Forensics in Digital Images-an Approach to Contrast Enhancement

Nishat Fatema¹ M.S Chaudhari²

¹M.Tech. Student ²HOD

1,2Department of Computer Science & Engineering

Priyadarshini Bhagwati College of Engineering, Maharashtra, India

Abstract— Nowadays use of Contrast Enhancement in Digital Images is on the verge of rise and the issue of current research Many techniques under Image contrast enhancement have come into existence in previous years , but there is need of some techniques which must be very efficient and removes the drawbacks of previously used methods. As digital images or photos have been widely used as evidence in investigation field, medical, historical records, reports of journalist etc. Also with this the availability of most powerful tools which are capable of easy modification , manipulation , forgeries to image becoming quite easier .This paper is based on the study of different contrast enhancement techniques used in previous years and the methods they used. Also it explains the proposed methodology which uses nonlinear pixel mapping that introduce artifacts into an image histogram, and then detecting locally applied contrast enhancement in image , detecting histogram equalization in image and one image security algorithm is also used to add more security.

Key words: Contrast Enhancement, Histogram Equalization

I. INTRODUCTION

Image processing is a rapidly developing field based both on mathematics and computer science. It is naturally connected to and strongly influenced by image acquisition. Not only common customers but astronomers investigators journalist and also the people related to the field of medical science (MRI ,CT Scan etc) and many biologist are wide variety of users involved .Users demand regarding the image quality that means in terms of resolution and noise ratio is also growing rapidly. Enhancement may be the technique of improving the superiority of a electrically stored image. To produce a picture lighter or darker or to increase or decrease contrast. One can make an unauthorized copy of images and manipulate images such that that could lead to financial issue or even loss of human lives. Digital Image Forensics is a relatively new research field.

Various operations under image processing includes modification of the pixel values, but image content is unaltered. Other operations may also include quantization, compression, geometrical transformations like rotation, scaling etc. An effective and famous technique for image enhancement is histogram equalization. This technique works on remapping the gray levels of the image based on the probability distribution of the input gray levels. Also it expands the dynamic range of the image’s histogram and resulting in overall contrast enhancement. But this technique of Histogram Equalization suffers from many drawbacks..This technique is powerful enough in highlighting the borders and edges between different objects but it may reduce the local details within these objects, especially smooth and small ones.

Some other techniques under Histogram equalization are Mean Brightness Preserving Equalization Histogram (MBPHE),multilevel component based histogram equalization (MCBHE), Brightness preserving dynamic histogram equalization (BDPHE) Weighting mean separated sub histogram equalization (WMSE). The field of image restoration (sometimes referred to as image desharpnessing or image deconvolution) is concerned with the reconstruction or estimation of the uncorrupted image from a sharpened and noisy one. Though considerable research is done in such areas, as contrast enhancement is subjective in nature and is dependent on the nature of the original images, generalised contrast enhancement technique is not yet developed.

II. PROPOSED WORK

A. Detecting Globally Applied Contrast Enhancement in Image

Contrast enhancement operations are viewed as non linear pixel mapping which introduce artifacts into an image histogram. Non linear mappings are separated into regions where the mapping is locally contractive. The contract mapping maps multiple unique input pixel values to the same output pixel value. Result in the addition of sudden peak to an image histogram.

B. Detecting Locally Applied Contrast Enhancement in Image

Contrast enhancement operation may be locally applied to disguise visual clues of image tampering. Localized detection of these operations can be used as evidence of cut and paste type forgery. The forensic technique is extended into a method to detect such type of cut and paste forgery.

C. Detecting Histogram Equalization in Image

Just like any other contrast enhancement operation, histogram equalization operation introduces sudden peaks and gaps into an image histogram. The techniques are extended into method for detecting histogram equalization in image.

D. Image Security algorithm

- Input data of the cipher are pixel matrices, i.e. three matrices of color components in RGB coding, where each element of the matrix takes a value from 0 to 255. If the image is monochromatic, there is obviously one matrix of numbers (grayscale values).
- The value of each color component of the pixel is used as initial value for the logistic equation. Conversion to floating-point numbers and back to colors are realized by formulas
- Encryption procedure
- Let the plain image contain N £M = m pixels, and let i = 1; 2; : : : ; m be a pixel index. To make the description simpler, let us assume that the i*image is black and white, represented by one matrix of numbers.
- Decryption procedure
- Again, let us assume for simplicity, that the encrypted image is black and white.
Firstly, to recover the original image, pixels of ciphertext should be converted to a matrix of floating-point numbers.

Then, from the value of m-th pixel we subtract the value of the previous pixel, which was earlier iterated n times on the chaotic map. If the result is less than 0, it should be normalized by adding ±x.

These operations are repeated for all pixels of the image, remembering about the assumed condition for the last pixel. The whole image is processed j times.

If we have a color image, we expand the algorithm in a way analogous to the encryption procedure.

III. METHODOLOGY

A. Advanced Forge Algorithm

Here the raw image is taken as input. And after taking that image, Advanced forge algorithm is applied over that image in order to highlight the artifacts.

The flow of algorithm is as follows:

- **Input image**
- **Step 1:** Coarse light background elimination
  - 1. FFT
  - 2. Subtracting
- **Step 2:** Image balancing
  - 1. Choosing a reference block
  - 2. Adaptive linear transformation
- **Step 3:** Max-mean-min radiation correction
  - 1. Choosing max and min gray values
  - 2. Correction using color preserving factor
- **Output image**

Fig. 1: Flow of Algorithm

After applying the Advanced forged algorithm the next part is to make our image secure. For security purpose here we are using two algorithms i.e. hybrid 3DES and MD5.

The goal of Information security is to achieve confidentiality by cryptography, integrity by hashing, and availability by access control. Information security use cryptography when transferring information such that information is unable to unauthorized parties. There are two cryptographic techniques are Symmetric and Asymmetric techniques.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryption, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually.

B. Result

Fig. 2: Raw Image

Fig. 3: Applying the Advance Filter

After applying the advanced forged algorithm the Contrast enhancement is enforced in the other region to simulate the both-source enhanced composition. To measure the accuracy for locating tampered regions, the proportion of blocks classified correctly in the selected rectangular region is defined as $P_A$, while the proportion of blocks classified incorrectly in the other region is measured as $P_B$. As shown in Fig. 3 indicates, the mean of $P_d$.

IV. CONCLUSIONS

Advanced forged algorithm the next part is to make our image secure Local Contrast Enhancement etection, Dualistic Sub-Image Histogram equalization Automatic-Mean Weighting Mean Separated Histogram, Contextual and variational
contrast Enhancement, Minimum Mean Brightness Error Bi-Histogram Equalization by Advanced forge algorithm. Methodology which uses non linear pixel mapping that introduce artifacts into an image histogram, and then detecting locally applied contrast enhancement in image, detecting histogram equalization in image and one image. As far as the security is concerned the previous works does not deal with the anti-forensic activities security related to it. But in this paper along with different techniques of contrast enhancement a security algorithm multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryption, you simply type in the entire 192-bit.

ACKNOWLEDGEMENT
We are thankful to all the researchers who helped us throughout this research. We would like to express our special thanks to our professors for giving us constant motivation and encouragement.

REFERENCES