Image Authentication using semi-fragile watermarking

[1]Pushpanjali Bharati, [2]Manoj kumar gautam, [3]Swatantra Tiwari

Abstract **Image authentication techniques have recently gained great attention due to its importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as the Internet. Therefore, military, medical and quality control images must be protected against attempts to manipulate them; such manipulations could tamper the decisions based on these images. To protect the authenticity of multimedia images, several approaches have been proposed. These approaches include conventional cryptography, fragile and semi-fragile watermarking and digital signatures that are based on the image content. Image authentication identifies the ownership of digital image using Digital Watermarking. The Digital watermarking concept is used to hide and detect information from image. It is the best way to copyright protection of the user. By the use of digital watermarking, user can blame on faker for ownership.**

Keywords**: Digital images, Image authentication, multimedia images, watermarking**

1. Introduction

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. 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.

Here this propose error resilient image authentication techniques which can authenticate images correctly even if there uncorrectable transmission errors. An image feature distance measure is also proposed to improve image authentication system performance. The proposed perceptual distance measure is quite general that it is able to be used in many content-based authentication schemes which use features containing spatial information, such as edge, block DCT coefficients based features, highly compressed version of the original image, block intensity histogram. The proposed perceptual distance measure, when used as the feature distance function in image authenticity verification stage, will improve the system discrimination ability. Many acceptable manipulations, which were detected as malicious modifications in the previous schemes, can be bypassed in the proposed scheme. The proposed feature distance measure can be incorporated in a generic semi-fragile image authentication framework to make it able to distinguish images distorted by transmission errors from maliciously tampered ones.

Cryptography and digital signature techniques are beyond the scope of this thesis, since they have been well studied in the data security area, and are not the key techniques that make our research different from others. The authentication techniques proposed in this thesis can produce good robustness against transmission errors and some acceptable manipulations, and can be sensitive to malicious modifications. Moreover, the perceptual distance measure proposed for image authentication would improve the system performance of content-based image authentication schemes.

2. Active Image Authentication

Active image authentication uses a known authentication code during image acquiring or sending, which is embedded into the image or sent along with it for assessing its authenticity or integrity at receiver side. It is different from classic data authentication. Robustness and sensitivity are the two main requirements of active image authentication. The main approaches of active image authentication are based on digital watermarking and digital signatures.

3. Content-based image authentication or selective authentication

We defined a content modification as an object appearance or disappearance, a modification to an object position, or changes to texture, color or edges. We have also listed the image processing operations that preserve the image content. Thus, lot of applications that base their decisions on images need authentication methods that can tolerate content preserving manipulations while at the same time detect any manipulation that change the image content. This leads to new watermarking methods known as semi fragile watermarking, and to new approaches known as content-based signatures. In this section we will present and compare semi-fragile techniques and content-based signatures approaches that provide selective image authentication service.

3.1 Semi-fragile watermarking

Robust watermarking is designed to resist all attempts to destroy the watermark. Its main application includes the intellectual property protection and owner identification. The robustness of the embedded watermark is crucial to resist any intentional and even unintentional manipulation. The goal of these techniques is not the verification of the image authenticity, but rather the verification of their origins. Conversely, fragile watermarking, is designed to easily destroy the embedded watermark following any kind of manipulations of the protected image. It is useful for applications where strict authentication is needed, that is where the main objective is to determine whether the image has been modified or not, with the possibility of locating and reconstructing image regions that have been tampered. On the other hand, semi-fragile watermarking combines characteristics of fragile and robust watermarking techniques.

Basically, the idea of semi-fragile watermarking is to insert a watermark 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. For image authentication purposes watermarking algorithms should be invisible. Visible watermarking algorithms are applied for on-line content distribution, transaction tracking or owner identification. The procedures of generating a watermark and embedding it into the image can be dependent on a private or public, symmetric or asymmetric, key system in order to increase the overall system security. This is a trade-off between security and computational time. Generally, symmetric key systems are less secure than asymmetric ones, and asymmetric key systems consume more resources and consequently need more computing time.

The general schema for semi-fragile watermarking methods is shown in Fig. 3.1. The watermark is computed from the result of an image-processing algorithm applied on the image pixels. The computation of the watermark varies as different image processing algorithms can be used. A secret key K1 can be used to extract specific information from the image. In order to generate the watermark, the extracted image information is often combined with a binary logo using another secret key K2. Usually, the generated watermark is then inserted in a set of frequency coefficients that are in the middle range. The set of coefficients where the watermark is inserted may be determined with the help of a secret key K3. The computed watermark may be encrypted with a key K4. Similarly, the general verification schema is shown in Fig. 3.1b. The secret keys must be known to the receiver, as well. The receiver uses the same key to determine the set of pixels where the watermark is dissimulated in order to extract it. Also, the receiver uses the same algorithms to compute the watermark from the received image and then compares the computed watermark with the dissimulated one to decide whether the image is authentic or not.

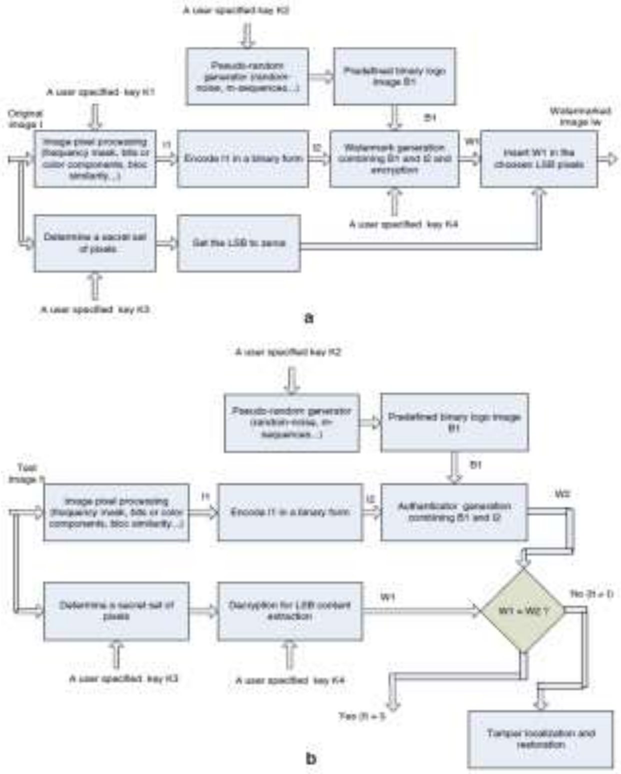

A user specified key K2
Pseudo-random generator (random-noise, m-sequences...)
Predefined binary logo image B1
A user specified key K1
Original image I
Image pixel processing (frequency mask, bits or color components, bloc similarity...)
I1
Encode I1 in a binary form
I2
B1
Watermark generation combining B1 and I2 and encryption
W1
Insert W1 in the chosen LSB pixels
Watermarked image Iw
Determine a secret set of pixels
Set the LSB to zero
A user specified key K4
A user specified key K3
a
A user specified key K2
Pseudo-random generator (random-noise, m-sequences...)
Predefined binary logo image B1
B1
Test image It
Image pixel processing (frequency mask, bits or color components, bloc similarity...)
I1
Encode I1 in a binary form
I2
Authenticator generation combining B1 and I2
W2
Determine a secret set of pixels
Decryption for LSB content extraction
W1
W1 = W2 ?
No (It ≠ I)
A user specified key K3
A user specified key K4
Yes (It = I)
Tamper localization and restoration
b

Fig. 3.1 Selective authentication system by semi-fragile watermarking; a generation of authenticator; b verification of authenticity

Van Schyndel, Tirkel and Osborne proposed a method that exploits the maximum length shift register sequence, called the m-sequences. The m-sequences are often used to represent random sequences. These sequences are of length L= $(2^n - 1)$ bits, where n is the number of echelons in a register. They are generated from m shift registers with looping. The registers mainly depend on primer polynomials coefficients. These m-sequences have a period L and each one of them contains (2^{n-1}) elements equal to (+1) and $(2^{n-1}-1)$ elements equal to (−1). The most important characteristic of the m-sequences is the auto-correlation function $R_{x,x}(q)$:

$$R_{x,x}(q) = \sum_{I=0}^{L-1} x_i x_{i+q} = \begin{cases} L, if & {\scriptstyle q=0} \\ -1, if & {\scriptstyle q\neq 0} \end{cases} \qquad (3.6)$$

Where 0≤q<L is a shift between two sequences.

For large i, where i is the number of bits, the following property $R_{x,x}(0) >> R_{x,x}(q)$ is obtained, q≠0. This property allows the localization of the random sequence even in the presence of additive noise. The method suggested by the authors modifies the LSB by adding extended m-sequences to the lines of the original image. The m-sequences can be generated recursively by the relation of Fibonacci. The auto-correlation function and the spectral distribution of these m-sequences are similar to those of a Gaussian noise. For a 512×512 image, coded with 8 bits, a sequence of 512 bits length is randomly changed and coded line by line in the LSB of each pixel. A simple cross-correlation is used to test for the presence of the watermark by comparing the content of the LSB of each pixel with a watermark that is generated with the same parameters. The security of this system, which is based on the security of the generated m-sequences, was tested and approved in several works. To exploit the unique and optimal auto-correlation function of the msequences, the authors proposed another technique in the same work which adds the bits of the watermark to the LSB of each pixel instead of replacing it. The detection capabilities are good but localization capabilities are not optimal. Robustness against noise addition and compression based on adaptive histogram manipulation and JPEG standard are also demonstrated. However, the algorithm is not able to recover the damaged data in an image. In fact, if an image is declared to be non-authentic, there is no information that can be used for restoration since the m-sequences used as a watermark are not dependent on the image. Moreover, the algorithm needs high computationally time which makes it almost impractical.

This method has been further improved by Wolfgang and Delp with small modifications that enhance its robustness and its capability to localize the corrupted regions. To generate the watermark, a binary sequence is mapped from {0, 1}to {−1 ,1}, rearranged in desired blocks of dimensions 8×8, and added to the pixels value of the correspondent 8×8 blocks in the original image with the following expression:

$$Y (b) = X(b) + W(b) \qquad (3.7)$$

Where Y(b) is the watermarked image, X(b) is the original image and W(b) is the watermark. The presence of the watermark can be simply verified by:

$$\delta (b) = Y (b)W(b) – Z(b)W(b) \qquad (3.8)$$

The values of δ (b) are then compared with a threshold to decide about the authenticity of the tested image Z(b). The threshold represents a compromise between the robustness of the system and its capacity to detect any malevolent manipulation. The authors proposed to compute it from the number of elements in the watermark block. Another proposition may be an adaptation of the threshold to different image regions. This could help tolerate different operations dependently on the image information in each region. The main advantage of this method consists in allowing an authorized user who knows the watermark to reconstruct the original image. Moreover, since the correlation properties cannot be affected without the knowledge of the embedded sequence, this method is secure. However, an attacker can compute the watermark in a block, knowing a limited number of consecutive hidden bits. To avoid this problem, the authors proposed to use other codes, such as the nonlinear codes of gold or Kasami codes. This algorithm preserves robustness against noise addition and compression. Moreover, it is able to survive some filtering operations and can localize malevolent manipulations with acceptable precision. However, some additional tests still need to be carried out with other manipulations that preserve the content.

Alternatively, Zhu and Tewfik proposed two techniques that use a mask in the spatial or in the frequency domain. Their watermark can detect errors until half of acceptable manipulations for each pixel or each frequency coefficient according to whether the mask is used in space or in the frequency domain. Generally, the effects of space or frequency masking are often used to form sequences of pseudo noise in order to maximize the energy of a watermark while maintaining the watermark itself invisible. The authors used the masking values obtained by the model with visual threshold from their work on image binary rate low coding. In fact, the spatial or frequency masking is inspired by the human visual system model (HVS). This model is used to determine the maximum invisible distortion that can be applied to each pixel or each frequency coefficient. The original image is subdivided into blocks and for each block a secret random signature (a pseudo-random sequence uniformly distributed in the interval [0, 1]) is multiplied by the mask values of this same block. The resulting signal depends on the image block, and it is added to the original block. The resulting values are then quantified by the same mask values. The authors apply this technique to blocks of dimensions 8×8. The blocks are transformed thereafter using the DCT, and the mask values M (i, j) for each DCT coefficient P(i, j) are computed by the frequency mask model. The values M (i, j) are the maximal changes that do not introduce perceptible distortions. The DCT coefficients P (i, j) are modified by the following expression:

$$P_s(i,j) = M(i,j) \left\{ \left| \frac{P(i,j)}{M(i,j)} \right| + sign\big(P(i,j)\big) r(i,j) \right\} \qquad (3.1)$$

Where, r(i, j) is a key dependent noise signal, $\lfloor x \rfloor$ round x to zero and sgn(x) is the sign of x defined as:

$$\text{Sign (x)} = \begin{cases} 1, if \;\; x \geq 0 \\ -1, if \;\; x < 0 \end{cases}$$

The error introduced by the operation below is smaller than the threshold of imperceptibility. This means that:
|Ps(i,j) – P(i,j)|≤ $M(i,j)$, which implies that the modifications made to the DCT coefficients are invisible. For a test image with DCT coefficients Ps ' (i, j), the mask values M' (i, j) are computed. The error e' is estimated by:

$$e' = P'_S - M'\{sign(P'_s)r + \lfloor \tfrac{P'_s}{M'} - (r - \tfrac{1}{2})sgn(p'_s) \rfloor\}$$

Where, all the values are evaluated at the same frequency location (i, j). This technique can detect malevolent manipulations and can localize them with acceptable precision. The algorithm is robust against JPEG compression with small ratios. However, it detects only errors smaller than half of the acceptable distortion for each pixel. In other words, this method gives good results when the distortions in the tested image are relatively small. Moreover, its robustness against other manipulations that preserve the image content was not shown. Frequency masking method is more powerful than the space masking method, which is very sensitive to the noise introduced by the watermark shape. The algorithm did not show any restoration capabilities.

4. Simulation results

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

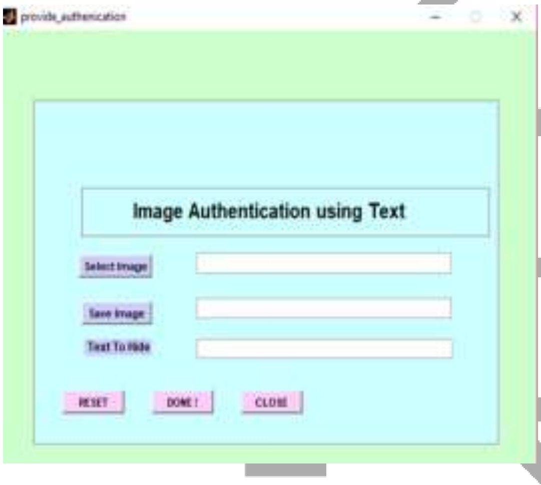


Fig 4.1: Main GUI that is the first layout develop in MATLAB

Fig 4.2: Image Authentication using Text Image

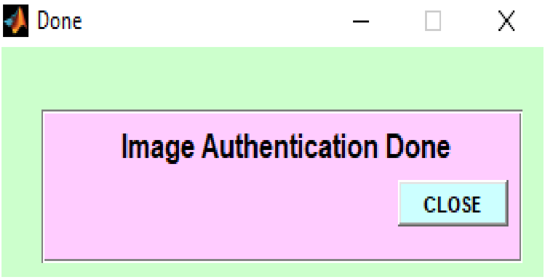


Image Authentication Done

Fig 4.3: Image Authentication done

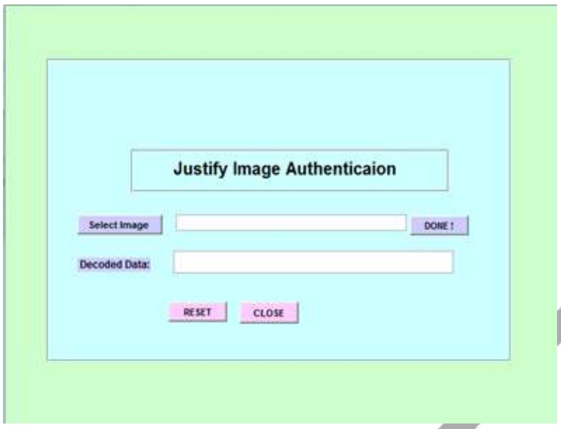
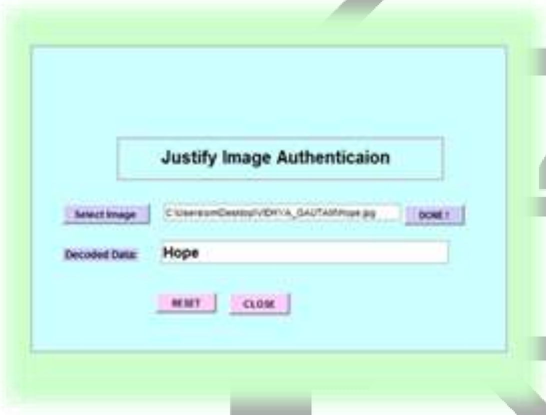


Fig 4.4: Justify image Authentication



C:\Users\som\Desktop\VIDHYA_GAUTAM\hope.jpg

Decoded Data: Hope

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.

Image Authentication techniques enable the recipients to verify the integrity of the received image. The increasing need for trustworthy distribution of digital multimedia in business, industry, defence etc. has led to the concept of content-based authentication. Nowadays manipulating digital images efficiently and seamlessly has become very easy with the availability of powerful software and necessary to ensure confidentiality as well as integrity of the images that are transmitted. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Number of image processing tools to change images for different purposes, it leads to problems such as copyright infringement and hostile tampering to the image contents. Image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication.

5. Conclusion

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] AdilHaouzia& 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

[14] Alexandre H. Paquet[1], wavelet packets-based digital watermarking for Image verification and Authentication, 27 July 2003, pp. 2-24

[15] Christian Rey and Jean-Luc Dugelay, A Survey of Watermarking Algorithms for Image Authentication, (2002), pp. 613–621

[16] Eric Kee et al. Digital Image Authentication from JPEG Headers, pp.1-9