Image Authentication using Modified DCT-LSB Technique

Vindhya Gautam[1], Kalpana Tiwari[2]

[1]M.Tech Scholar, [2]Assistant Professor
Department of Electronics and Communication, VITS, Satna,

***Abstract*: Image authentication is the process of proving image identity and authenticity. Digital images are increasingly transmitted over non-secure channels such as the Internet. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Nowadays image authentication techniques have recently gained great attention due to its importance of multimedia applications. The traditional cryptographic hash functions, such as MD5 and SHA-1 are used for authentication. However, these hash functions are not suitable for image authentication. Because they are so sensitive that even one bit change of the input data will lead to a significant change of the output hash. Besides, image authentication system requires the main content sensitive. In order to make up for the disadvantage of the traditional cryptographic hash functions in image authentication.**

***Keywords*: Image authentication, image identity, Digital images, authentication techniques**

1. Introduction

Image Authentication

We are living in a world where seeing is no longer believing. The increasing popularity of digital cameras, scanners and camera-equipped cellular phones makes it easy to acquire digital images. These images spread widely through various channels, such the Internet and Wireless networks. They can be manipulated and forged quickly and inexpensively with the help of sophisticated photo-editing software packages on powerful computers which have become affordable and widely available. As a result, a digital image no longer holds the unique stature as a definitive recording of scenes, and we can no longer take the integrity or authenticity of it for granted. Therefore, image authentication has become an important issue to ensure the trustworthiness of digital images in sensitive application areas such as government, finance and health care.

Image authentication is the process of verifying the authenticity and integrity of an image. Integrity means the state or quality of being complete, unchanged from its source, and not maliciously modified. This definition of integrity is synonymous with the term of authenticity. Authenticity is defined as "the quality or condition of being authentic, trustworthy, or genuine". Authentic means "having a claimed and verifiable origin or authorship; not counterfeit or copied". However, when used together with integrity in this thesis, authenticity is restricted in the meaning of quality of being authentic that verified entity is indeed the one claimed to be.

Error Resilient Image Authentication

Image transmission over lossy channels is usually affected by transmission errors due to environmental noises, fading, multi-path transmission and Doppler frequency shift in wireless channel, or packet loss due to congestion in packet-switched network. Normally errors under a certain level in images would be tolerable and acceptable. Therefore, it is desirable to check image authenticity and integrity even if there are some uncorrectable but acceptable errors. For example, in electronic commerce over mobile devices, it is important for recipients to ensure that the received product photo is not maliciously modified. That is, image authentication should be robust to acceptable transmission errors besides other acceptable image manipulations such as smoothing, brightness adjusting, compressing or noises, and be sensitive to malicious content modifications such as object addition, removal, or position modification.

Passive Image Authentication based on Image Quality Inconsistencies

A requirement of active image authentication is that a signature or watermark must be generated and attached to the image. However, at present the overwhelming majority of images do not contain digital watermark or signature. Therefore, in the absence of widespread adoption of digital watermark or signature, there is a strong need for developing techniques that can help us make statements about the integrity and authenticity of digital images. Passive image authentication is a class of authentication techniques that uses the image itself for assessing the authenticity of the image, without any active authentication code of the original image. Therefore, the second problem this paper focuses on is how to passively authenticate images without any active side information from signature or watermark.

2. Review of Literature

Zhicheng Ni et al. proposed In this paper, they first point out that this technique has suffered from the annoying salt-and-pepper noise caused by using modulo-256 addition to prevent overflow/underflow. **Chun-Shien Lu et al.** suggested that the novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. **Chun-Shien Lu et al.** proposes a new digital signature scheme which makes use of an image's contents (in the wavelet transform domain) to construct a structural digital signature (SDS) for image authentication. The characteristic of the SDS is that it can tolerate content-preserving modifications while detecting content-changing

modifications. Many incidental manipulations, which were detected as malicious modifications in the previous digital signature verification or fragile watermarking schemes, can be bypassed in the proposed scheme. Performance analysis is conducted and experimental results show that the new scheme is indeed superb for image authentication.

Elisabet Pérez-Cabré et al. proposed that the photon-counting imaging is integrated with optical encryption for information authentication. An image is double random-phase encrypted, and a photon-limited encrypted image is obtained. **Chien-Chang Chen and Cheng-Shian Lin** suggested that a robust image authentication approach that distinguishes malicious attacks from JPEG lossy compression. The authentication procedure calculates the relationships between important DCT coefficients in each pair of DCT blocks and predefined thresholds to form the authentication message, and then embeds the encryption of the authenticated message into other DCT coefficients. The message calculation and embedding procedure are based on two proposed quantization properties that always exist under different JPEG quantization tables. Therefore, the proposed image authentication approach can tolerate JPEG compression efficiently. Experimental results demonstrate the effectiveness of the proposed image authentication approach. **Christian Rey et al.** proposed that the digital image manipulation software is now readily available on personal computers. It is therefore very simple to tamper with any image and make it available to others. Insuring digital image integrity has therefore become a major issue. Water marking has become a popular technique for copyright enforcement and image authentication. The aim of this paper is to present an overview of emerging techniques for detecting whether image tampering has taken place. Compared to the techniques and protocols for security usually employed to perform this task, the majority of the proposed methods based on watermarking, place a particular emphasis on the notion of content authentication rather than strict integrity. In this paper, they introduce the notion of image content authentication and the features required to design an effective authentication scheme. They present some algorithms, and introduce frequently used key techniques. **Farid Ahmed and Ira S. Moskowitz propsed** that a correlation-based digital watermarking technique for robust image pattern authentication. They hide a phase-based signature of the image back into its Fourier magnitude spectrum in the embedding stage. The detector computes the Fourier transform of the watermarked image and extracts the embedded signature. Authentication performance is measured by a correlation test of the extracted signature and the signature computed from the watermarked image. The quality of the watermarked image is obtained from the peak signal-to noise ratio metric. They also furnish simulation results to show the robustness of our approach to typical image processing as found in JPEG compression. **Tetsuji Takada and Hideki Koike** proposed that there is a trade-off between security and usability in user authentication for mobile phones. Since such devices have a poor input interfaces, 4-digit number passwords are widely used at present. Therefore, a more secure and user friendly authentication is needed. This paper proposes a novel authentication method called "A-waste-E". The system uses image passwords. It, moreover, integrates image registration and notification interfaces. Image registration enables users to use their favorite image instead of a text password. Notification gives users a trigger to take action against a threat when it happens. A waste-E is implemented so that it has a higher usability even when it is used through a mobile phone. **Franco Bartolini** proposed that in automatic video surveillance (VS) systems, the issue of authenticating the video content is of primary importance. Given the ease with which digital images and videos can be manipulated, practically they do not have any value as legal proofs, if the possibility of authenticating their content is not provided. In this paper, the problem of authenticating video surveillance image sequences is considered. After an introduction motivating the need for a watermarking- based authentication of VS sequences, a brief survey of the main watermarking-based authentication techniques is presented and the requirements that an authentication algorithm should satisfy for VS applications are discussed. A novel algorithm which is suitable for VS visual data authentication is also presented and the results obtained by applying it to test data are discussed. **Shui-Hua Han and Chao-Hsien Chu** suggested today's global digital environment, the Internet is readily accessible anytime from everywhere, so does the digital image manipulation software; thus, digital data is easy to be tampered without notice. Under this circumstance, integrity verification has become an important issue in the digital world. The aim of this paper is to present an in-depth review and analysis on the methods of detecting image tampering. They introduce the notion of content-based image authentication and the features required to design an effective authentication scheme. They review major algorithms and frequently used security mechanisms found in the open literature. They also analyze and discuss the performance tradeoffs and related security issues among existing technologies.

3. Research Methodology By defining the general requirements that are essential for any authentication system. These requirements are: **Sensitivity:** The authentication system must be able to detect any content modification or manipulation. For strict authentication algorithms, detection of any manipulation is required and not only content modification.

Robustness: Also called tolerance. The authentication system must tolerate content preserving manipulations. This property is valid just for algorithms that provide a selective authentication service.

Localization: The authentication system must be able to locate the image regions that have been altered.

Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered. **Security:** The authentication system must have the capacity to protect the authentication data against any falsification attempts.

Portability: The authentication system must be able to carry the signature with the protected image during any transmission, storage or processing operation

Complexity: The authentication system must use real-time implemented algorithms that are neither complex nor slow.

Strict image authentication

Strict image authentication methods do not tolerate any changes in the image data. These methods can be further

separated in two groups according to the techniques that are used: methods based on conventional cryptography and methods that use fragile watermarking.

4. Result and Discussion

4.1 Implementation in MATLAB

MATLAB supports developing applications with graphical user interface (GUI) features. MATLAB includes GUIDE (GUI development environment) for graphically designing GUIs.

4.2 Execution in MATLAB

Fig 4.1: Main GUI that is the first layout develop in MATLAB

Fig 4.2: Image Authentication using Text Image

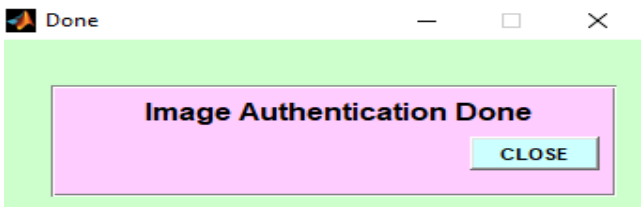

Fig 4.3: Image Authentication done

Fig 4.4: Justify image Authentication

Fig 4.5: Justify Image Authentication

Image authentication is the process of proving image identity and authenticity. Digital images are increasingly transmitted over non-secure channels such as the Internet. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Nowadays image authentication techniques have recently gained great attention due to its importance of multimedia applications. The traditional cryptographic hash functions, such as MD and SHA-1 are used for authentication. However, these hash functions are not suitable for image authentication. Because they are so sensitive that even one bit change of the input data will lead to a significant change of the output hash. Besides, image authentication system requires the main content sensitive. In order to make up for the disadvantage of the traditional cryptographic hash functions in image authentication, robust image hashing was first introduced which provide good ROC performance, low collision probability.

5. Conclusion Future scope

User typically creates unforgettable passwords that area unit straightforward for attackers to guess, however robust system assigned passwords area unit tough for users to recollect. Authentication done mistreatment text-based arcanum is vulnerable to several attacks. Users typically produce passwords that area unit straightforward to hit the books giving a chance for attackers to guess it. System generated passwords area unit secure, robust however tough for users to recollect. Despite the vulnerabilities, it's the natural tendency of the users to travel for brief passwords for easy remembrance and conjointly lack of awareness concerning however attackers tend to attacks. sadly, these passwords area unit broken pitilessly by intruders by many straightforward means that like masquerading, overhang dropping and alternative means that like wordbook attacks, shoulder aquatics attacks, social engineering attacks. To handle these authentication issues, a brand new various authentication

technique are planned that uses pictures as passwords. Image based mostly Authentication conjointly referred as Graphical User Authentication is associate authentication system that works by having the user choose from pictures in an exceedingly specific order conferred in MATLAB Graphical interface (GUI).

References

[1] Zhicheng Ni et al. Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication,, VOL. 18, NO. 4, APRIL 2008, pp .497-509
[2] Chun-Shien Lu et al. Multipurpose Watermarking for Image Authentication and Protection, VOL. 10, NO. 10, OCTOBER 2001, pp. 1579-1592
[3] Chun-Shien Lu et al. Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, Vol. 5, No. 2, June 2003, pp. 161-173
[4] Myungjin Cho et al. Information authentication using photon-counting double-random-phase encrypted images, Vol. 36, No. 1 / January 1, 2011, pp. 22-24
[5] Chien-Chang Chen and Cheng-Shian Lin toward a Robust Image Authentication Method Surviving JPEG Lossy Compression, (2007), pp. 511-524
[6] Christian Rey and Jean-Luc Dugelay, A Survey of Watermarking Algorithms for Image Authentication, June 2002, pp. 613–621
[7] Farid Ahmed and Ira S. Moskowitz, Correlation-based watermarking method for image authentication applications, Vol. 43 No. 8, August 2004, pp. 1-6
[8] Tetsuji TAKADA et al. Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images
[9] Franco Bartolini et al. Image Authentication Techniques for Surveillance Applications, VOL. 89, NO. 10, OCTOBER 2001, pp. 1403-1418
[10] Shui-Hua Han · Chao-Hsien Chu, Content-based image authentication: current status, issues, and challenges, (2010) 9: pp. 19–32
[11] Adil Haouzia & Rita Noumeir, Methods for image authentication: a survey, (2008) 39: pp. 1–46
[12] Chang-Chou Lin, Wen-Hsiang Tsai, Secret image sharing with steganography and authentication, (2004) pp. 405–414
[13] Ching-Yung Lin et al. A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation, VOL. 11, NO. 2, February 2001, pp. 153-168