ISSN:2320-0790

An International Journal of Advanced Computer Technology

Image Authentication Techniques and Advances Survey

Derroll David[1], Divya B.[2]

[1]PG Scholar, [2]Head of Department
Department of Computer Science and Engineering,
Vimal Jyothi Engineering College, Kannur, Kerala, India

Abstract: With the advanced technologies in the area of Engineering the World has become a smaller place and communication is in our finger tips. The multimedia sharing traffic through electronic media has increased tremendously in the recent years with the higher use of social networking sites. The statistics of amount of images uploaded in the internet per day is very huge. Digital Image security has become vulnerable due to increase transmission over non-secure channel and needs protection. Digital Images play a crucial role in medical and military images etc. and any tampering of them is a serious issue. Several approaches are introduced to authenticate multimedia images. These approaches can be categorized into fragile and semi-fragile watermarking, conventional cryptography and digital signatures based on the image content. The aim of this paper is to provide a comparative study and also a survey of emerging techniques for image authentication. The important requirements for an efficient image authentication system design are discussed along with the classification of image authentication into tamper detection, localization and reconstruction and robustness against image processing operation. Furthermore, the concept of image content based authentication is enlightened.

Keywords: Image Authentication, Forgery, Watermarking, Digital image signature, Hashing.

1. Introduction

Information is facts provided or learned about something or someone. Exploitation of information can be used for profiteering. Traditionally, voice or manuscripts are used for communication but in the modern era information can travel miles. Images are transmitted through unsecure medias that are used for these communications and hence volatile to attacks and create a risk factor in area such as military, crime file, researches, medical diagnosis etc. Preprocessing operation such as quantization, compression, scaling, rotations may not change the semantic meaning of the image and thus identification of the image based on robustness is encouraged. Image Authentication is a mandatory in areas where image security is challenged. The basic requirements for an image authentication system are sensitivity, robustness, localization, recovery, security, portability and complexity. Some of the Mathematical Tools used in message authentication are modified for image authentication namely cryptography, digital signatures and hash functions. Image forensic can be identified by using some tools as pixel-based technique that detect statistical anomalies introduced at pixel level, format-based technique that leverage the statistical correlations introduced by a specific lossy compression scheme, camera-based technique that exploits artifacts introduced by camera lens, sensor or chip post-processing, physical-based technique that explicitly model and detect anomalies in the 3D interaction between physical objects, light, and the camera, geometric-based technique that make measurements of objects in the world and their positions relative to the camera.

A. Classification for Image Authentication

Firstly, digital image forgery detection can be classified as active and passive approach. In active approach, the digital image requires some preprocessing such as watermarking or signature associated with an image. In passive approach, digital forgeries may not leave any visual difference but they alter the underlying statistics of the image.

Secondly, image authentication is classified as strict and selective authentication. In strict authentication, even if a single image pixel or bit is changed the image is considered as non-authentic. Usually it is rarely used in practical scenarios. In selective authentication, when the protected image needs to be robust to some image processing operation such as geometric transformation, filtering, compression etc the exact pixel match is not encouraged. Conventional cryptography and Fragile Watermarking are techniques for strict authentication whereas Semi-fragile Watermarking and Image Content signature are techniques for selective authentication. Reversible Watermarking is a subclass of Fragile Watermarking in which the image is reconstructed to obtain the exact original image.

B. Procedure of Image Authentication

Image authentication is used to verify or validate whether an image is authentic. It provides an agreement that there is no change to the original image and the test image. The image to secure is first passed through some image authentication techniques such as watermarking, hashing etc. It is then transmitted through a non-secure media or communicated to the receiver. At the receiver, sequence generated by image authentication technique is restored and computed to compare

if it matches the original. If there is a match then the image is authentic else not.

2. Literature Survey

Image authentication has obtained significance because many areas in science and literature are using images for diagnosis, proof of identity, entertainment etc. There are many image authentication techniques.

2.1 Conventional Cryptography

A message authentication code (MAC) is generated from the image using hash function [2] - [8]. The hash is further encrypted using secrete private key of the sender or by public key of the receiver and appended to the image. At the receiver, the hash is extracted and decrypted using private key. Both these hashes are compared to check the validity.

In line – column hash functions, for each line and column a hash is generated and stored. At the receiver, the same process is repeated and the hashes are then compared with the stored. If any change is identified then manipulations have occurred and if not it is declared authentic. Tampering can be localized by the corresponding line and column where the difference happened. Unfortunately, the issue with this approach is called ambiguity problem. That is, if more than one region is corrupted then tampering cannot be identified.

Wolfgang and Delp [9] proposed a solution for the ambiguity problem. The image is divided into blocks of same block size. Hashes are computed for each block in an image separately and compared with the original images hash value. If there is any change for blocks, then the image is tampered and localization is possible else it is authentic. Localization capability has increased due to hash computed for each block separately. But restoring of tampered regions is not possible.

2.2 Watermarking

Watermarking is a technique by which a watermark is computed and hidden in the image. It is then extracted whenever necessary. There are two types of watermarking namely,

- Fragile Watermarking

  Watermark is generated and inserted in the image. Any modification to the image will also be reflected in the inserted watermark. Authenticity is verified by the presence of watermark and if there is no change in the pixels. Tamper localization is possible and image distortion cannot be tolerated.

- Semi-Fragile Watermarking

  Watermark is generated and inserted in the original image in such a way that the protected image can undergo some specific image processing operations while it is still possible to detect malevolent alterations and to locate and restore image regions that have been altered.

Walton S. [10] was the first to propose an image authentication technique using fragile watermarking. Image information is used to generate the watermark. The checksum calculated with the grey level of the seven most significant bits of pseudo-randomly selected pixels are inserted in the least significant bits (LSB). Manipulations can be detected and localized but does not have the capability to restore the original images.

Fridrich et al. [11] proposed a system in which a sufficiently large number N which impacts the probability of tamper detection is chosen to calculate the checksums. The original image is first subdivided into blocks of size 8×8; in each block, a pseudo-random walk through its 64 pixels is generated. The checksum S is computed and the binary format of the same is encoded with a secret key using a coding algorithm. Hence security is ensured. Image authenticity is achieved by extracting the checksum and recalculating in a similar way for the received image. If they are same then it is authentic else not. Detection and localization of tampering is identified in a simple and fast method. However, it cannot detect the manipulation if blocks from the same position of two different images, which are protected with the same key were exchanged. Several improvements were made to this method by extracting more robust bits [12]. Restoration capability is not provided.

Yeung and Mintzer proposed a method [13] to generate a binary function with a secret key. The function of binary function is to map integers from the interval {0 - 255} to binary values 0 or 1. For color images, the function is created for each color channel. These binary functions are used to code a logo L. For checking the authenticity, the user can check the value of logo for each pixel. The logo L can be inserted more deeply by using more grey levels to increase the security of the method. Image integrity and localization of tampered area is possible. Fridrich and Memon [14, 15] showed it is possible to estimate the inserted logo or binary function, if secret key for binary function is used in many images. This attack is called vector quantification attack [16]. To prevent it, Fridrich proposed in his work [17], to make the logo dependable on image indexes. These indexes are inserted in the original image several times into various blocks to exclude all attempts to remove them. However this technique remains vulnerable to this attack because the used method is not very reliable.

To avoid the vector quantification attack, Wong et al. [18, 19] proposed an asymmetric method based on public or private key which was improvised along with Memon [20]. The original image and the logo are subdivided into blocks. For each block another corresponding block is generated which are elements of the former except the LSB that is zero. Hash is generated for the new block using MD5 hash function. A new block is formed by combining the hash with its corresponding block from the logo. Finally, each element of the resulting block is inserted in the LSB of the corresponding element in the block. In the verification process the same process is repeated with the test image and the logo is generated only if the parameters used to generate the hash are unchanged. Localization of tampered image is provided. However its security depends on the security of the used keys. If the key is private then it demands for secure channel. Restoration capability is still not solved.

Byun and Lee [21] proposed a method to authenticate color images. The original color image is decomposed into its three color components red, green and blue. Blue component is used for hiding information as frequency response is much smaller than red and green [22]. Red and green components are used as authentication data by extracting the LSB from both to form a vector. Vector elements are permuted using a key. The hash function MD5 is calculated on the permuted vector to generate a sequence of 128 bits. The logo and hash is resized to form the same dimension as original image and hence exclusive OR operation is computed and encoded by public or private key.

In the verification procedure the LSB of blue component is extracted and decoded using corresponding secret key. Similarly, a hash is obtained from the red and green components for the insertion. Exclusive OR is applied, element by element, between the result from blue component and the hash. The result of this operation will be the inserted logo if and only if the checked image is identical to the original. The problems faced in this method are key security; restoration of damaged data is not possible as watermark is lost in case of

any changes. However, it can localize the modification and apt for strict color image authentication.

Fridrich and Goljan proposed a method [23, 24] in which the original image is converted to grey level and then is translated to interval [-127,128]. The result is then divided into 8×8 blocks and DCT transform is applied to MSB of pixels. The DCT coefficient of each block is arranged in a zigzag order using JPEG compression. The first 11 coefficient of each block is quantified by JPEG quantization and will reduce the quality by 50%. Quantified values are binary encoded on 64 bits and inserted to the LSB pixels of another block. This is the only method till now that allows restoration capability because it has significant information hidden. Localization is also possible as it is using 8×8 blocks as the authenticator. Quality of the restored image is lower than 50% but this is efficient for the user to understand the original content. Improvement is made to hide the 11 DCT coefficients in 2 LSB so that more significant information is achieved but have poor quality for watermarked image. This method is vulnerable to the whole image attacks that destroy the capacity of restoration such as setting all LSB bits to zeros.

2.3 Image Content

Content based characteristics are significant as it represent the image semantic content. It is a challenging problem as there is no exact definition to identify the image content.

One of the first efforts to exploit image content signature was proposed by Schneider and Chang [25]. The image histogram is used to represent the image content as it is believed that the histogram changes with content. Local spatial information of image intensities is not represented if the histogram of the whole image is considered. Hence, the original image is subdivided into blocks of equal dimension and the histogram of each block is considered. This approach provides localization capabilities. But has long signature hence long computational time. As an improvement, the dimensions of the blocks are varied according to the detail distribution within image. Small size blocks protected regions with finer details and bigger size for larger details. As a result, computational time is reduced along with preserving detection and localization capabilities but not restoration. Major drawbacks are there are techniques to alter the image content without changing the histogram and also robust against compression of small rates only.

Dittmann, Stabenau and Steinmetz [26] have proposed a method based on determining the image edges and transforming them into a characteristic code to generate the image content signature. The authors used the Canny detector to compute the edges. The result, a new image C, called edge characteristics, was then transformed into binary edge characteristics, called a binary characteristic shape, which was compressed with the variable coding length to produce a code ready to be signed by a digital signature algorithm. The authors did not detail the binary characteristics shape generation procedure. Therefore, the restoration capability of the algorithm could not be well evaluated. Detection and localization performances are very satisfying. However, likewise all other methods based on edges, this method suffers from the same problems mentioned above. Moreover, its robustness against compression was not well demonstrated.

El'arbi M. and Ben Amar C. proposed in [27] DCT domain based on neural networks. The watermark is constructed from the image to be watermarked. It consists of the average value of each 8 × 8 block of the image. Each average value of a block is inserted in another supporting block sufficiently distant from the protected block to prevent simultaneous deterioration of the image and the recovery data during local image tampering. Embedding is performed in the middle frequency coefficients of the DCT transform. In addition, a neural network is trained and used later to recover tampered regions of the image. Robust to JPEG compression and can also not only localize alterations but also recover them.

DWT has applications such as filtering, image compression [1]. Ye Xueyi et. al. [28] Robustness is an important index for digital watermarking. Most watermarking methods are robust to common attacks, but cannot resist geometric attacks. According to the Zernike moments' rotation invariance and scale invariance, a robust DWT-SVD watermarking algorithm is presented based on Zernike moment (ZM). In this scheme, the inscribed circle of the original image matrix is selected as the ZM calculation area, and the square of the inscribed circle is chosen to embed watermark. Firstly, the watermarking embedding area is conducted with 1-level DWT and the low frequency DWT coefficient is divided into non-overlapping blocks; SVD is applied to every block. Secondly, a bit of the watermark is embedded through slight modifications of the singular value (SV) matrix in each block. Finally, some selected ZM of the watermarked image are saved to detect and correct the possible geometric attacks. The simulation has proved that the proposed not just has good resistance to rotation, scaling attacks, and as well, kinds of common signal processing, and can achieve blind extraction.

2.4 Image Hashing

R. Venkatesan, S. M. Koon, M.H. Jakubowski and P. Moulin [29] proposed a method that utilizes a wavelet representation for images and new randomized processing strategies for hashing. The image is submitted to Haar Wavelet decomposition and the rectangles statistics are calculated and quantized using randomized rounding. At the decoding stage, the Reed Muller error correction code is used to generate the final hash bit. It is robust to some of the attacks such as rotation (2 degree), cropping (upto 10%), scaling (upto 10%), shifting (upto 5%), JPEG compression (upto 10%), median filtering. Algorithm is not key dependent and also the Collision Probability for unrelated image is less. The disadvantages are it does not support large rotations, computationally more complex and support minor geometric distortion.

C. De Roover, C. De Vleeschouwer, F. Lefebvre and B. Macq proposed a method in [30] using radial projection of image pixels for robust image hash. RASH (Radial hASH) considered moments of different order. It identifies the pair of equivalent or distinct images. The image is subjected to some operations and the Radial variance vector (RAV) is generated. It then computes the DCT of the RAV and hence the transformed RAV or TRAV. The first 40 coefficients are called RASH. The advantage of using such a system is the computational complexity is less, robust to filtering and geometric distortion and collision risk is very less. The disadvantages are collision avoidance property not sufficient for secure applications and RASH collision intractability is low.

Ashwin Swaminathan, Yinian Mao and Min Wu proposed in [31] that the image hash can be generated based on Fourier transform features and controlled randomization. Three steps are included in this process namely; pre-processing, feature generation and post-processing. The advantage is that the hash function is resilient to content preserved modification i.e. to moderate geometric and filtering distortion. It provides excellent security and robustness along with invariant to 2D affine transformation. The disadvantage of this approach is that some hashes are computed easily than others.

Shijun Xiang, Hyoung-Joong Kim and Jiwu Huang proposed a method [32] in which image histogram shape invariance to geometric distortions is exploited for image hashing. The image is passed through a low pass filter. During histogram extraction, the mean of the image along with the output of the low pass filter is manipulated for generating hash. The hash is protected using a key. The approach is robust to geometric attacks and cannot distinguish images with similar histograms but different contents.

Vishal Monga and M.K. Mihcak proposed [33] a method to compute image hash using non-negative matrix factorization. Pseudo random sub-image is selected from the image and NMF is applied and forms a secondary image. The NMF is applied to secondary image again and a NMF-NMF vector is formed. Hash bits are generated hence. It prevents intentional attacks of guessing and forgery. The drawback is that it cannot locate forged regions.

Zhenjun Tang, Shuozhong Wang, Xinpeng Zhang, Weimin Wei and Shengjun Su in [34] used global method using non-negative matrix factorization. The pixels are rearranged and converted to fixed pixel arrays. The NMF is applied on the secondary image to obtain feature bearing coefficient matrix and then coarsely quantized. So formed binary string is scrambled to form the hash bits. The approach is robust against Gaussian filtering, moderate noise contamination, JPEG compression, re-scaling and watermark embedding. Hashes of different images have very low collision probability. It has the advantage of detect tampering to local image areas. It is not capable to resist rotation attacks is a major drawback.

Fouad Khelifi and Jianmin Jiang proposed a method in [35] where robust and secure perceptual image hashing based on Virtual Watermark Detection. In order to produce the hash bit, the original image undergoes some pre-processing and the extracted coefficients along with the virtual watermark produced by passing the key through pseudo random noise generator is given to the watermark detector. Robustness is provided against normal image processing operation and geometric transformation. It also detects content changes in relatively large areas. Detection of small area forgery and localization of forged regions are not possible.

Yanqiang Lei, Yuangen Wang and Jiwu Huang in [36] produced robust image hashing using Radon Transform. Select the significant coefficients from Radon transform of image. Calculate the moment and DFT. Normalization and quantization of the result produces the hash bits. It is tolerant to image processing manipulations such as JPEG compression, geometric distortion, blur, addition of noise and enhancement. Detection of small area forgery is not possible.

Yan Zhao, Shuozhong Wang, Guorui Feng and Zhenjun Tang proposed a method in [37] based on rotation invariant Zernike moments. Firstly, Zernike moment transform of pre-processed image gives the extracted Zernike moment features for the hash. It is successfully secured using a key to produce the final hash. Robust features of the image is extracted and secure from content preserving attacks such as JPEG compression, additive noise, watermark embedding, scaling, brightness and color adjustments, gamma correction, Gaussian filtering and rotation. It has the advantage of detecting inserted objects.

3. Conclusion

The various techniques that are there in the area of image authentication are discussed. The classification is also provided to these techniques for generalization and better understandability. The importance and significance of the advanced techniques that provides ensuring results such as hashing, wavelets etc are highlighted over the traditional approaches. It also provides an insight of how the content of an image is preserved and identified even if the image is subjected to pre-processing operation. By the various image authentication techniques that are presented it is clear that it is having great application in area of medicinal, industry and military etc. In case of medicinal, documentation of image or military strict authentication is satisfactory as it is not subjected to any modifications and hence detection and localization are possible with acceptable restoration techniques are explained. The image content preserving modification such as rotation, scaling, geometric transformation etc give way to new challenges in the area of image authentication to provide robustness against content preserving manipulations. A flexible algorithm that allows the user to specify the list of desirable and malevolent manipulations does not exist yet. Therefore, this analysis provides a feasibility to identify the features that are best suited for a specific application.

References

[1] Antonini M, Barlaud M, Mathieu P, Daubechies I, "Image Coding using Wavelet Transform", IEEE Transaction on Image Processing, 1992, pp. 205-220.

[2] Harry A, "VDM specification of the MD4 message digest algorithm", Nat Phys Lab Teddington, UK, NPL DITC 1992.

[3] Matsuo T, Kaoru K,"On parallel hash functions based on block-ciphers", In: Proceedings of the IEICE transactions on fundamentals of electronics, communications and computer sciences, 2004, pp 67–74.

[4] Rivest R, "The MD4 message digest algorithm". RFC 1320, MIT and RSA Data Security, Inc, 1992.

[5] Rogier N and Chauvaud P, "MD2 is not secure without the checksum byte". Designs Codes Cryptogr 12(3):245–251, 1997.

[6] Skala V and Kucha M, "The hash function and the principle of duality". In: Proceedings of the computer graphics international, vol 200, pp 167–174, 2001.

[7] Stallings W, "SHA: the secure hash algorithm". Dr. Dobb's Journal of Software Tools 19(4):32–34, 1994.

[8] Xiaotie D, Chan L, Huafei Z, "A proposal for secure hash algorithm". In: Proceedings of the 1999 international workshop on cryptographic techniques and e-commerce, pp 254–258, 1999.

[9] Wolfgang RB and Delp EJ, "Techniques for watermarking digital imagery: further studies". In: Proceedings of the international conference on imaging science, systems, and technology, vol 1, pp 279–287, 1997.

[10] Walton S, "Information authentication for a slippery new age". Dr Dobb's Journal 20(4):18–26, 1995.

[11] Fridrich J, "Methods for tamper detection in digital images". In: Proceedings of the multimedia and security workshop at ACM multimedia, pp 29–33, 1999.

[12] Cox IJ, Linnartz MG, " Public watermarks and resistance to tampering". In: Proceedings of the ICIP'97, 1997.

[13] Yeung M, Mintzer F, "An invisible watermarking technique for image verification". In: Proceedings of the ICIP'97, 1997.

[14] Memon N, Fridrich, "Attack on a fragile watermarking scheme". In: Proceedings of the SPIE international conference on security and watermarking of multimedia contents, 2000.

[15] Memon N, Fridrich J, Goljan M, "Further attacks on Yeung–Mintzer watermarking scheme". In: Proceedings of the SPIE international conference on electronic imaging 2000, 2000.

[16] Holliman M, Memon N, " Counterfeiting attacks on oblivious block-wise independant invisible watermarking

schemes". IEEE Transaction on Image Processing 6:432 – 441, 1997.

[17] Fridrich J, Goljan M, Baldoza AC, "New fragile authentication/watermark for images". In: Proceedings of the ICIP, 2000.

[18] Wong PW, "A watermark for image integrity and ownership verification". In: Proceedings of the IS&T PIC conference,1998.

[19] Wong PW, "A public key watermark for image verification and authentication". In: Proceedings of the ICIP, 1998.

[20] Wong PW, Memon N, "Secret and public key image watermarking schemes for image authentication and ownership verification". IEEE Transaction on Image Processing 10:1593–1601, 2001.

[21] Byun SC, Lee IL, Shin TH, "A public key based watermarking for color image authentication". In: Proceedings of the IEEE international conference on multimedia and expo, vol 1, pp 593–600, 2002.

[22] Sayrol EJ, Cabanillas VS, "Optimum watermark detection for color images". In: Proceedings of the IEEE international conference on image processing, vol 2, pp 231–235, 1999.

[23] Fridrich J, Goljan M, "Protection of digital images using self embedding". In: Proceedings of the symposium on content security and data hiding in digital media, 1999.

[24] Fridrich J, Goljan M, "Images with self-correcting capabilities". In: Proceedings of the IEEE international conference on image processing, vol 3, pp 792–796, 1999.

[25] Schneider M, Chang S-F, "A robust content based digital signature for image authentication". In: Proceedings of the IEEE international conference on image processing, pp 227–230, 1996.

[26] Dittmann J, Steinmetz A, "Content-based digital signature for motion pictures authentication and content-fragile watermarking". In: Proceedings of the IEEE international conference on multimedia computing and systems, vol II, pp 209–213, 1999.

[27] El'arbi M and Ben Amar C, "Image Authentication algorithm with recovery capabilities based on neural networks in the DCT domain", IET Image Processing, vol 8. Issue 11, pp.619-626, 2014.

[28] Ye Xueyi, Deng Meng, Wang Yunlu and Zhang Jing, "A Robust DWT-SVD blind watermarking algorithm based on Zernike moments", Communications Security Conference, pp.1-6, 2014.

[29] R. Venkatesan, S. M. Koon, M.H. Jakubowski and P. Moulin, "Robust Image Hashing", In: Proceeding of International conference on Image processing, 2000, Vol. 3, pp. 664 – 666.

[30] C. De Roover, C. De Vleeschouwer, F. Lefebvre and B. Macq, "Robust Image hashing based on Radial variance of pixels", International Conference on Image Processing, 2005, pp. III-77-80.

[31] Ashwin Swaminathan, Yinian Mao and Min Wu, "Robust and Secure Image hashing",IEEE Transaction on Information Forensics and Security, 2006, Vol. 1, Issue 2, pp. 215-230.

[32] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations", In Proc. ACM Multimedia and Security Workshop, 2007, pp. 121–128.

[33] V. Monga and M. K. Mihcak, "Robust and secure image hashing via non-negative matrix factorizations", IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 376–390, Sep. 2007.

[34] Z. Tang, S.Wang,X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.

[35] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection", IEEE Transaction on Image Processing, vol. 19, no. 4, pp. 981–994, Apr. 2010.

[36] Y. Lei, Y.Wang, and J. Huang, "Robust image hash inRadon transform domain for authentication", Signal Processing: Image Commun., vol. 26, no. 6, pp. 280–288, 2011.

[37] Yan Zhao, Shuozhong Wang, Guorui Feng and Zhenjun Tang, "A Robust Image Hashing Method Based on Zernike Moments", Journal of Computational Information Systems, pp. 717-725, 2010.