Volume : 4 | Issue : 10 | October 2015 • ISSN No 2277 - 8179

Research Paper

Combining Hashing Techniques in Image Authentication system:A Survey

Computer Science

KEYWORDS : Content based Image authentication ,DWT and SVD, AMAC ,Fixed Point Theory, HMM and SVM

K.Alice Asst Prof ,GKM College of Engineering and, Technology, Anna University

N.Ramaraj Professor, Thanagavelu Engineering College, Anna University

ABSTRACT

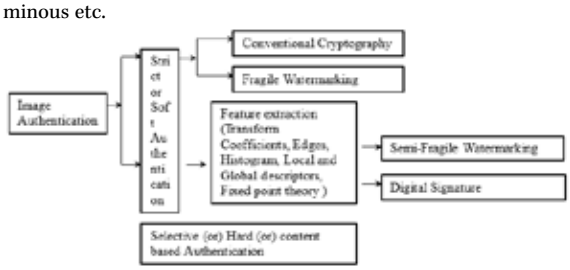
In content based image authentication system the image hash is generated by extracting image features that holds the content of the image using transform coefficients, Edges, Statistical methods, Local and Global descriptors, Histogram etc. Many authentication systems employ any one of the feature extraction methods to generate an image hash. Recently most authentication system uses a combination of two or more feature extraction methods, to extract the content of image and then to generate an image hash. This is done to fully exploit the advantage of two or more methods over just a single method. In this paper a survey on most recent work in the area of content based image authentication that uses two or more feature extraction techniques and a performance analysis on each of the system based on the requirement of an authentication system is given.

1. Introduction

The widespread use of multimedia data in internet increases the need for image authentication. Image authentication verifies the originality of the transmitted image at the receiver end. Image authentication is highly essential in the area of military target images, court evidence images, quality control images, digital notaries' document, medical images, etc where false judgment leads to tragic results. Multimedia data authentication is different from other data authentication because multimedia data is always preprocessed (Quantized, Compression, Scaling or Cropping) before usage and transmission [2].

Image authentication is broadly classified into two categories: Strict (Hard) authentication and Selective (Soft or Content based) authentication [1]. Strict authentication cannot tolerate even a single pixel change in image. This authentication is implemented by using conventional cryptographic algorithm (SHA-1, MD5 etc) and fragile watermarking techniques. The basic idea behind fragile watermarking technique is use to generate a watermark and it is inserted in the image in such a way that any modification in the image is reflected in the inserted watermark. Simply verifying the presence of the inserted watermark allows the image authenticity verification. The image is considered authentic if and only if its entire pixel remains unchanged.

Selective authentication can be classified as digital signature [7] and semi-fragile watermarking [8]. Selective authentication method authenticates the image as long as the content of the image is preserved during the modification. Some of the content preserving modification includes image file format, geometric transformations, (scaling, translation, rotation etc) transmission errors, transmission noise, compression, quantization etc. This method fails in authentication for those modifications that change the content of image. Some of the manipulation that change the image content may be deletion of objects from the image, addition of objects into the image, position change of the object in the image , change in image background, change in luminous etc.



Content based image authentication concentrates on authenticating the content of the image rather than image as a whole. Most approaches extract the features of the image that holds the content of the image and provide security and authenticity. Features can be extracted based on transform coefficients' (DCT, DWT, SVD, etc), edges, histogram, local and global descriptors etc. These features are used to create image hash for authentication purpose.

The basic requirement of a good authentication system can be given as follows [1]: Robustness- The system should tolerate content preserving transformations. Security- The system should be able to protect the data from malicious attack. Sensitivity- The system should detect any content modifications or manipulations. Localization - The system should be able to locate the area of tampering. Recovery- The system should be able to reconstruct the tampered regions. Complexity - The system must be neither complex nor slow. Portability- The system must be able to carry the digital signature within the image.

The paper is organized as follows: Section II describes the methods of few recent works in the area of image authentication. Section III provides a performance analysis of all the methods described in section II based on the requirement of authentication system. Section IV concludes the paper.

2. Few recent work in the area of content based image authentication

Two phase image authentication

Two phase image authentication method [2], uses a combination of strict and selective authentication using two most generic approximate message authenticate codes (AMAC). Image feature that contains the content of image are extracted and are protected by hard authentication using AMAC which enables forgery detection and the less fragile content holder parts are protected by soft authentication to provide robustness to the mechanism

Discrete cosine transformation is applied to equal sized blocks of the image and the low frequency elements of the image is subjected to first phase to generate tag1 using DCT-RS(Reed Solomon) based scheme. If the first phase succeeds, some high frequency of the image are left for the second phase to generate tag 2 using probabilistic target collision and resistant hash function. Tag 1 and tag 2 is concatenated to generate digital signature for the image.

MAC is sensitive to noise but AMAC is noise tolerant. The use of AMAC increases robustness. AMAC enables error detection and partial error localization. The proposed method is unable to classify and identify the type of attack or to localize the affected part of the image.

Watermarking for image based on DWT & SVD

The proposed method [3] generates a digital watermark by combin-

ing DWT and SVD. This method uses two watermark one text and another logo. The image is transformed using DCT and SVD is applied to HH1 sub band. SVD is applied to the two watermarks. The SV's of first watermark is embedded in suitable SV's of HH1 sub band of the original image and key1 is generated for reconstruction of watermark 1. The second level on decomposition is applied to HH1 and SVD is applied to HH2 sub band of HH1. The SV's of second water mark is embedded in suitable SV's of HH2 sub band and a key 2 is generated to reconstruct watermark 2.

In this method a text is embedded in the first DWT level and logo is embedded in second DWT level. The two watermarks are separate and text can be extracted without affecting logo and vice versa. For watermark extraction, the watermarked image undergoes two levels of DWT decomposition. Then from two HH sub bands using key1 and key2 the two watermarks are reconstructed based on the SV's and orthogonal matrices.

Image authentication using local and global features

The image hash in [4] generated from Haralick features and MOD-LBP feature with luminance and chrominance which are computer using Zernike moments .Local features like Haralick MOD-LBP feature are extracted from preprocessed image (rescaled and divided into non overlapping equal sized blocks) and global features like luminance and chrominance are extracted from Zernike moments . From the local and the global descriptors, feature vectors are constructed and they are encrypted. The encrypted feature vectors and concatenated to generate the image hash. At the receiver the image hash is verified by finding the difference in both local and global feature vectors and also there total difference .The threshold of hash distance for the proposed method is selected as 1. Blocks' having a hash distance greater than 1 is regard as tampered block.

Spatial and Frequency domain complimentary water mark

A dual watermarking scheme [5] is proposed that generated two watermarks, one watermark is based on spatial domain and other watermark is base on frequency domain. The two watermarks complement each other. In spatial domain edge features are extracted using canny edge detector and protected using AMAC. Since AMAC is noise tolerant it can tolerate minor modifications .The frequency domain transform coefficients (DCT-RS based scheme) are protected using error correcting codes which is used in error localization and correction, only if the number of modifications is below the error correction capability of RS codes.

Image Authentication base on fixed point theory

The propose method [9] introduces a new technique called fixed point theory. In fixed point theory a fixed point image is created which is very close to original image. The system transforms a original image into a fixed point image using Gaussian convolution and deconvolution transform and sends the fixed point image instead of original to receiver. At the receiver using the same transform a fixed point image is generated for the received image. The integrity of fixed image is tested by comparing the fixed point image received and computed at the receivers end to locate the tampered areas. For finding the fixed point three iterative algorithms are used with few number of iterations.

The proposed fixed point theory uses Gaussian kernel in frequency domain. It generates a fragile system and semi fragile system for image authentication. The system shows good performance in transparency, fragility, security, and tampering localization. Semi fragile system is resistant to rotation by a multiple of 90 degree flipping and brightness attack.

Image Authentication based on HMM and SVM classifiers

The proposed system [6], uses machine learning methods (ie) Hidden Markov Model and Support Vector Machine to classify the input image as authentic (Class I) or forged image (Class II). The system undergoes a training phase using HMM and SVM models to make the system learn to classify authentic and forged images. Training is performed using 1250 authentic and 1250 forged images randomly selected from the CASIA image database.

Once the training phase is over the system is ready for testing phase. In testing the input image features are extracted using DCT, LBP, Gabor filter and Curvelet transform. Feature vector is normalized and a one is added to all feature vector values because HMM can process only non zero values. Initial data classification is done by HMM. A search is performed for best combination of states for the maximum a posteriori possibility using log likelihood estimator. If the likelihood value is infinite then the data is classified using SVM and it is deducted as Class I or Class II.

3. Performance Analysis

The basic requirement of an authenticated system includes robustness, sensitivity, security, localization, recovery, portability, and complexity. All the method of image authentication discussed in Section II is based on the combination of two or more mechanisms for generating image hash function. This is done to increase the performance of the authentication system. The computational complexity increased by using combination of methods can be compromised by the security achieve by the system. Portability exists in all the systems as the system is able to carry the digital signatures with the image. The following TABLE I analysis the various methods of section II in terms of Robustness, Sensitivity, Security, Localization and Recovery.

4. Conclusion

In content based authentic system combination of hash techniques to generate image hash is employed to have a choice in increasing the Robustness, security and sensitivity on the system. To develop a system that is robust against JPEG & JPEG 2000 compression DCT or DWT transform coefficients can be used. SVD & NNMF are robust to geometrical minor modifications [2] AMAC can tolerate noise [5] water mark embedded in frequency domain is more robust than water mark embedded in Spatial [3]. Drawback of content based authentication system is the possibility of having same feature vector for different images [5] this vulnerability cannot be removed decisively, but can be avoided by generating a combination of global and local image features.

In all the methods discussed in section II tamper localization is addressed in [4],[5],[9], and recovery of tampered regions of an image is done partially using Read Solomon code [5] is used for partial recovery but it has its limitation.

TABLE I : Performance Analysis

Methods	Robustness	Sensitivity	Security	Localization and Recovery
Two phase Image Authentication	Tolerate at high level: JPEG compression, additive Gaussian noise, Blurring, Uniform filtering. At low level: Average filtering, Gamma Correction, Shearing. The system does not tolerate Rotation and Scaling	The use of MAC guarantees that any change in secret key should be detectable by the corresponding change of approximately 50% of the output bits	The security threat is image tampering attacks. The tampered pixels are not reflected by the protected components.	It is unable to localize or reconstruct the affected part of the image.

Watermarking for image based on DWT & SVD	Robustness is measured in terms of correlation coefficient for the attacks like rotation, resize, JPEG compression, Average Filtering, Median Filtering, Motion Blurring, Histogram Equalization, Sharpen, Contrast Adjustment(lie in the range of 0.847 to 0.997. The system is inefficient with cropping attack.	Peak signal to noise Ratio is used to measure the visual quality of the watermarked image in comparison to the original image. It has high PSNR (up to 98.03)because the SV's of watermark are embedded in the Suitable SV'S of original image	The security of the system is improved by using DWT and SVD. It also uses a key to ensure the security of watermark during Embedding and Extraction process.	It is unable to localize or reconstruct the affected part of the image.
Image Authentication using local and global features.	MOD-LBP features are robust to content preserving modifications. The method is robust to JPEG coding, additive noise, rotation, scaling, brightness, contrast adjustment and slight cropping.	The use of Haralick features extracted from image blocks are sensitive to tampering as compared to MOD-LBP feature.	The security of the system is improved by combining both local and global descriptors	Image localization can be achieved by comparing the image blocks at the receiver and if the hash distance is greater than 1 for any two blocks it is then considered as tampered block. No Recovery.
Spatial and Frequency domain complementary watermark.	AMAC used to generate watermark1 can tolerate salt pepper noise of magnitude .01 and 0.1 but in frequency domain watermark it cannot tolerate high noise level (magnitude 0.1)	The use of ACs in feature vector strengthens the scheme against attacks based on recovery of DC coefficients	For images of high resolution AMAC is computed using Normalized Hamming Distance to avoid security vulnerability. The security of the system is improved by combining image edges and DCT coefficients.	In Frequency domain the use of RS Code in watermark generation is used to locate the forgery areas but was unable to recovery forgery if the number of modifications is beyond the error correction capability of RS codes.
Image Authentication based on Fixed Point Theory.	Fragile System cannot tolerate JPEG compression, scaling, Low pass filter, cropping, contrast adjustment and noise attack. Since the modified image is a non fixed image it cannot pass the authentication. Semi fragile system can tolerate rotation, flipping and Brightness attacks.	Even if image is changed by single pixel the change can be found with a probability of 0.965 for single pixel and 0.999 for two pixel changes. It is sensitive to key, since different keys have very small probability to produce identical fixed point images. if the size of the fixed point image is changed by the attacker then the GCD transform will vary since it is built for both key and image size.	In fragile system the security of the system depends on the secret key. The key space must be large. The Kernel should have less modification. The Selected key must be sufficiently far away from the center of the kernel. In Semi fragile system the security is improved by an additional chaotic transform to enlarge the key space	Localization is possible because if the image is tampered then the receiver can generate only a non fixed image. The difference in received and generated image is used to identify the tampered regions. No Recovery.
Image Authentication base on HMM and SVM classifiers.	It is tolerant to Lossy JPEG compression with Q from 50-90, Gaussian blurring , AWGN, Image splicing and copy move forgery	It refers to the ability of the algorithm to deduct a forged image correctly as forged can be given as TN/TN+FP where TN (True negative) = authentic image identified as authentic. FP (False positive) – Authentic image identified as forged	The system classifies the image as authentic or forged using HMM and SVM models. It does not address about providing security to the system.	It is does not address about localization and recovery.

REFERENCE

A.Haouzia, R Noumeir, "Methods for image authentication A survey" , Multimedia tools Appl 39: 1-46,Springer 2008. [2]. Seyed Amir "Secure and robust two-phase image authentication", IEEE transaction on multimedia, Vol 17, No 7, ppno 945 -956 July 2015. [3]. Tri.H.Nguyen,Duc.M.Duong and Duc.A.Doung,"Robust and High Capacity watermarking for image based on DWT-SVD", IEEE RIVF, International conference on computing and communication Technologies Research Innovation and Vision for Future(RIVF) 2015. [4]. Lima Sebatian,Abraham Varghese,Manesh.T ," Image Authentication by content preserving robust image hashing using local and global features",1877-0509, published by Elsevier B.V, Copyright 2015 [5]. Obaid Ur Rehman, S. Amir Hossein A.E. Tabatabaci, Natasa Zivic,Christoph Ruland, "Spatial and frequency domain complementary watermarks for image Authentication and Correction.SCC 2015 in Hamburg,Germany,CopyrightVDE Verlag GMBH Berlin, Feb 2-5 2015 [6]. M.F.Hashmi,A.R.Hambarde,A.G Keskar, "Robust image authentication based on HMM and SVD Classifiers" , Engineering letters 22: 4 El-22-4-04-Nov 2014. [7]. G.L.Friedman , " The trustworthy digital camera: Restoring the credibility to the photographic image", IEEE Trans.Consum.Electron..Vol 39 no 4 pp 905-910, Nov 1993 [8]. S.Walton, "Information authentication for a slippery new age", Dr.Dobbs.J.Vol 20 no 4 pp 18-26 April 1995, [9]. XuLi,Xingming Sun, " Image Integrity Authentication Scheme based on Fixed Point Theory", IEEE trans. On Image processing Vol 24,no2 Feb 2015