] because of feature selection. Considering the space complexity in terms of hash storage, the hash length proposed system is optimum with only 320 bit.

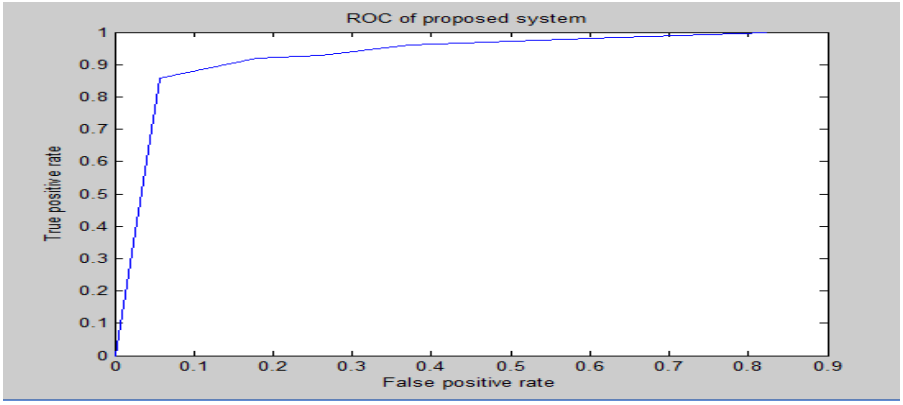



**Figure 9: ROC Curve**

## Conclusion

The main purpose of feature selection is to eliminate irrelevant and interrelated features without reducing the accuracy of the system under consideration. The removed features add no useful information but they actively hinder the authentication process.In the proposed work, Image authentication was done by using hash functions. The circular blocks were used for HF feature extraction and most influencing HF was selected by Chaos Genetic Feature selection Optimization. Then the results were compared with the hash functions by using all HF. The experimental outcomes have shown that,results obtained by selected 4 features such as energy homogeneity, correlation, contrast and entropy are similar to those of using all the features.

## References


[1] Alice, K, Ramaraj, N &Rajagopalan, SP 2020, "Rotation Invariant image authentication using haralick features" , *Multimedia tools and Applications,* Springer , Vol 79 no 1 pp 17211-17 225, Mar 2020

[2] A.Haouzia, R Noumeir, "Methods for image authentication A survey" ,*Multimedia tools and Applications,* Springer Vol 39no 1 pp1-46, 2008.

[3] Canny JF,"A computational approach to edge detection.",*IEEE Trans Pattern Anal Mach Intell*Vol 8 No6 pp 679–698,Dec 1986

[4] F.Khelifi and J.Jiang , " Preceptual image hashing based on virtual watermark detection,"*IEEE Transaction on Image Processing,* Vol 19, no 4, pp 981-994 Apr 2010.

[5] F.Ahmed, M.Y.Siyal, and V.U.Abbas, "A Secure and Robust hashing scheme for image authentication,"*Signal Processing,* vol.90 no.5 pp 1456-1470,2010.

[6] Gerhard Venter "Review of Optimization Techniques", *Encyclopedia of Aerospace Engineering in 2010 by John Wiley & Sons, Ltd.* Dec2010

[7] Hao Chen, Wen Jiang, Canbing Li, and Rui Li (2013),"A Heuristic Feature Selection Approach for Text Categorization by Using Chaos Optimization and Genetic Algorithm", *Hindawi Publishing Corporation Mathematical Problems in Engineering* Vol 2013, Article ID 524017, 6 pages ,2013

[8] Kailasanathan C, Safavi-Naini R, OgunbonaP ,"Image authentication surviving acceptable modifications". *IEEE-EURASIP, workshop on nonlinear signal and image processing*June 2001

[9] Lima Sebastian,AbrahamVarghese,Manesh.T ," Image Authentication by content preserving robust image hashing using local and global features",*Procedia Computer Science* Vol 46 pp 1554 – 1560 2015

[10] Lin CY, Chang SF,"A robust image authentication method distinguishing JPEG compression from malicious manipulation". IEEE Transactions On Circuits And Systems Of Video Technology, Vol. 11, No. 2, Feb 2001

[11] M.F.Hashmi,A.R.Hambarde,A.GKeskar, "Robust image authentication based on HMM and SVM Classifiers" , *Engineering letters* 22: 4 El-22-4-04-Nov 2014.

[12] Mohammad Javidi , RoghiyehHosseinpourfard, " Chaos Genetic Algorithm Instead Genetic Algorithm ", *The International Arab Journal of Information Technology,*, Vol. 12, No. 2, pp 163 - 168,Mar 2015.

[13] Nilesh,Dalton,Badal,Saroj,"Robust perceptual image hashing using fuzzy color histogram", *Multimedia Tool Applications,* Springer Vol. 77 No 23, p30815-30840 Dec 2018.

[14] Obaid Ur Rehman, S. Amir Hossein A.E. Tabatabaci, NatasaZivic,ChristophRuland, "Spatial and frequency domain complementary watermarks for image Authentication and Correction",*SCC 2015; 10th International ITG Conference on Systems, Communications and Coding,* Feb 2-5 2015

[15] Petra Snaselova ,Frantisek Zboril,(2015) " Genetic Algorithm using Theory of Chaos ",*ICCS 2015 International Conference On Computational Science , ProcediaComputerScience, Elsevier,*Vol51, pp 316–325,2015
[16] Robert M.Haralick, K.Shanmugam,Its'hakDinstein,"Textural features for image classification*",IEEE transaction on sytems , man and cybernetics*,vol 3. No 6. pp 610-621 Nov 1973.
**[17]** Schneider M, Chang S-F,"A robust content based digital signature for image authentication". *In: Proceedings of the IEEE international conference on image processing*, pp 227–230 1996
[18] Seyed Amir "Secure and robust two-phase image authentication", *IEEE transaction on multimedia*, Vol 17, No 7, ppno 945 -956 July 2015.
[19] Storck D,"A new approach to integrity of digital images". *In: Proceedings of the IFIP conference on mobile communication*, pp 309–316 1996.
[20] Sun Q, Chang SF,"Semi-fragile image authentication using generic wavelet domain features and ECC". *In: Proceedings of the ICIP*Vol 3 Sep 2002
[21] Tri.H.Nguyen,Duc.M.Duong,Duc.A.Doung,"Robust and High Capacity watermarking for image based on DWT-SVD", *IEEE RIVF, International conference on computing and communication Technologies Research Innovation and Vision for Future(RIVF)* 2015.
[22] V.Monga and M.K.Mihcak,"Robust and secure image hashing via non negative matrix factorizations",*IEEE Transaction on Information Forensics and Security*, vol 2, no 3 pp 376-390,Sep 2007.
[23] Wu CW,"On the design of content based multimedia authentication systems". *IEEE Transaction on Multimedia*Vol 4 No 3 pp 385–393, 2002
[24] Yan Zhao,ShuozhongWang,Xinpeng Zhang and Heng Yao "Robust Hashing for Image Authentication using Zernike Moments and Local features ",*IEEE Transactions on Information Forensics and Security*,Vol 8,No 1, pp 55-63, 2013
**[25]** ZhenjunTang,XianquanZhang,LiyanHuaug,Yumin Dai "Robust image hashing using ring based entropies", *Elsevier Signal processing*Vol 93 pp 2061-2069 ,2013.
**[26]** Z.Tang,Y.Dai,X.Zhang,"Perceptual hashing for color images using invariant moments", *Applied Mathematics and information sciences* Vol 6 pp 6435-6505,2012.

K.Alice received her PhD Degree in Information and Communication Engineering from Anna University,India in 2020, and the M.E Degree in Computer Science and Engineering from SathyabamaUniversity,India in 2005 and the B.E Degree in Computer Science and Engineering from MaduraiKamaraj University,India in 1999. She is currently working as an Associate Professor in Bharath institute of Higher Education and Research Chennai, India. Her research interests are in image processing, Deep learning and information Security