ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Photo Proof Approach for Authenticating Transformations on Image

Prof. Pankaj Agarkar[1], Manisha Khandagale[2], Shweta Somwanshi[3], Kalpna Dhavare[4], Swati Ombale[5]

Research Scholar, Dept. of Computer, JJTU, Zhunzuno, Raj, India[1]

Dept. of Computer Engineering, Pune University, *Pune, India*[2,3,4,5]

ABSTRACT: Photo is a picturerepresentation of any incidence or situation, because of this it is used as proof of any incidence or situation. but there are many tools available now a days which are sufficient for making the fake images. Thus many methods has been developed to overcome this problem, some of them are thumbnails,digitalsignature,semifragrilewatermarking, robust hashing etc.but they permit only few of transformations on image and have other disadvantages also.

We present photo proof scheme which overcome all the disadvantages of existing system such as non negligible error probability, vulnerability to adversaries,lack of succinctness.

This approach also permit any set of transformations on image according to application thus it can be configured according to need of application. Thisapproach has a key term called PCD(proof carrying data) ,which is a set of computationalintigrity represents proof stating that an image is original image or transformations performed on image are permissible(it does not changed image data).

KEYWORDS: PCD, Thumbnails, Robust hashing,semifragrilewatermarking, digital signature.

I. INTRODUCTION

photography is most popular trade or media for new generations,cameras are usually inbuilt into mobile devices portable computers,to make photography more effective many editing tools invented .also there are many tools which are common and have ability to change the image data in such a manner that the image became fake. In some areas image is used as proof of any event, in such a areas image data is very sensitive and should not be get changed. Distinguishing the original image from fake images just by observing is very difficult and time consuming.Thus many of methods developed for authenticating images or for distinguishing original images.

Following are the techniques which was invented earlier for proving orignal image:

Thumbnails:earlier forensic experts has been used this method.thisapproach include thumbnails included into its header files and whenever image data changes thumbnail get changed.but this technique was very time consuming and unreliable.

Digital Signature: This is another approach which readily verified anywhere, in this approachthe secrete signing key is embedded into its Image signal processor. The signature Is verified every time using public signing key but because of sensitive design it was not too popular,even for smallest change in image the signature get mismatched.

Semifragrile watermarking: In this approach a key sign is embeddedinto image and the signature which is embedded is completelyinvisible. Unlike previous digital signature it was not too sensitive design thus it allows some transformations. when these fixed transformations performed on image it accept those.semifragile term comes later which divides image into block and applies watermarking on these blocks.

Robust Hashing: In this scheme the digest value is used for verifying the image. For every image is calculated by using hash function. If the transformations done on image is permissible then thealtered image's digest number is close to original image.

All the techniques discussed above havefollowing disadvantages:

Fixed set of transformations: These all approachsupports only few of transformations.

DOI: 10.15680/IJIRCCE.2016. 0410083

Generally every approach support only some set of transformations. None of them can support every transformations thus the cant be configured according to application.

Vulnerabilities to advertises: If the attacker is familiar with these techniques then he can easily attack the image or change any image. And after changing image completely alsoit can seems realistic.

Lack of succinctness: this is the a problem occurs in all above techniques in which image size grows rapidly as any transformation performed on it, thus verification of actual image become time consuming process..for robust hashing method this result in larger image data and in watermarking because of this image quality decreases.

Certipics: It is scheme is intended by Walsh. It is an image authentication software which run on nexus operating system. In this software we have to define first allowed transformations and editing rules. This software has disadvantage like succinctness.

II. FOCUS

Our goal is to present photo proofapproach which will allows any set of transformations on image so that it can be configured according to any application .to Following are the methods which are used as key terms:

1]PCD(proof carrying data) [1]-it is the term defined by cheisa and tromer which attaches proof to every image in distributed network.proof is nothing but the computationalintegrity which prove that image is not fake.verifier only have to check the proof instead image.

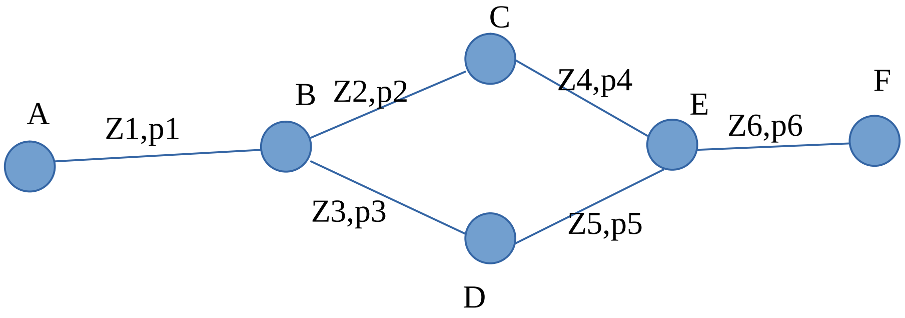

Fig: A PCD computation transcript.

For example there are six systems connected in a distributed network suppose A,B,C,D,E,F are the systemsconnected in that way as one system gives input image(z1) to other image along with proof (p1) that is computational integrity distinguishes the actual image from fake image. Every system sends PCD along with image thus at verification side only proofs verified not image itself. In the above figure system A sends image Z1 with p1 system B verifies the proof and if want to any transformations it perform and generates proof stating that the transformations performed was permissible the original image data has not changed. At last verifier has to check only the proof of last system that is F in fig.

The working of PCD is prover prove to verifier and at that time he gives to verifier following properties - 1] zeroknowledge: the actual image data remains secret still proverproves that data is valid and verifier accept 2]soundness: soundness proof system called as argument which is computationally sound. 3] Succitness: Proof is not lengthy and easy to verification.

We uses libSnark library of c++ which is useful for following implementation: 1]Rank 1 ConstraintSystem(R1SC) is a NP-Complete language is used for pre-processing of zkSnark. Gadget Library: 2]Two Gadget Libraries are gadgetlib1.

Gadgetlib1 uses template and it’s a low level library dadgetlib1 use for reduction and PCD.gadgetlib2 -gadget lib2 does not uses templates and its alternate to gadgetlib1.using library following are important steps :use generator algorithm of libsnarks,useprover algorithm of libsnarks,use verifier algorithm libsnarks.

2] Semifragrile watermarking technique which accept a JPEG lossy compression on the image which is watermarked and then rejects the malicious attack.Usingof JPEG compression adjustment of brightness the image is done that updated image authenticator. By using secrete block mapping function controls the signature generating process. Authenticator based on two invariant properties of discrete cosine transform (DCT) coefficients before and after JPEG compressions. - C.y.Lin and s -f chang.

3] Image authentication used to detect actualness of an image from malicious manipulations. so this describe technique for image authentication .image authentication technology able to secure the image from image producing until it uses. For achieving authenticity of digital image two methods are used. First is encrypted digital signature which is inbuilt in image. Digital signature uses public key encryption. The image is encrypted by private key and to decrypt the image public key is used. Second method is watermark which is used in an image. After manipulation or transformation of image fragile watermark was destroyed. In image authentication authenticity of image is also checked by watermark. There are two ways of transformations on image as method and purpose.

EXISTING SYSTEMS

Sr. No.	Paper Name	Parameters Used			Technology Used		
		Flexible specifica -tion	Negligible error probability	Size Over-head	Semifragile Water-marking	Robust Hash-ing	Proof carry-ing data
1	Semifragile Watermarking.	×	×	O(n)	✓	×	×
2	A robust image authentication method.	×	×	O(n)	×	✓	×
3	Proof carrying data .	Any efficient transformation	✓	O(1)	×	×	✓

III. Conclusions and Future Direction

we present the new a approach called Photo proof which is depend on concept PCD.There are many existing system discussed in this paper, every method is depend on new technique .since first method invented called thumbnail to Proof carrying Data(PCD) every method follows different way for verifying the image or distinguishing original image from fake images every method have its own advantages and disadvantages.All existing methods does not support all tranformations.In this approach which we have presented support all transformations thus according to application we can decide which set of transformations should be allowed.

Iv. Acknowledgment

I take this opportunity to thank our guide Prof. PankajAgarkar ME coordinator of CSE for his inspiration and guidance .We thanks to HOD comp, Prof. Soumitra Das and Director, Dr.S.S.Sonavane.

References

1. Lin and Chang."Semifragile watermarking for authenticating JPEGVisualcontent,"in Electronic Imaging.
2. Lin and S.Chang."A robust image authentication method distinguishing JPEG compression from malicious manipulation".
3. Chiesa and Tromer,"Proof-carring data and hearsay arguments from signature cards."