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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Comparative Study of Image Authentication Techniques in Noisy Channels

Athira P R [1] , Geethu G [2] ,Nithya Das K H [3] , Shima M S [4] , Jumana Nahas [5]

U.G. Student, Department of Computer Engineering, Model Engineering College, Ernakulam, Kerala, India[1]

U.G. Student, Department of Computer Engineering, Model Engineering College, Ernakulam, Kerala, India[2]

U.G. Student, Department of Computer Engineering, Model Engineering College, Ernakulam, Kerala, India[3]

U.G. Student, Department of Computer Engineering, Model Engineering College, Ernakulam, Kerala,India[4]

Assistant Professor, Department of Computer Engineering, Model Engineering College, Ernakulam, Kerala, India[5]

ABSTRACT: Authentication plays an important role in protecting data against unauthorized access. Authentication of image is very different from standard data authentication. Image authentication has several applications in various fields like medical, surveillance, military. A wide variety of techniques have been used for image authentication which are basically divided into Hash based and Watermark based. This paper presents a survey on various image authentication techniques. We also give a comparison study of various image authentication techniques and the algorithms used in those techniques.

KEYWORDS: Authentication, Watermarking and Hash based techniques, AMAC Algorithms.

I. INTRODUCTION

Image authentication techniques have recently gained great attention due to is importance for a large number of multimedia applications. Digital information revolution has brought about many advantages and new issues with the ease of editing and, unauthorized manipulation of digital image has become an important concern. It is often desirable to determine if a digital image has been modified in any way from the time of its transmission, including manipulations such as cropping. Different classifications exist for image authentication techniques according to their construction and functionality. Image Authentication techniques enable the recipients to verify the integrity of the received image. The existing image authentication techniques are watermarking based authentication, cryptography based authentication, and robust image hashing authentication.Digital watermarking is the science and art of embedding copyright information called watermarks in the files. Cryptography based authentication includes encryption and decryption to transfer documents or images. Robust image hashing is based on rotation-invariant moments (ORIMs) that can effectively catch important information in an image.

>>Why image authentication?
With rise in the use of cell phones, mobile cameras and other digital photography devices, the cases of doctored and altered digital photography's has also increased. Photoshop and other photo editing software's has made tampering easier while making it difficult for individuals and examiners to recognise the doctored digital photograph, therefore increasing the need for image authentication. Image authentication is needed to be able to determine whether an image has been altered or not .To be able to integrate authentication data with host image rather than as a separate data file and the embedded authentication data be invisible under normal viewing conditions in order to locate alteration made on the image. Either the photography device or author of the image can provide undisputable proof of the origin of image .Epson and Kodak have produced

DOI: 10.15680/IJIRCCE.2017. 0503314

cameras with security features such as the Epson PhotoPC 3000Z and the Kodak DC-290 which are irremovable features added to the pictures. These features distorted the original image, making them unacceptable for some applications such as forensic evidence in court. Thus image authentication is essential in many important applications.

>>Authentication requirements

1. Sensitivity.
   The system must be able to detect manipulations in the content of the image.
2. Robustness.
   The authentication system must be able to tolerate content preserving manipulations.
3. Localization.
   System must be able to localise the alterations in the image.
4. Recovery.
   System must be able to recover the tampered parts of the image.
5. Security.
   The authentication system must be able to protect the authentication data.

>>Challenges of image authentication?

There are a number of techniques to authenticate an image. An image authentication technique must be efficient, fast and must contain error correction techniques to reconstruct an image. If the authentication technique can detect the places where the error is seemed, then it is very easily to recover the image. Image authentication actually verifies the authenticity of the image. Also there is a chance to occur changes in the image by unauthenticated third parties, due to noise, image compression, filtering etc. So the proposed authentication technique must provide high robustness against image compression, noise and filtering. The image authentication technique must also provide fragility. Fragility of an image authentication technique is an indication of discrimination capability .An image authentication technique not only detect the forgery attacks but also detect the content changes. The defined algorithm also must capable of providing efficient and fast image authentication method.The above mentioned are the challenges in image authentication techniques.

>>Applications of image authentication?

The use of image authentication techniques grows in day to day life. Manuscripts and voice are used as the main method for communication in traditional life. But now the information including data, images and videos can travel miles within milliseconds. When the communications are takes place through unsecured channels, there may chance to occur volatile attacks and also create a risk factor in areas such as militaries, medical fields, crime files, researches etc. Image authentication actually provides image security. In medical field there have a huge importance for the image authentication, a small change in the image can cause a big fault. Military services requires at most protection because it is all about the security of the country. Communication via images is vital part in military service to detect the faults. So image authentication become an important technique in military service.

II. RELATED WORK

*** Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain.**

This technique proposes image authentication in DCT domain based on neural networks. The authentication is done by creating watermark from the input image. Before constructing watermark it first divide the image into equal blocks of size 8*8 .Then transform each block to the frequency domain by using Discrete Cosine Transform. Then calculates the average value of each block and finally convert it to the binary to obtain the watermark. It uses two blocks, supporting block(SB) and protecting block(PB).Supporting block is used to embed the average value of each block. The average value of each block is stored in protected block. Then transform it to the DCT domain. The watermarked image is obtained by applying inverse discrete cosine transform.

Here the neural network is used to recover the image from the average value. If 8*8 block is altered, then we extract the average value from support block and give it as the input to the neural network. Thus the neural network can reproduce the image before alteration. To extract the image from watermark, first divide the image into blocks and find supporting blocks, finally apply DCT .So we can extract DCT through this way.

This technique provide high quality image and tt can successfully localise the alteration and recover them.

***Scalable fragile watermarking for image authentication**

This technique is suitable for authentication of scalable JPEG2000 compressed images. A fragile watermarking technique is used to authenticate image. Fragile watermarking protects higher layer and quality layer from tampering .In first step image is quantized. Each coefficient of image assigned an index i, which is used to generate pseudo random numbers. For each selected coefficient there is a watermark element is generated corresponding to it and then embedded using quantise and replace embedding. Each watermark bit carefully constructed from the corresponding image coefficients, to ensure high levels of scalability and security against attack. It uses mainly two algorithms ‘embed’ and ‘detect’. The embed algorithm is used to embed the watermark to the image and detect algorithm is used to detect the missing watermarked bits and to find it by adjusting the other watermarked bits.

Unlike the other semi-fragile authentication watermarks, this technique generates an efficient image features using layers above the lowest authenticable bit rate. This prevents an attacker from modifying higher layers. It provide tamper localization.

***Watermarking Algorithm for Authentication and Self-Recovery of Tampered Images Using DWT**

Currently there are various techniques for image authentication. However, most of these techniques can only protect a region of interest within digital image, the alteration of certain regions that are not protected. This technique proposes a digital watermarking algorithm, which consist of two stages; the first one is protection. In this stage, digital image that is performed by half toning , Daubechies DWT, and QIM methods; the second one is used for authentication, detection and self-recovery of tampered regions by using methods like IDWT, inverse half toning and median filtering. In the first stage, three watermarks are generated from the original image, where they are embedded into DWT sub-bands of the original image using Daubechies wavelet. In the Authentication and self-recovery stage, the authentication matrix and the matrix key are extracted; later, the self-recovery matrix is extracted using the matrix key. A post-processing is done in the self-recovery matrix to generate the approximation matrix of the original image. Finally, to generate the recovered image, it is necessary to use the authentication matrix, the approximation matrix of the original image and the tampered image.

***A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption Technique for Security and Authentication of Digital Images**

This technique proposes a hybrid image cryptographic encryption and digital watermarking technique for the encryption and authentication of digital image content. The image encryption was done on the RGB channels and the spatial watermarking applied to the RGB colour bands of the digital image. This rendered watermark is not visible .The invisibility of the watermark will make it difficult for detection and hacking. The digital watermarking technique was engaged to authenticate the image and detect modifications to the watermarked image. This technique contain two phases. First one is image cryptographic phase and second is watermarking. First phase uses visual image encryption technique as well as pixel displacement. There is no pixel expansion during the encryption process but there is a change in pixel position. There is a change in pixel values after the application of the watermark but during the decryption phase, the watermark was removed and the pixel was restored. This approach is effective because the watermark can be extracted and the image can easily be recovered without pixel expansion or data loss. This proposed approach is suitable for effective watermark authentication and applications in which full recovery of image content is necessary after deciphering of the ciphered image and removal of watermarks. This technique can be applied in applications such as medical images stored in the cloud, military communication networks where authentication of visuals is crucial for example, Unmanned Aerial vehicles, video surveillance systems, satellite communication systems etc.

***Image Authentication scheme using Digital Signature and Digital Watermarking**

This method divides the image into 16x16 pixels and generates N random matrices using secret key with entries uniformly distributed in the interval [0, 1].Then random smooth patterns are obtained by applying a low-pass filter repeatedly. The mean is subtracted from each pattern and the image block B is projected on each pattern and the absolute value is compared with a threshold to obtain N bits which are content dependent digital signature that is embed back into original image as watermark. In this method joint DWT-DCT scheme is used. After the application of a 3-level DWT on the host image, the extracted digital signature, that is the watermark, is scrambled by Arnold cat map and then embedded in the coefficient sets of the transformed host image. The PN-sequences of the watermark are then embedded into the middle frequencies coefficients of DCT transform, applied on each selected DWT sub-band. In the extraction process at receiver side, the watermarked image initially undergoes pre-filtering by combination of sharpening and Laplacian of Guassian filters, followed by the same procedure as embedding process to extract the DCT middle frequencies of each sub-band. Finally, the watermarked bits are calculated by the correlation between mid-band coefficients and PN-sequences.

***Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation**

This method is a hybrid watermarking scheme that uses the important features of DWT,DCT and SVD. During watermark embedding, on the host image, single level DWT is applied followed by DCT on the lower right frequencies. The DCT frequencies are mapped to 4 quadrants by zigzag scanning and SVD is applied to each quadrant. On the watermark image, DWT is applied followed by DCT on lower right frequencies and SVD is applied. The two output from SVD along with a key is embedded into image. The resultant watermarked image is obtained after applying IDCT and IDWT.

In the watermark extraction process, DWT is applied to attack watermarked image followed by DCT. The DCT coefficients which are mapped into 4 quadrants by zigzag scanning, along with a key is used to extract singular values from each quadrants from which the SVD matrix is reconstructed. The watermarked image is obtained by applying UDCT followed by IDWT on each quadrant.

***Secure and robust two phase image authentication**

This technique is constructed based on combination of hard and soft authentication using twoexisting techniques such as approximate message authentication codes (AMACs). The AMACs techniques combine error-correcting codes with cryptographic primitives such as message authentication codes and symmetric encryption algorithms. The message authentication codes are used for hard authentication. The 2-phase image authentication scheme verifies the authenticity of an image in two phases. In the first phase, low frequency elements of the image in a transform domain are subjected while some higher frequency elements are left to the second phase if the first phase succeeds. The results shows that this technique shows high discriminating capability and can detect meaningful forgery attacks on images while preserving the robustness.

>>Security Parameters

1. Confidentiality:

This ensures that the data is visible only to authorized users. The AES encryption algorithm promises to achieve data confidentiality in this system.

2. Authentication:

Authentication is the process of verifying the identity of user. It provides authentication by using two algorithms AMAC1 and AMAC2.

3. Integrity:

Integrity ensures that during transmission, received image has not been manipulated. It provides integrity by using the algorithms.

III. Proposed Algorithm

Algorithm1:Two Phase Tag Generation

```
Input: Image I, Image dimensions (in terms of image blocks): M, N, input parameters of Algorithm 1, input
parameters of Algorithm 2

1. Start procedure for 2-phhhasse tag generation
2. Normalize image I using bilinear interpolation and map into a square fixed size image
3. Apply low-pass Gaussian filter to create the pre-processed image J
4. Divide J into non overlapping square blocks
5. For each block, do steps i to iii
        i.   Apply 2-dimensional DCT
        ii.  Quantize DC elements
        iii. Quantize AC elements
6. Concatenate quantized DCs together to form q-bit message for hard authentication part corresponding to
AMAC1.Returned value is stored as tag1
7. Concatenate quantized ACs together to form q-bit message for hard authentication part corresponding to
AMAC2.Returned value is stored ass tag2
8. Concatenate tag1 and tag2 to get final tag
9. Return final tag
10. Stop
```

Algorithm 2.1: AMAC1

```
1. Start procedure AMAC1- Tag(k1,k2,x) where k1, k2 are used in AMAC1, k1 & k2 : Shared secret keys, x-
m bit message, $\delta$ – Error correction Capability
2. Apply Encoding function to message ‘x’ and $\delta$ to create parity check which is appended to the message.
3. Tag is generated from MAC function
        T <- MAC(k,x)
4. Cipher text C is generated using Encryption algorithm
        C <- Ek2(pc)
   Where Ek2 is the Encryption Algorithm
5. Tag is generated by concatenation of C and $T_1$
        Tag <- C II $T_1$
6. ReturnGenerated Tag Value
7. End Procedure
```

Algorithm 2.2: AMAC2

Input: shared secret key k generated by Kg, initial value IV , m-bit message x, block size c, number of blocks t, approximate correctness parameters P and δ approximate security parameter γ. The messages having difference up to δ bits are assumed identical by the user. u ∈ { 0,1}k , π is a permutation function ,and L ∈ { 0,1}m. ρ is used to select i1....i t1 randomly from {1....t} tcr denotes a target collision resistant hash function, is a type of Second Preimage Resistance, and is implied by Collision Resistance.

```
1: Compute t1 = m ⌈ 2/ δ ⌉ and t2 = ⌈-10 log(1 - P)⌉
2: Start procedure for AMAC2 - Tag(k, x)
```

```
        3: Apply PRF(k) with initial value IV .Divide the random number to 4 parts. Beginning and ending part will
        be {0,1}m and π and  ρ.
        4: Perform L⊕x and given to π.Then divide the input x to blocks ,ie {x1,x2....,xt}
        5: For i = 1 to t2 do steps 6 to 7
        6: Move elements from xi(1) to xi(t1) to Ni
        7: Apply target collision resistance hash function on each Ni and store in Ti.
        8: Tag is obtained by concatenating initial value and Ti's
   9: Return tag
        10: End procedure
```

Algorithm 3 :Gaussian Filter

Input: Image,kernal size z
Output: Image (blurred image)
gaussianBlur(image, z)

```
        1. Choose the kernal size for 2D image.
        2. For each kernal do 2 to 8.
        3. To calculate the weight matrix, choose a value for σ.
        4. Calculate the kernal by using σ by the equation
```

$$G=[1/(2Л\sigma^2)]\ e^{-(x^{\wedge}2+y^{\wedge}2)/(2\sigma^{\wedge}2)}$$

```
        5. Find the sum of all values in the kernal
        6. Divide the each point by the obtained sum, and make a new kernal with new values.
        7. Multiply the weighted value with corresponding kernal value to obtain the new value.
        8. Update the value in centre point of weighed matrix.
        9. Return image.
```

IV. Comparison

Techniques	Advantages	Disadvantages
Watermarking Algorithm for Authentication and Self-Recovery of Tampered Images Using DWT	It provides robustness to JPEG compression, the tamper detection and the recovery capability of the tampered regions. Quality of the recovered image is above 32 dB of PSNR	It takes more pre-processing time.
A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption Technique for Security and Authentication of Digital Images	It can detect temperament or malicious attack.	Complex methods needed
Secure and Robust two phase image authentication	The error-correcting codes provide certain degree of robustness in authentication.	Implementation of two algorithms is difficult.

Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain.	This technique can efficiently recover the image by using neural network. It can successfully localise the alteration.	It includes neural network to localise the alteration, So it may be little bit complex in implementation.
Scalable fragile watermarking for image authentication	This method try to protect the quality layer and higher layer from alteration. Also it provide tamper localisation.	Very difficult to implement. It is most suitable for authentication of scalable JPEG2000 compressed images.
image Authentication scheme using Digital Signature and Digital Watermarking	Efficient method if the Internet is in congestion. An additional bandwidth is not necessary for the digital signature since it is embedded in the host image.	More computations.
Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation	Improved watermarking performance.	Applied only to grayscale images in this paper.

V.CONCLUSION AND FUTURE WORK

In this paper, we presented a detailed comparison of latest image authentication techniques. Each technique has its own method for authentication purpose. Neural networks are successful in tamper localization even though it is complex in implementation. Scalable fragile image authentication technique proposes a new method to increase the efficiency of authentication. Authentication of image using hybrid cryptographic and spatial encryption technique can be applied in crucial applications. Image authentication using a combination of DCT, DWT and SVD improves the watermarking performance. On comparing, all of these techniques image authentication in two phases gives more robust and secure result.

REFERENCES

1. Maher El'arbi, Chokri Ben Amar,"Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain", IET Image Processing
2. Angela Piper, Reihaneh Safavi-Naini ,"Scalable fragile watermarking for image authentication", IET Image Processing.
3. Javier Molina-Garcia, Rogelio Reyes-Reyes, Volodymyr Ponomaryov, Clara Cruz-Ramos,"Watermarking Algorithm for Authentication and Self-Recovery of Tampered Images Using DW", IEEE 2016
4. Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu , Sophie Gire ,Jojo M. Eghan , Nii Narku Quaynor, "A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption Technique for Security and Authentication of Digital Images",2015 17th UKSIM-AMSS International Conference on Modelling and Simulation
5. Seyed Mohammad Mousavi,"Image Authentication scheme using Digital Signature and Digital Watermarking", IJCEM International Journal of Computational Engineering & Management, Vol. 16 Issue 3, May 2013
6. Mohammad Ibrahim Khan, Md. Maklachur Rahman and Md. Iqbal Hasan Sarker,"Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation"
7. S. Amir Hossein Tabatabaei, Obaid Ur-Rehman, Natasa Zivic and Christoph Ruland,"Secure and robust two phase image authentication", 1520-9210 (c) 2015 IEEE