iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5446

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Smart Pix

Anishma. T. S
KMP college of engineering

Abstract: SMART PIX is a photographic site through which professional photographers can upload their photo With Security And normal users can view and download photographs with the permission of the photographer. In Smart pix Identification of duplicate Image is done trough the Technique Robust Image Hashing with Ring Partition and Invariant Vector Distance". Histogram generation is done through Multichannel Decoded Local Binary Patterns for Content Based Image Retrieval Encryption of the Original Image is done through Blowfish Encryption along with chaos mapping encryption. Before storing the image, the original image is Encrypted and Watermarked. Here I use the technique of "Improved-AMBTC Algorithm with edge detection" for hiding the authentication Data in the Image

I. INTRODUCTION

Hashing refers to the use of hash functions to verify that an image is identical to the source media. Hashing is like a digital fingerprint for a file. It is mathematically derived from the contents of the item being hashed, and is displayed in a set of numbers and letters. The length of the hash depends on the type of hash used. It is incredibly unlikely that two image files with different contents would ever generate the same hash. There are several hashing algorithms that are commonly used, such as MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm), SHA256, and others. MD5 is a 128 bit 32 character algorithm and is the most commonly used hashing algorithm. There are other hashing algorithms available for encryption; however forensics primarily focuses on MD5, SHA1, and SHA256. Hashing is used in many other areas of digital study such as Download confirmation and encryption.

While altering anything within the contents of the disk image will alter the hash value (like adding or removing a single character in a document or changing one pixel in an image), changing the name or extension of the image will not alter the hash value.

Hashing is pivotal in the scope of forensics investigations, as the hash verifies the integrity of the disk image. Anyone at any time during or after the investigation should be able to rehash the disk image and replicate the exact same hash value that was given the first time the disk image was ever hashed. ash function is a method for generating fixed length output from input data, aimed at improving the efficiency of data processing. It has been widely used in processing variable-length data in real applications, such as image processing, information retrieval and cryptography. Image hashing is a technique for deriving a content-based compact representation from input image, called image hash

It is pretty practical to generate image hashing at a good level of both rotation robustness and discrimination. Accordingly, Designed an image hashing based on ring partition and invariant vector distance, which is with good rotation robustness and desirable discriminative capability. The main contributions are as follows.Perceptual statistical features are extracted from image rings in CIE L*a*b* color space. Since image pixels of each ring are almost the same after rotation, ring-based statistical features are invariant to image rotation with arbitrary angle. The CIE L*a*b* color space is selected for feature extraction because it is perceptually uniform and image features extracted from this uniform space are more stable than those from other color spaces.

Feature vectors are taken as points in a high dimensional space, and the Euclidean distance between feature vectors is exploited to represent the original features. This strategy is based on the observation that vector distance is invariant to commonly-used digital operations to images (e.g., JPEG compression, gamma correction, and brightness/contrast adjustment).

An ige histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance.

mage histograms are present on many modern digital cameras. Photographers can use them as an aid to show the distribution of tones captured, and whether image detail has been lost to blown-out highlights or blacked-out shadows. This is less useful when using a raw image format, as the dynamic range of the displayed image may only be an approximation to that in the raw file.

The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. The left side of the horizontal axis represents the black and dark areas, the middle represents medium grey and the right hand side represents light and pure white areas. The vertical axis represents the size of the area that is captured in each one of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and center of the

©IJRASET: All Rights are Reserved

graph. Conversely, the histogram for a very bright image with few dark areas and/or shadows will have most of its data points on the right side and center of the graph. IMAGE indexing and retrieval is demanding more and more attention due to its rapid growth in many places. The aim of Content Based Image Retrieval (CBIR) is to extract the similar images of a given image from huge databases by matching a given query image with the images of the database. Matching of two images is facilitated by the matching of actually its feature descriptors (i.e. image signatures). It means the performance of any image retrieval system heavily depends upon the image feature descriptors being matched.

Texture based image feature description is very common in the research community. Recently, local pattern based descriptors have been used for the purpose of image feature description. Local binary pattern (LBP) has extensively gained the popularity due to its simplicity and effectiveness. Here proposed two multichannel decoded local binary pattern approaches namely multichannel adder based local binary pattern ( ) and multichannel decoder based local binary pattern ( ) to utilize the local binary pattern information of multiple channels in efficient manners. Total + 1 and 2 number of output channels are generated by using multichannel adder and decoder respectively from number of input channels for ≥ 2.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected," and graphein meaning "writing".

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be

in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's principle.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

The term steganography was used to conceal the secret message into other media file. In this paper, a novel image steganography is proposed, based on adaptive neural networks with recycling the Improved Absolute Moment Block Truncation Coding algorithm, and by employing the enhanced five edge detection operators with an optimal target of the ANNS. Here propose a new scheme of an image concealing using hybrid adaptive neural networks based on I-AMBTC method by the help of two approaches; the relevant edge detection operators and image compression methods. Despite that, many processes in our scheme are used, but still the quality of concealed image looking good according to the HVS and PVD systems.

Here present a novel scheme for image steganography which is based on a high compress method for color images and another high payload steganography mechanism using a hybrid edge detector. The current Technique proposes a new scheme of compression image concealing based on the hybrid adaptive neural networks with the enhanced of AMBTC algorithm based on one of the most popular edge detection operators and adaptive neural networks. With this scheme, a large amount of compressed bits can be concealed into the color image with five layers of security.

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

©IJRASET: All Rights are Reserved

One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the ciphertext. Normally, there is an expansion of space requirement in visual cryptography. But if one of the two shares is structured recursively, the efficiency of visual cryptography can be increased to 100%.

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention, and Schneier recommends Blow fish for modern applications.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is
unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone.

Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

Data security requirement increased due to transmission of huge data over the communication channel. For this, we have proposed a double encryption technique using Blowfish algorithm and Cross chaos map. These techniques have been chosen due to their resistance over the cryptanalysis attacks.

II. PROPOSED SYSTEM

This project aims at developing a photography site In which Professional photographers can post Their photos. When a photographer upload his photo the image is compared with all other images in the system to Identify whether that image already existing, If it is already existing he cannot post that image.

To Identify Whether it is a duplicate Image two techniques are used for image comparison one is by using Image hashing technique and other one is using Multichannel Decoded Local Binary Patterns.

does not already exist the secret information which is identification of the photographer is concealed in the original image for authentication. The data hiding is done trough a steganography technique using an Improved-AMBTC Algorithm.

Before Storing the Image, image is encrypted using blowfish encryption technique to ensure secure storing of image

A. Phase 1

Phase one of the paper is completed in 3 levels. In level 1 Completed1 technique for image comparison which is “Robust Image Hashing with Ring Partition and Invariant Vector Distance”. —Robustness and discrimination are two of most important objectives in image hashing. Here incorporate ring partition and invariant vector distance to image hashing algorithm for enhancing rotation robustness and discriminative capability.

As ring partition is unrelated to image rotation, the statistical features that are extracted from image rings in perceptually uniform color space, i.e., CIE L*a*b* color space, are rotation-invariant and stable. In particular, the Euclidean distance between vectors of these perceptual features is invariant to commonly-used digital operations to images (e.g., JPEG compression, gamma correction, and brightness/contrast adjustment), which helps in making image hash compact and discriminative.

In level 2 Completed Data hiding using the technique “Steganography Scheme to Conceal a Large Amount of Secret Messages Using an Improved-AMBTC Algorithm”, In which novel image steganography is proposed, based on adaptive neural networks with recycling the Improved Absolute Moment Block Truncation Coding algorithm, and by employing the enhanced five edge detection operators with an optimal target of the ANNS.

Here propose a new scheme of an image concealing using hybrid adaptive neural networks based on I-AMBTC method by the help of two approaches; the relevant edge detection operators and image compression methods.

In level 3 of the project web designing and encryption of the image is done. The Encryption technique used in my project is blowfish along with chaos mapping.

©IJRASET: All Rights are Reserved

In encryption, propose an algorithm for dual encryption. It uses blowfish and Cross chaos map techniques. We have divided the entire operation in three sections:

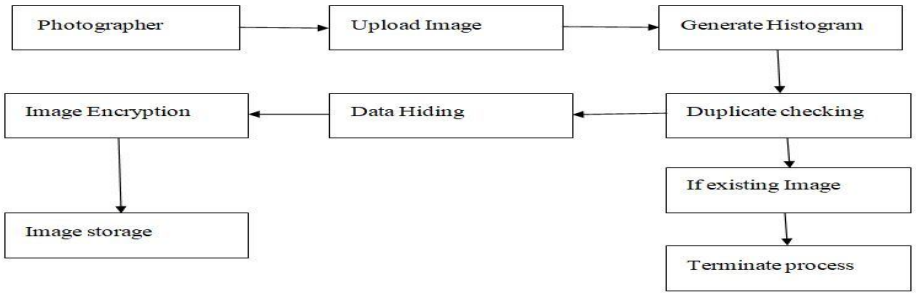
B. Phase 2

Duplicate Image Retrieval using Local Binary Patterns.This Technique proposes a novel method for image description with multichannel decoded local binary patterns. Local binary pattern (LBP) is widely adopted for efficient image feature description and simplicity. To describe the color images, it is required to combine the LBPs from each channel of the image. The traditional way of binary combination is to simply concatenate

the LBPs from each channel, but it increases the dimensionality of the pattern. In order to cope with this problem, here proposes a novel method for image description with multichannel decoded local binary patterns. I introduce adder and decoder based two schemas for the combination of the LBPs from more than one channel. Image retrieval experiments are performed to observe the effectiveness of the proposed approaches and compared with the existing ways of multichannel techniques. Here introduce adder and decoder based two schemas for the combination of the LBPs from more than one channel.

C. Advantages Of Proposed System

1) Image hashing used in my project is much better than existing popular hashing algorithms at robustness and discrimination.
2) Proposed hashing can resist commonly-used digital operations to images, including rotation with any angle, reach desirable discriminative capability and be sensitive to visual content changes.
3) It is observed that the introduced multichannel adder and decoder based local binary patterns significantly improves the retrieval performance over each database and outperforms the other multichannel based approaches in terms of the average retrieval precision and average retrieval rate.
4) proposed steganography scheme makes the fact that the pixel visual differencing (PVD) and human visual (HVS) are less sensitive to change in high contrast areas of the image and therefore, attempts to conceal the secret image bits into edge pixels of the cover image file.
5) Blowfish Encryption techniques have been chosen due to their resistance over the cryptanalysis attacks.



Block Diagram of the system

III. IMPLEMENTATION

Implementation is the realization of an application, or execution of a plan, idea, model, design, specification, standard, algorithm, or policy.

A. Modules

1) Image Comparison Using Hash Generation
2) Histogram generation Using LBP
3) Data Hiding
4) Encryption and decryption
5) Web design

B. Modules Description

1) *Image Comparison Using Hash generation:* This is the module that Compare an image with existing images By generating Hash of the Image through Ring Partition and invariant vector Distance . Designed an image hashing based on ring partition

©IJRASET: All Rights are Reserved

and invariant vector distance, which is with good rotation robustness and desirable discriminative capability. The main contributions are as follows. (1) Perceptual statistical features are extracted from image rings in CIE L*a*b* color space. Since image pixels of each ring are almost the same after rotation, ring-based statistical features are invariant to image rotation with arbitrary angle. The CIE L*a*b* color space is selected for feature extraction because it is perceptually uniform and image features extracted from this uniform space are more stable than those from other color spaces. Feature vectors are taken as points in a high dimensional space, and the Euclidean distance between feature vectors is exploited to represent the original features. This strategy is based on the observation that vector distance is invariant to commonly-used digital operations to images

2) *Histogram generation using LBP:* This module Generate histogram of the image using local binary patter. In this algorithm, proposed two multichannel decoded local binary pattern approaches namely multichannel adder based local binary pattern ( ) and multichannel decoder based local binary pattern ( ) to utilize the local binary pattern information of multiple channels in efficient manners. Total + 1 and 2 number of output channels are generated by using multichannel adder and decoder respectively from number of input channels for ≥ 2.

3) *Data Hiding:* In this module posted image is authenticated using the technique of stegnog raphy .Here we use Sobel edge Detection algorithm to find the edges of the image. The stego-file is produced by using the proposed algorithm to achieve a high level of robustness and visual quality with acceptable embedding rate of up to 50% (iv) Encryption and DecryptionData security requirement increased due to transmission of huge data over the communication channel. For this, Here proposed a double encryption technique using Blowfish algorithm and Cross chaos map. These techniques have been chosen due to their resistance over the cryptanalysis attacks. Parameters such as NPCR (Number of Pixels Changing Rate), UACI (Unified Average Changing Intensity) and CC (Correlation Co- efficient) are used for the effectiveness of our proposed technique. The result provides a high level of security

4) *Web Design:* Here in our system There are two users one is photographer and other one is normal user . This project aims at developing a photography site In which Professional photographers can post Their photos. When a photographer upload his photo the image is compared with all other images in the system to Identify whether that image already existing, If it is already existing he cannot post that image. To Identify Whether it is a duplicate Image two techniques are used for image comparison one is by using Image hashing technique and other one is using Multichannel Decoded Local Binary Patterns. If Image does not already exist the secret information which is identification of the photographer is concealed in the original image for authentication. The data hiding is done trough a steganography technique using an Improved-AMBTC Algorithm. Before Storing the Image, image is encrypted using blowfish encryption technique to ensure secure storing of image. The photographer can see his posted photos in the album section. In photographer home page there is an Inbox section through which he can view and accept the download requests from the user. In the user page, user can search photographers and follow favuorite photographers, followed photographers photographs are updated in the user's home page. the user can send download request for the photo. If the photographer accepts the request, the user can download image by providing the key which is send by the photographer, actually the key is to decrypt the Image. The user can also view the data hidden in the image ,but he cannot extract the information

IV. CONCLUSIONS

The system has been developed for the given conditions and is found working effectively under all circumstances that may arise in real environment. The proposed system, which has been implemented using provides many advantages. The system was tested for a wide range of input and found to be error free in all test cases. The entire system has been tested with a sample data. The system is highly user friendly and is well efficient to make easy interactions with the users of the system. The system is developed, tested and implemented with high degree of accuracy. The system is done with an insight into the necessary modifications that may be required in the future. Hence the system can be maintained successful without much work .In this project image comparison is done incorporating ring partition and invariant vector distance to image hashing algorithm for enhancing rotation robustness and discriminative capability. In my project Data hiding is done through A novel image stenography scheme with high payload method, to conceal a large amount of secret data. Symbol edge detection algorithm is used for edge detection and data is embedded in edges
Data security requirement increased due to transmission of huge data over the communication channel. For this, we have proposed a double encryption technique using Blowfish algorithm and Cross chaos map. These techniques have been chosen due to their resistance over the cryptanalysis attacks. Two multichannel decoded local binary patterns are introduced namely multichannel adder local binary pattern (maLBP) and multichannel decoder local binary pattern (mdLBP). Basically both maLBP and mdLBP have

©IJRASET: All Rights are Reserved

utilized the local information of multiple channels on the basis of the adder and decoder concepts. The maLBP descriptor is not showing the best performance in most of the cases while mdLBP descriptor outperforms the existing state-of-the-art multichannel based descriptors. It is also deduced that Chisquare distance measure is better suited with the proposed image descriptors. The performance of the proposed descriptors is much improved for three input channels and also in the RGB color space. The performance of mdLBP is also superior to non-LBP descriptors. It is also pointed out that mdLBP outperforms the state-of-the-art descriptors over large databases. Experiments also suggested that the introduced approach is generalized and can be applied over any LBP based descriptor. The increased dimension of the decoder based descriptor slows down the retrieval time which is the future direction of this research.

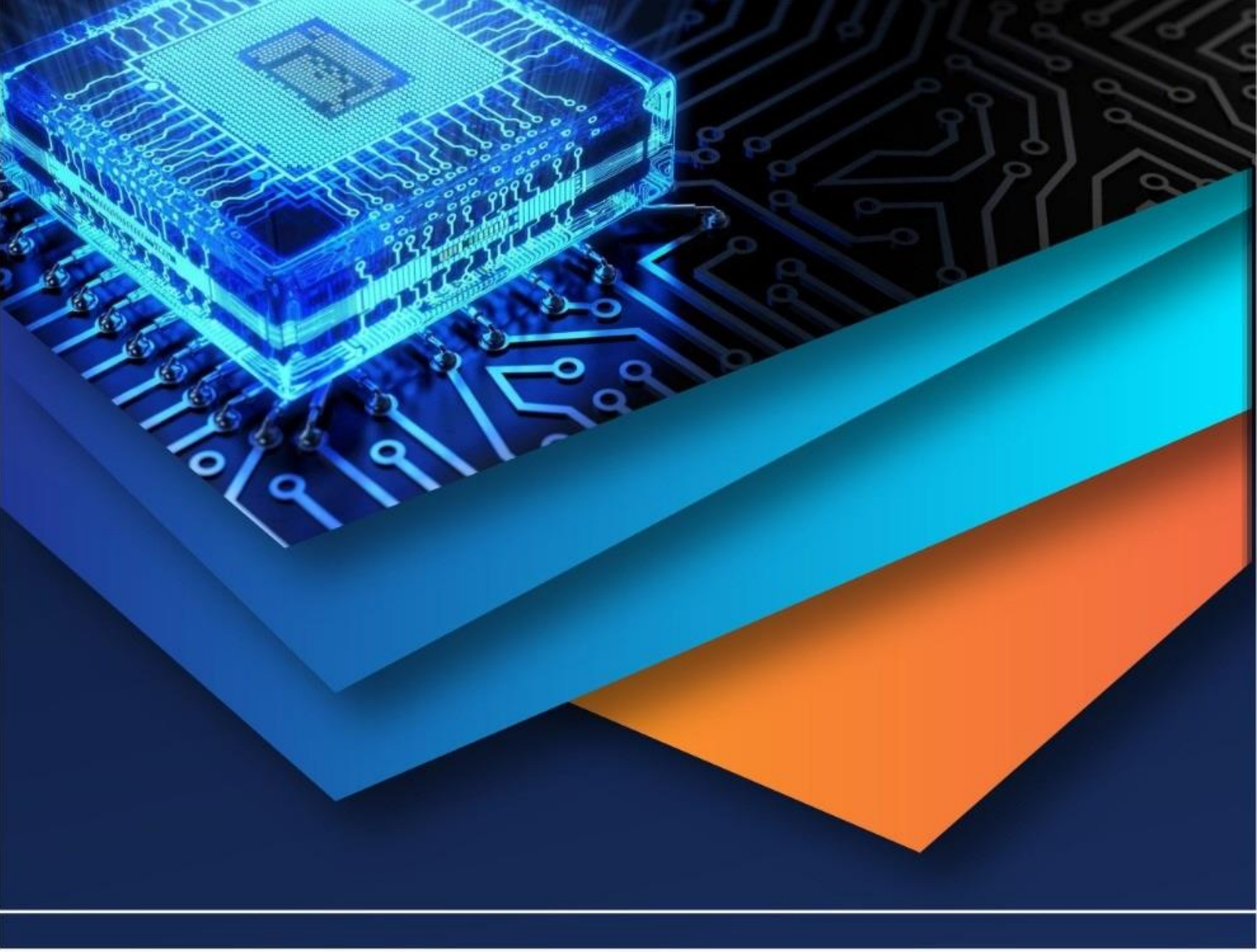
V. FUTURE WORKS

My project can be extended to add live photographs and quality of the image can be anaylsed through histogram. Depending on the type of image, the histogram can give you a general idea about the contrast of an image (whether it's too bright or too dark). Histograms are sometimes used in photography to adjust exposure One future aspect of this project is to make the descriptors used in LBP generation noise robust which can be achieved by using the noise robust binary patterns over each channel as the input to the adder/decoder. In the image hashing area further work include the capability of tamper localization and content recovery, new techniques of dimensionality reduction for image hashing, and efficient hashing algorithms for reduced-reference image quality assessment

REFERENCES

[1] R. Venkatesan, S.-M. Koon, M. H. Jakubowski and P. Moulin(2000). Robust image hashing. Proc. of IEEE International Conference on Image Processing, pp. 664–666, 2000.
[2] Z. Tang, X. Zhang and S. Zhang(2005). Robust perceptual image hashing based on ring partition and NMF. IEEE Transactions on Knowledge and Data
[3] Z. Tang, S. Wang, X. Zhang, W. Wei and S. Su(2008). Robust image hashing for tamper detection using non-negative matrix factorization. Journal of Ubiquitous Convergence and Technology, Vol. 2, No. 1, pp. 18–26, 2008.
[4] Z. Fouroozesh and J. Al ja'am(2014), Image stenography based on lsbmr using sobel edge detection, in e-Technologies and Networks for Development (ICeND), 2014 Third International Conference on. IEEE, 2014, pp. 141–145.
[5] A. Ioannidou, S. T. Halkidis, and G. Stephanides(2012), A novel technique for image steganography based on a high payload method and edge detection, Expert systems with applications, vol. 39, no. 14, pp. 11517– 11524, 2012.
[6] J.-G. Yu, E.-J. Yoon, S.-H. Shin, and K.-Y. Yoo(2008), A new image steganography based on 2k correction and edge-detection, in Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on. IEEE, 2008, pp. 563–568.
[7] C.-C. Chang, Y.-H. Yu, and Y.-C. Hu, (2008)Hiding secret data into an ambtc-compressed image using genetic algorithm, in Future Generation Communication and Networking Symposia, 2008. FGCNS'08. Second International Conference on, vol. 3. IEEE, 2008, pp. 154–157.
[8] X.-Y. Luo, D.-S. Wang, P. Wang, and F.-L. Liu(2008), A review on blind detection for image steganography, Signal Processing, vol. 88, no. 9, pp. 2138–2157, 2008
[9] N. Sethi, D. Shanna(2012),A Novel Method of Image Encryption using Logistic Mapping", International Journal of Computer Science Engineering, Vol. I, No. 2, 2012, pp. 115-119.
[10] M. Heikkilä, M. Pietikäinen and C. Schmid(2009), "Description of interest regions with local binary patterns," Pattern Recognition, vol. 42, no. 3, pp. 425-436, 2009.
[11] S. Liao, M.W.K. Law, and A.C.S. Chung(2009), Dominant local binary patterns for texture classification, IEEE Transactions on Image Processing, vol. 18, n8659+o. 5, pp. 1107-1118, 2009.
[12] Z. Guo, L. Zhang and D. Zhang(2010), Rotation invariant texture classification using LBP variance (LBPV) with global matching, Pattern recognition, vol. 43, no. 3, pp. 706-719, 2010.
[13] Z. Guo, and D. Zhang(2010), A completed modeling of local binary pattern operator for texture classification," IEEE Transactions on Image Processing, vol. 19, no. 6, pp. 1657-1663, 2010.
[14] X. Tan and B. Triggs(2010), Enhanced local texture feature sets for face recognition under difficult lighting conditions, IEEE Transactions on Image Processing, vol. 19, no. 6, pp. 1635-1650, 2010.
[15] B. Zhang, Y. Gao, S. Zhao and J. Liu(2010), Local derivative pattern versus local binary pattern: face recognition with high-order local pattern descriptor,IEEE Transactions on Image Processing, vol. 19, no. 2, pp. 533-544, 2010
[16] S.R. Dubey, S.K. Singh and R.K. Singh(2015), Local Neighborhood Based RobusColour Occurrence Descriptor for Colour Image Retrieval," IET Image Processing, vol. 9, no. 7, pp. 578-586, 2015
[17] W.T. Chu, C.H. Chen and H.N. Hsu(2014), Color CENTRIST: Embedding color information in scene categorization, Journal of Visual Communication and Image Representation, vol. 25, no. 5, pp. 840-854, 2014
[18] C.K. Heng, S. Yokomitsu, Y. Matsumoto and H. Tamura(2012), Shrink boost for selecting multi-lbp histogram features in object detection, In IEEE International Conference on Computer Vision and Pattern Recognition, pp. 3250-3257, 2012. 21

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)