International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 11 125- 129

Content Authentication and Forge Detection using Perceptual Hash for Image Database

Ms. Gauri Barse
Department of Computer Engineering
Jayawantrao Sawant College of Engineering,
Pune-411028

Prof.S.D.Satav
Department of Information Technology
Jayawantrao Sawant College of Engineering,
Pune-411028

Abstract :- Popularity of digital technology is very high. Number of digital images are being created and stored every day. This introduces a problem for managing image databases and security of images. One cannot determine if an image already exists in a database without exhaustively searching through all the entries. Further complication arises from the fact that two images appearing identical to the human eye may have distinct digital representations, making it difficult to compare a pair of images. Also the security of database server is questionable. The proposed framework provides the content authentication and forges detection of image. This can be done by generating perceptual image hash using SIFT algorithm, Perceptual image hash also known as perceptual image signature. It has been proposed as a primitive method to solve problems of image content authentication. The perceptual image hash is generated by using the perceptual features that are in accordance with human's visual characteristics. It allows tampering of images to permissible extent e.g. improving slight brightness or contrast in image. A perceptual image hash is expected to be able to survive unintentional distortion and reject malicious tampering within an acceptable extend .Therefore it provides a more efficient approach to analyzing changes of image perceptual content and make sure database server is authenticated or not.

Keywords-*Perceptual image hash, content authentication, tampering detection, tampering localization, SIFT algorithm*

*****

I. INTRODUCTION

Currently there is tremendous amount of image data being generated over internet, this data is very vulnerable to tampering, also it resulted in an explosive growth of image illegal use, e.g. image phony and unapproved usage and hence it is necessary to provide an authentication process for image dataset as images are many times used as proofs.Perceptual image hash, also known as perceptual image signature, has been proposed as a primitive method to solve problems of image content authentication. A perceptual image hash is a short summary of an image's perceptual content. It has many important applications, for example, image content authentication, tampering detection.

Utilizing this hash, an image altering identification and altering restriction strategy is produced. Also, it accomplishes an exchange off between strength to endure geometric twisting and altering restriction. Contrasted and cutting edge conspires, the proposed plan yields better execution .The proposed strategy can be utilized for image verification and for image recovery and coordinating in extensive scale image databases .The proposed framework can be utilized as a part of numerous zones, for example, in police systems for scientific exploration, in business organizations for keeping up security or for workers' pictures for cards and so on.

Perceptual image hash, otherwise called perceptual image signature, has been proposed as a primitive strategy to take care of issues of image substance validation. A perceptual image hash is a short outline of a image's perceptual substance. It has numerous vital applications, for instance, image content validation, altering recognition, image recovery and image registration.A perceptual image hash is expected to be able to survive unintentional distortion and reject malicious tampering within an acceptable extend. Currently there is gigantic measure of image information being created over web, this information is extremely powerless against altering, henceforth it is important to give a confirmation procedure to image dataset as images are ordinarily utilized as evidences as a result of that we persuaded to do this task.

II. PROBLEM DEFINITION

To develop a new and more secured way so that we can save and authenticate the user's image data on the basis of perceptual hash. We are proposing this client based application which can be installed on the system and performs operations like Uploading Image to Server, Generating perceptual hash. The application will generate advance perceptual hash and save them at local storage for every image uploaded and Authenticate content and detect forgery Where The application will on downloading images back will perform content authentication on every images using locally stored hash

information. So that we provide the way to keep image data safe as well as find out whether the server is safe or not.

III. LITERATURE REVIEW

In Xiaofeng Wang, Kemu Pang, Xiaorui Zhou, Yang Zhou, Lu Li, and Jianru Xue [1], outlined, a real perceptual image hash method for content authentication is proposed. Using this hash, an image tampering detection and tampering localization method is developed. Their contribution involves Watson's visual model is used to extract the visually sensitive features that play an important role in the process of humans perceiving image content. The proposed method is robust to a wide range of geometric distortions and content- preserving manipulations such as JPEG compression, adding noise, and filtering. Furthermore, it is sensitive to content changes caused by malicious attacks. They have proposed method has the functionality of tampering localization. Additionally, it achieves a trade-off between robustness to tolerate geometric distortion and tampering localization. Also they have outlined Image-block-based features and key-point-based features are combined to generate intermediate hash code. They proposed to use Gaussian random matrices to reduce the vector dimension, and encryption and randomization are used to generate the final hash code. It is sensitive to changes caused by malicious attacks, and it achieves a trade-off between robustness against geometric distortion and tampering localization. The effectiveness and the availability of the proposed algorithm for different tampering attacks Compared with state-of-the-art schemes, yields better performance. R.Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin [2], introduces a novel calculation that uses a wavelet representation of pictures and new randomized preparing systems for hashing. They introduced a picture hashing calculation that changes over pictures into short, hearty piece strings. Utilizing this calculation, can think about two pictures by checking no good strings for definite correspondence, instead of endeavoring the much more included issue of looking at "fuzzy" picture information. Image hashes were powerful to different assaults, including both regular picture preparing and vindictive contortions. The hashing calculation joins different thoughts from the elds of mistake redressing codes, and cryptography.

Fang Liu(&) and Lee-Ming Cheng [3], proposed a perceptual hashing plan in light of wave particle change and randomized pixel tweak, which is fitting for picture content validation, picture database recovery. The proposed calculation can verify the pictures which have experienced basic substance protected picture preparing operations, for example, pressure, altering, clamor expansion furthermore the geometric control. It is all the while delicate to pernicious messing with the assurance of framework security. Rather than utilizing conventional change like DWT, DCT or other change, They have propose to utilize wave molecule change for the sparser development and better qualities to concentrate composition highlights when contrasted and others. the major disadvantage of the existing media hashing technologies is their limited resistance to geometric attacks.[4] Chun-Shien Lu Chao-Yong Hsu illustrate a novel geometric distortion-invariant image hashing scheme, which can be employed to perform copy detection and content authentication of digital images. a scenario of copy detection and tracing is given to outline how an image hashing approach can be employed to manage digital image contents. Given an image owned by its creator, an image copy detection sys- tem needs to find out whether illegal copies of the image exist on the Internet and, if they exist, return a list of suspect URLs. This content searching strategy can be accomplished by means of image hashing, and the output of the hashing system can offer owners information about unauthorized use of their precious media data. The hash database used for querying and searching can be built in an offline manner. As a result, time is mainly spent on mesh-based hash generation of an incoming query image. However, their scheme compensates for this cost by offering robustness against geometric distortions. A fast matching process has also been proposed to speed up searching in a large image database

Mohammad Fakhredanesh, Reza Safabakhsh, and Mohammad Rahmati [5], proposes to use Watson's visual model to improve perceptual undetectability of model-based steganography. The proposed method prevents visually perceptible changes during embedding. First, the maximum acceptable change in each discrete cosine transform coefficient is extracted based on Watson's visual model. Then a model is fitted to a low precision histogram of such coefficients and the message bits are encoded to this model. Finally, the encoded message bits are embedded in those coefficients whose maximum possible changes are visually imperceptible. Experimental results show that changes resulting from the proposed method are perceptually undetectable, whereas model-based steganography retains perceptually detectable changes. Their Experimental results show that the proposed method does not retain any perceptible change in the image while the model-based method retains many perceptible changes in the stego images.

Lima S Sebastiana, Abraham Varghese, Manesh T [6], proposes an image hash which is generated from Haralick and MOD-LBP features along with luminance and chrominance, which are computed from Zernike moments. Sender generates the hash from image features and attaches it with the image to be sent. The hash is analyzed at the receiver to examine the authenticity of the image. The method detects image forgery and locates the forged regions of the image. The proposed hash is robust to common content preserving

modifications and sensitive to malicious manipulations. The proposed hash is applicable to image authentication.

IV. PROPOSED APPROACH

In this paper we are proposing content authentication, tampering detection and security of server for the user who wish to save the image data stored on server like cloud, LAN. So that will make the storage more secure. Currently there is tremendous amount of image data being generated over internet, this data is very vulnerable to tampering, and hence it is necessary to provide an authentication process for image dataset as images are many times used as proofs. Here a real perceptual image hash method is proposed. Based on this hash, an image tampering detection is presented. The proposed method is sensitive to changes caused by malicious attacks, and it achieves a trade-off between robustness against geometric distortion and tampering localization. The proposed method can be used for content-based image authentication and for image retrieval and matching in large-scale image databases.

A perceptual image hash is expected to be able to survive unintentional distortion and reject malicious tampering within an acceptable extends .It involves proposing content based image authentication, forge detection. Additionally, it achieves a trade-off between robustness to tolerate tampering. Develop a client based application which can be installed on the system. The application will upload images to cloud server. The application will generate advance perceptual hash and save them at local storage for every image uploaded. The application will on downloading images back will perform content authentication on every images using locally stored hash information.

A. SIFT ALGORITHM.

1. Create internal representations of the original image to ensure scale invariance. This is done by generating a "scale space".
2. Find key points in an image and approximate it using the representation created earlier.
3. We now try to find key points. These are maxima and minima in the Difference of Gaussian image we calculate in step 2
4. Get rid of bad key points: Edges and low contrast regions are bad key points. Eliminating these makes the algorithm efficient and robust.
5. Assigning an orientation to the key points: An orientation is calculated for each key point. Any further calculations are done relative to this orientation. This effectively cancels out the effect of orientation, making it rotation invariant.
6. Generate SIFT features: finally, with scale and rotation invariance in place, one more representation is generated. This helps uniquely identify features. Let's say you have 50,000 features. With this representation, you can easily identify the feature you're looking for (say, a particular eye, or a sign board).

B.System Architecture

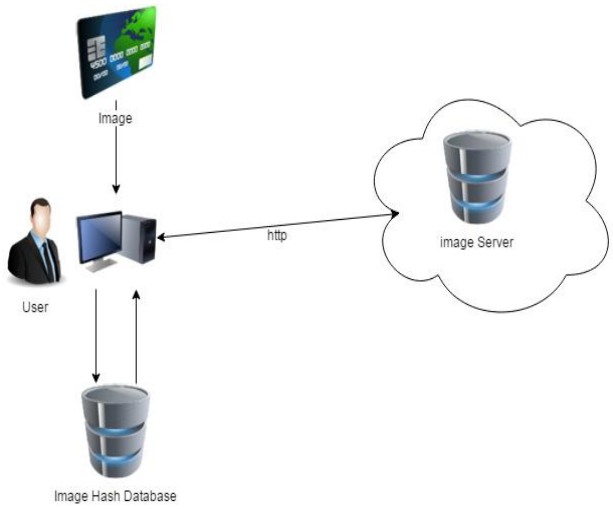

Fig.1. System Architecture

Fig.1. shows the architecture of the proposed system. Architecture contains User in the mid, who will upload or download image. Whenever user upload or download the image from server hash will be generated and stored in hash database. So that the comparison of hash values be done.

C. Mathematical Model for Proposed System

Proposed system can be represented as a set
$X = \{I, O, S_C, F_C\}$
Where,
I=set of inputs
O=set of outputs
SC= set of outputs in success cases
FC = set of outputs in failure cases

Input set $I = I = \{U_D, I_S\}$
Where, U_D = Set of user details,
I_S = Set of Images.

Output set $O = O = \{I_S, S_M, F_M\}$
Where, I_A = set of Images,
S_M = Success messages,
F_M = Failure message.

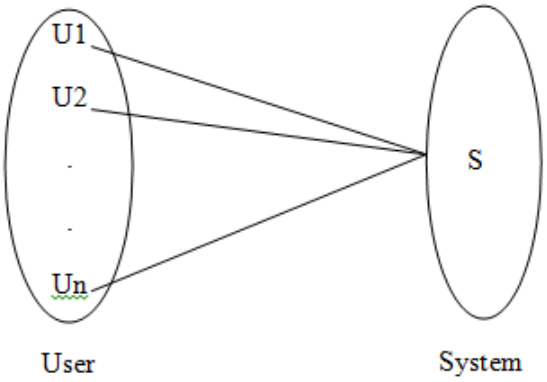

Fig.2. Mapping of User To System

Figure shows many users are allowed to use the system. So above figure shows mapping between system and user is one-to-many.

$S_C = \{I_{Un}\}$

Where, I_{Un} = valid set of images uploaded

$F_C = \{I_{Un}, NULL\}$

Where, I_{Uo} = invalid set of images uploaded

NULL represents no output

$C = \{C_1\}$

Where, C_1 = "System only accepts images of file types such as bmp, jpeg, png"

I_U, I_{Uo}, I_{Un} are in the form

$I = \{I_1, I_2 \ldots I_n\}$

Where, $I_1, I_2, \ldots, I_n$ are images.

NP-Complete: - Our application is NP-Complete. All the image processing hashing algorithms being used are at pixel level. Hence the performance of these algorithms is directly proportional to resolution of image. Thus in our application there is guarantee that we get output. Hence our application is NP-complete.

V. IMPLEMENTATION AND DISCUSSION

1. File Module

This module has 2 sub modules:

Upload Module: This module allows logged user to upload image file to cloud space. It will only allow image based file extension e.g. jpg, png only.

Download Module: This module includes all functionalities which allow users to select one of the uploaded files and download it.

2. Block Feature Extraction:

This module has all functionalities and algorithm required to calculate block wise hash values for input image. This input image is processed by Watson's visual model. First image is split into multiple non overlapping blocks. Features are calculated using SIFT algorithm for each block. This hash is stored at local machine in an index file and not at cloud.

3.Block Feature Matching:

This module contains functionality to compare two images. It reads the downloaded image first and performs block feature extraction. Using field it will get previously calculated hashes from index file. Now it will compare the hashes block by block. If all blocks match, then image is authenticate, no modification has taken place on image.

A. Input:-

Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the Time and performance of system.

Fig.3.Original image

Fig.4.Forged Image

B. Expected Result:-

Parameter	Proposed	Existing
Tampering rate	60	70
Hash generation	72	60

Compare Existing Vs. Proposed w.r.t Performance

Fig.5.Forged Detection

VI. CONCLUSION AND FUTURE SCOPE

In this paper, a genuine perceptual image hash strategy is proposed. It is necessary to provide an authentication process for image dataset as images are many times used as proofs. Here a real perceptual image hash method is proposed in which an image tampering detection and tampering localization method is presented. The proposed method is sensitive to changes caused by malicious attacks. It can be used for content-based image authentication and for image retrieval and matching in large-scale image databases So that it provide security to the image database and determines whether the database server is trustworthy or not. In future scope, provision for authentication of compressed images can be proposed. Also, Use of big data for performing authentication of vast image dataset can be researched.

REFERENCES

[1] Xiaofeng Wang, Kemu Pang, Xiaorui Zhou, Yang Zhou, Lu Li, and Jianru Xue, "A Visual Model-Based Perceptual Image Hash for Content Authentication," IEEE transactions on information forensics and security, vol. 10, no. 7, july 2015

[2] R.Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in Proc. Int. Conf. Image Process., 2000,pp. 664–666

[3] Fang Liu and Lee-Ming Cheng, "Wave Atom-Based Perceptual Image Hashing Against Content-Preserving and Content-Altering Attacks," Springer-Verlag Berlin Heidelberg 2015,Y.Q. Shi (Ed.): Transactions on DHMS X, LNCS 8948, pp. 21-37,2015.

[4] C.-S.Lu and C.-Y.Hsu, "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication," Multimedia Syst., vol. 11, no. 2, pp. 159–173, Dec. 2005.

[5] M. Fakhredanesh, R. Safabakhsh, and M. Rahmati, "A model-based image steganography method using Watson's visual model," *ETRI J.*, vol. 36, no. 3, p. 479, 2014.

[6] Lima S Sebastiana, Abraham Varghese, Manesh T, "Image Authentication by Content Preserving Robust Image Hashing Using Local and Global Features" International Conference on Information and Communication Technologies (ICICT 2014)

[7] D. G. Lowe, "Distinctive image features from scale-invariant key points," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, 2004.

[8] H. G. Schaathun, "On watermarking/fingerprinting for copyright protection," in Proc. 1st Int. Conf. Innov.Comput., Inf., Control (ICICIC), Aug/Sep. 2006, pp. 50–53.

[9] X. C. Guo and D. Hatzinakos, "Content based image hashing via wavelet and radon transform," in Advances in Multimedia Information Processing (Lecture Notes in Computer Science), vol. 4810. Berlin, Germany: Springer-Verlag, pp. 755–764.

.