ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A NOVEL IMAGE HASHING USING INVARIANT VECTOR DISTANCE WITH RING PARTITION.

S.Nithyadhevi[1],P.Sindhu[2],R.VincyRooth[2],R.Gomathi[2].

1. Asst.Professor/Department of CSE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India.
2. UG Scholar/Department of CSE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India.

Manuscript Info

Manuscript History:

Received: 14 January 2016
Final Accepted: 25 February 2016
Published Online: March 2016

Key words:
Ring Partition, Hash Generation, Digital Watermarking, Temper Detection.

Corresponding Author

S.Nithyadhevi.

Abstract

The image hashing is one of the most important technique in the multimedia security. The visually identical images provides more similar hash values. The hash values of an image can be calculated based on the features of an image such as texture, color, purity, intensity, brightness etc. In this paper we have to analyze the hacked image by comparing hash values of visually similar images which has the slight modifications. For this analysis we use ring partition method for detecting the temper from the original image. The features are extracted from image based on ring manner. After generating the hash values, they are compared with hash value of original image to determine the attacked image. In addition we achieve rotation robustness in our proposed scheme. In future we use watermarking concept for enhance the security.

Introduction:-

Now a days all kinds of peoples who uses the personal computers. They perform variety of task on it such as sharing ,retrieving, manipulation etc. These kind of operations leads a attacks, computer crimes such as hacking. Because of the attacks the peoples has a chance to loss their data or any information. To protecting and preventing data from the attack we have to use the discipline as computer forensics .The computer forensics is emerged during the time of investigating and recovering of digital evidences which is gathered from digital devices when the malfunctioning activity. Many forensics techniques are available to determine the forces of breaking and entering into the system such as forensics document examination, the use of galvanoplastic compounds to preserve footprints, ballistics and the dynamometer. The investigation of crime activities using some of the specialized mechanisms or procedures is called forensics investigation.

Fig.1(a) Activity Of Forensics Investigation.

Vulnerability is the flaw, many vulnerabilities are gathered from computer devices are documented into the common vulnerability and exposure(CVE) database. The vulnerability management is used to recovering the information, which are discovered from malfunctioning activity.

Vulnerability management uses the cyclical process of identifying ,classifying, remediating and mitigating the vulnerabilities. To secure the computer system from various attacks is important to understand about the various attacks. Various attacks has different motivation to breach the security of the system. Different categories of attacks are: Denial of service attack breach the security of the system by making the system or network resource is unavailable for the intended user. Attackers may enter wrong password continuously to cause the user account to be locked. Otherwise the attacker make overload to the capabilities of the system or a network resource to block the user at once. At that time, there may be a chance to get the information from the particular system by attacker.Tampering is the process of modification on the information for malicious purpose. After that the information may be used by any kind of user, they process with that malicious information .It may cause the problems into their process or system. Best example of tampering is Evil Maid attack.

In Privilege escalation, attackers has some restricted access, if they enter into the system without authorization. The privilege escalation describes a situation when the attackers access the system by fool it then escalate their privileges to access the restricted data. Even they act as a root and have a unrestricted access to the system.

In government entities, the local and regional government infrastructure like traffic light control, police and intelligence agency communications, financial systems, etc are may attacked by some criminal activities. The attacker commonly breach the security of military computer systems for know about the military information.

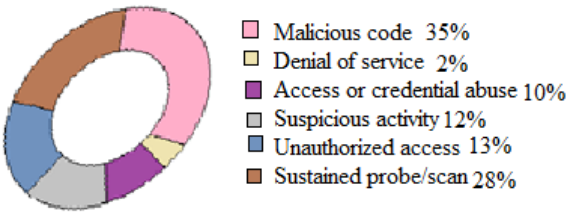

Fig.1(b)Categories Of Incidents.

Computer protection, The counter measure is an action ,event, procedure, mechanism or device to minimize the activity of threat, vulnerability, even an attack. It may discover the action from computer devices and reporting for take the corrective action against the harmful process. The security management may be improved via a design, hardware protection mechanism, secure operating system, secure codings, by responsing to breach.The knowledge of this domain was used in our proposed system. In this proposed system, the attacked images are discovered from digital devices and they are recovered from attack. Also providing the security to the image by using watermarking mechanism.

In the earlier mechanisms, they also attempting to recovering the image from attack. But they not fully attain their goal. According to the existing system, they attempt to generating a secondary image from the input image by dividing the input image into number of blocks, randomly selecting the sub image and so after preprocessing the input image. From the secondary image the features are extracted by using YC_bC_r color model, HSV color model for identifying the attacked image. These kinds of color models are does not providing the stable values. It may vary depending on their digital representation. So it cannot provide the optimal values for identification. There may be a possible to identify the original image as attacked one. Earlier methods unable to identify the minor modifications on the image caused by intruder. Also they cannot provide the similar values of same image, if the image is rotated. So they do not obtain the rotation robustness. Some of they obtain rotation within particular degree. If we attempt to apply any operation for temper detection, it may be fragile. To reduce these kinds of disabilities, we propose the ring partition mechanism. In our proposed system, the input image is divided into number of rings. From each ring the features are extracted by using CIE L*a*b* color space. Using that values the hash values are generated for corresponding image. Then the values are compared to visually identical image's hash value for identify the attacked image. After that the original image will be watermarked by using specified algorithm for improving the security of that image. This method can achieve rotation robustness with arbitrary angle.

Related work:-

Kang.L.W et.al [1] proposed a method, that only detecting the authentication of an image by generating the hash values. The hash code is generated by compressive sensing based random projection after down sampling that image. This technique cannot achieve the rotation robustness.

Lin.C.Yet.al[2]conclude the authentication strategy. In this approach, the JPEG image is encrypted with the help of secret key. Then it produce the signature. At the receiver end, the signature and received image will be decrypted. If the two values are equal, the image is considered as original one otherwise, hacked one.

Mongo.V et.al [3] exposed a clustering based approach to the image hashing for authenticate the image. In this approach the features are directly extracted from the image. From that the intermediate hash codes are generated. Then the final value is created by compress the intermediate hash code. This method also consider the authentication only, does not has the care about hacked image.

Mongo.V et.al [4] discussed about the determination of hacked image. In this paper non-negative matrix factorization method is used for generate the matrix values for randomly selected sub image of input image. Using the matrix value it creates the hash code. The randomly selecting manner may be reducing the detecting technology on attacked image.

Petitcolas.F.A.P et.al [5]describes the watermarking methodology to the image. The evaluation tool of watermarking provides simplicity, customization and modularity also a choice of test, but it do not check the content representation of the input image.

Swaminathan A et.al [6] discussed about the robust and secure hashing mechanism. But it achieve the rotation robustness within the 5°~20°. If we attempt to exceeds that degree the image will be fragile. It is difficult to find the minor modifications.

Tang.Z et.al [7] exposed a generation of hash values based on invariant moments of the image. In this, the input image is converted to normalized image. Then the color image is converted to the HSI and YC_bC_r color spaces. There is a need of two more color space conversions. After that the features are extracted based on its invariant moments. It does not has the rotation robustness.

Tang Z et.al [8] proposed ring based image hashing using non-negative matrix factorization. In this approach, the input image preprocessed and then divided based on ring mannerism. From the rings, the secondary image is formed by creating the number of strips. Then the features are extracted from the secondary image.

Tang.Z et.al [9] conclude detection of temper by using non-negative matrix factorization. In this approach, the noise is filtered from the input image. Then the image is divided into number of blocks. From the blocks the features are extracted and the similarities are checked by using hamming distances. It does not able to detect the minor changes on the image. It resists the rotation robustness.

Tang Z et.al[10] discussed about the image hashing based on lexicographical framework. The features of image are gathered and construct the dictionary. Then the image is divided into number of blocks. From the block the intermediate hash value is generated with the help of dictionary details. The final hash value is generated by compress the intermediate hash value. It will increase the computation burden.

Xiang.S et.al [11] proposed the histogram based image hashing scheme. In this scheme, the low pass filtering is applied to the input image. Then the features are extracted from the image based on histogram values. From that the hash values are created. But it has high computation cost.

Zhao.Y et.al [12] exposed robust image hashing based on Zernike moments. In this technique, preprocessing the input image and then the local and global features are extracted from the normalized image. After that the hash code is formed by using the features.

Proposed System:-

In our proposed system, the attacked image is identified from the input by using involved modules. Then the identified image removed and the original one is secured from other attacks by using watermarking mechanism. The modules includes preprocessing of image which performs filtering the noise from image. Then the image is converted into CIE L*a*b* color space. After that the image was divided into number of rings. Each rings has the same origin. From the ring required features are extracted by using CIE L*a*b* color space. Because this color space only gives the stable value. By using these values, the hash values are created. Then the attacked image is identified by checking the similarities between the hash values. For providing the security to the original image, the watermarking is used.

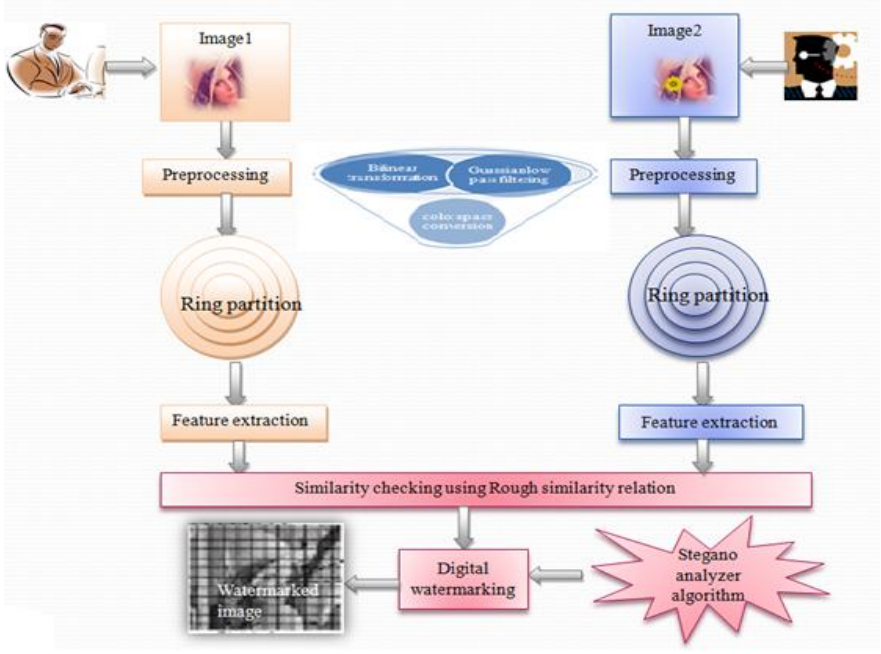

Fig.3 System Architecture

The modules of our proposed system are:-

Preprocessing:-

The input image has some addition of noise contamination or any modification of its digital representation. To determine the digital modifications of various images we have to use the preprocessing mechanism. It includes three different operations such as bilinear interpolation, Gaussian low pass filtering and color space conversion. The output of this module as normalized image. Normalized image is nothing but the intensity of that image is adjusted by using its pixels. The process of preprocessing as, the input image is converted into standard N×N size image for supporting different sized images. Then the Gaussian low pass filtering is applied to that image. The filtering can reduce the minor modification from the resized image. After that the color image is converted to CIE L*a*b* color space for extracting the stable values for hash code generation. The component of CIE L*a*b* color space represents, L* as lightness of image. Which is used for hash code generation. The values of L* component is more stable compared to the components of YC_bC_r color space and HSI color space. a* and b* are chromaticity coordinates of the image. The values of CIE L*a*b* color space are closely matches to the human perception level of lightness.

Ring partition:-

In this module, the preprocessed image is divided into number of rings. The center of the image is considered as origin of the ring. Each rings are divided based on the same origin. The number of rings of different images are expected to be same. The image contents of each rings does not change after rotation, so only we choose ring partition. From each ring the features are extracted, this property provides the chance to create hash values which is resistant to rotation.

Feature Extraction:-

The statistical features of each image are extracted from each rings of them. The CIE L*a*b* color space is used for providing the stable features for hash generation. To identify the visual content of rings, we have to determine the four different statistics such as mean, variance, skewness and kurtosis. Using these statistics we have to generate the hash values by using secure hashing algorithm. If any modification in the original image, however small changes it must cause a changes to the hash value. So the hash values of original one and attacked one both are fully different. Which is identified by checking the similarities between both hash values.

Similarity Checking:-

Checking the similarities between the hash values of both original and hacked images by using rough similarity relation. The rough similarity relation is a tool for determine the similarities of two different values. The tempered image has the different hash value compared with the hash value of original image.

Digital Watermarking:-

The watermarking mechanism is used for enhance the security to the original image. The steganography method is implemented into our proposed system for provide security to the specified image by using stegano analyzer algorithm. It prevents the image from the harmful attacks.

Conclusion:-

In this paper we have to analyze the hacked image by comparing hash values of visually similar images which has the slight modifications. During analysis of attacked images improve the rotation robustness and also compared with existing images using ring partition mechanism. Also we enhance the security of original image with the help of watermarking scheme.In future, implement this project for supporting all kinds of image. Also improves the capability of similarity checking for find hacked image, if the same hash value will be obtained.

Reference:-

1. Kang L W, Lu C S, and Hsu C Y(Nov.2009),"Compressive sensing-based image hashing," in Proc. IEEE Int. Conf. Image Process., pp. 1285–1288.
2. Lin C Y and Chang S F(Feb. 2001),"A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans.Circuits Syst. Video Technol., vol. 11, no. 2, pp. 153–168.
3. Monga V,Banerjee A and Evans B L(Mar. 2006),"A clustering based approach to perceptual image hashing,"IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68–79.
4. Monga V and Mihçak M K(Sep. 2007), "Robust and secure image hashing via non-negative matrix factorizations," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 376–390.
5. Petitcolas F A P (Sep.2000), "Watermarking schemes evaluation,"IEEE Signal Process. Mag., vol. 17, no.5, pp.58–64.
6. Swaminathan A,Mao Y and Wu M(Jun. 2006),"Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230.
7. Tang Z,Dai Y and Zhang X(2012),"Perceptual hashing for color images using invariant moments,"Appl.Math.Inf. Sci., vol. 6, no. 2S, pp. 643S–650S.
8. Tang Z,Zhang X and Zhang S(Mar. 2014),"Robust perceptual image hashing based on ring partition and NMF," IEEE Trans. Knowl. Data Eng., vol. 26, no. 3, pp. 711–724.
9. Tang Z,Wang S,Zhang X,Wei W and Su S(2008),"Robust image hashing for tamper detection using non-negative matrix factorization"J.Ubiquitous Converg.Technol.,vol.2,no.1,pp. 18–26.
10. Tang Z,Wang S,Zhang X,Wei W and Zhao Y(2011), "Lexicographical framework for image hashing with implementation based on DCT and NMF," Multimedia Tools Appl., vol. 52, nos. 2–3, pp. 325–345.
11. Xiang S,Kim H J and Huang J(2007),"Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Workshop Multimedia Secur.,pp.121–128.
12. Zhao Y,Wang S,Zhang X and Yao H(Jan. 2013),"Robust hashing for image authentication using Zernike moments and local features,"IEEE Trans. Inf. Forensics Security, vol.8, no.1, pp.55–63.