DOI: 10.21917/ijivp.2017.0233

AUTHENTICATION, TAMPER LOCALIZATION AND RECTIFICATION ALGORITHM WITH PRIVACY PRESERVATION OF IMAGE FOR THE CLOUD USING HMAC

Sayyada Fahmeeda Sultana[1] and D.C. Shubhangi[2]

[1]*Department of Computer Science and Engineering, PDA Engineering College, India*

[2]*Department of Computer Science, Visvesvaraya Technological University, India*

Abstract

Digital images like military, medical and quality control images are increasingly stored over cloud server. These images need protection against attempts to manipulate them since manipulations could tamper the decisions based on these images, many approaches have been proposed to protect the privacy of multimedia images over cloud through cryptography, these cryptographic approaches prevent the visibility of image contents but it does not identify if any changes are made on encrypted data by insider attack and cipher-text only attack. In this paper, we proposed to provide authentication, tamper localization, rectification along with privacy preservation of the image using padding extra bit plane for tamper localization, Hash message authentication code (HMAC) algorithm to authentication image, tamper rectification. The proposed algorithm will provide privacy to the image through hiding bit planes.

Keywords:

Image Authentication, Privacy Preservation, Tamper Localization, Cloud, Insider Attack, Sabotage Attack, Hash Message Authentication Code

1. INTRODUCTION

Cloud Computing is used in many areas that requires huge storage, high processing, alternative to local infrastructure by providing third party data centers managed by Cloud Provider, etc. In spite of many advantages Cloud Computing put forth some issues, which are the main subjects of study from security concern are privacy protection, Authentication.

Digital images when stored on cloud are more venerable of manipulation due to the availability of powerful image manipulation software's with minute changes it is almost impossible to Fig.out which is the original and manipulated image. Digital images stored on cloud are accessible to only the cloud service provider there workers or insider of the cloud and the owner of the image. The workers of cloud who have write permission to the image may tamper it maliciously this type of tampering to image by the people in the cloud is an insider attack.

Digital Images stored on the cloud may suffer from insider attack which is one of the most difficult problems in computer security, and indeed in all aspects of real-world security.

The insider attacks are categorized into following two categories [1] Sabotage attacks: An action taken by insiders that cause the results of a processing the images to be incorrect. These kinds of attacks are performed by any agent who is considered to have write permission for images. Data exfiltration: An attack that is characterized as actions by insiders that cause sensitive data to be made available to people that are not authorized to such access.

These attacks can degrade the security of cloud environment to overcome these problems authorities in cloud need to adopt a mechanism that performs authentication and privacy protection of highly sensitive digital images. To protect image privacy and combat unsolicited accesses in cloud by insider attack it need to be encrypted so that it is visually disturbed to protect the privacy of image.

The digital signature approach for image authentication embeds the signature with file in isolation from the original image, so this process demands extra bandwidth to transmit the image and digital signature. To overcome weaknesses of digital signature for content authentication most of the researchers proposed watermarking techniques for digital data authentication. Digital signature and digital watermarking approach for image authentication works by generating digital signature and embedded in image using watermarking [2]. In digital signature, content modification or data manipulation or tampering can be found out. But the location where such alteration has been found is not easy to identified [3] [4] [5] [6]. A combined approach of LSB watermarking method with Enhanced Modified Version of RC6 for encryption scheme to provide content authentication for image compressed as proposed in [7]. A wavelet-based reversible watermarking scheme was proposed to provide secure image authentication in [9]. The hybridization of text and image based authentication suggested for cloud services in [9]. Ascheme based on reversible watermarking to provide authentication along with residue number system [14]. To embed digital signature a 12-bit watermark key will be created from each block of host image which will be embed to last three significant bit of each block [11]. A method that utilizes a rehashing model to overcome easy collisions of the numerous metadata in key space, thereby innovatively enhancing its effectiveness against attacks the scheme embeds image feature values in the LSBs of the original image to protect the content of the image [16]

A camera signature retrieved from a JPEG image consisting of information about quantization tables, thumbnails, Huffman codes and EXIF format or theAdobe Photoshop signature these signatures are simple to extract and offer as a method to establishan another way of providing the authenticity of a digital image [12].

The above methods of watermark embedded in an image and signature extracted from a JPEG image have clear drawbacks. In their propositions, authenticity will not be preserved unless every pixel of the images is unchanged. The watermark usually will be destroyed after manipulation. Authenticity is determined by examining the watermark extracted from the received image [13].

The reasons for sabotage attack may include personal predispositions, stressful events, to plan or ongoing malicious acts, failed to detect rule violation are analyzed [14]. An insider attack with the cloud is easier to perform as whole image is stored on cloud [15], [14] and has far greater impact than an attack in a traditionalinfrastructure [17]. A method that provides image compression along with image security uses a combination of EZW for authentication& chaos for security proposed in [19]. An efficient and secure encryption scheme which combines arithmetic coding, both on static and adaptive models, with chaos-based pseudorandom bit generators to perform both lossless compression and encryption of images [20].

The paper proposed an image authentication algorithm is proposed based on binary pixel value padding for tamper location, detection of presence of tampering is performed by generating digital signature using HMAC authentication algorithm and tamper rectification, which will overcome the problems associated with watermarking. The proposed algorithms provide privacy preservation of image along with authentication.

Rest of the paper is organized with brief review of HMAC in section 2. In section 3, the methodology of our proposed image authentication, tamper localization and rectification algorithm are explained. Section 4 exhibits the examination analysis for results of the proposed method along with the comparison of result with others state of art methods using watermarking. Concluding remarks and future work of proposed method in section 5 along with contribution of proposed method.

2. THE HMAC FUNCTION

To verifying the integrity and authenticity of images stored on a cloud require a method by which cloud servers may validate the authenticity of images stored in the cloud to check it is unmodified. This authenticity can be performed using Message Authentication Code (MAC) that generate a checksum using Eq.(1).

Let F be indicates a hash function. The HMAC function [23] operates on x inputs of varying length and uses a random string k of length one as its key:

$$HMAC_k(x) = F(\bar{k} \oplus opad, F(\bar{k} \oplus ipad, x)) \tag{1}$$

where, $\bar{k}$ is complementation by adding 0's of k to a full b bit block-size of the iterated hash function, *opad* and *ipad* two fixed b-bits constants, is the bitwise Exclusive or operator and the concatenation represented by commas. In Eq.(1), *opad* is formed by respectively adding b-bit as many times as needed to get a b-bit block, and *ipad* designed with the bytes of SHA-1 (cryptography hash function SHA message authentication of data) these bytes are replicated 64 times.

3. THE PROPOSED ALGORITHM

The proposed image authentication, tamper localization, and rectification algorithm works following stages:

- *Code Generation*: Authentication code generation through HMAC authentication algorithm.
- *Header Attachment*: The code generated in code generation phase is attached to the image as header or footer (without performing watermarking) to allow any useful image processing operations to be done if needed directly on image no effect processing result.
- *Padding*: Each pixel value is padded with extra bits, so that if the image is tempered based on padding bit sequence temper location can be identified.
- *Tamper Rectification*.

3.1 CODE GENERATION

Authentication code provides authenticity to image, if any modifications are performed on image is identified using authentication code generated using algorithm 1.

Algorithm 1: Authentication

```
Input: Image $I(M×N)$
Output: Authentication Code, Authenticity Decision
Step 1:  Divide image $I(M×N)$ into number of logically blocks
Step 2:  $block\_size\_rows = no\_of\_rows$ in block
Step 3:  $block\_size\_columns = no\_of\_columns$ in block
Step 4:  For each $row = 1 : block\_size\_rows : M$
Step 5:  For each $column = 1 : block\_size\_rows : N$
             a. $row\_end = row + block\_size\_rows - 1$
             b. $col\_end = column + block\_size\_column$
           $OneBlock$ = Image($row$:$row\_end$, $column$ : $col\_end$)      (2)
           $Centre\_pixel$ ($C_p$) = Search centre pixel ($OneBlock$)      (3)
Step 6:  End
Step 7:  End
Step 8:  For every $Centre\_pixel$ ($C_p$) calculated using Eq.(2) and
         Eq.(3), HMAC is executed using Eq.(1) on $Centre\_pixel$ ($C_p$)
             a. Combined authentication code generated from
                authentication codes $Authn\_code$
             b. Attach authentication code Authn_code to image as
                footer to image.
             c. Receiver repeats step 1 to step 3 to authenticate
                image R_Authn_code
Step 9:  If ($Authn\_code == R\_(Authn\_code)$)
             a. Image is untampered
Step 10: Else
Step 11: Decision of tamper Localization
Step 12: End
Step 13: End
```

3.2 PADDING IMAGE WITH EXTRA BIT PLANE

To provide the tamper location images is padded with extra bit plane which is done as follows using Algorithm 2.

Algorithm 2: Tamper Localization

```
Input: Tampered Image $I'(M×N)$
Output: Tamper Localized image $I''(M×N)$
Step 1:  Convert each Pixel value of $I'$ into 8-bit binary number
         Eq.(4), Eq.(5)
             $P=i$, $i$ → all pixels in $I'(M×N)$ image      (4)
                     $B$ = bin($P$,8)      (5)
Step 2:  Choose a padding sequence.
```

Step 3: Place extra padding sequence before most significant bits of binary pixel value calculated in Eq.(4), Eq.(5)

$$NewB = \text{Concatenate}(paddingSequence, B) \tag{6}$$

$$B = NewB \tag{7}$$

Step 4: Repeat Step 3 for all pixels.

Step 5: Tamper Localization: Identification of tamper location comparing the padding sequence with each pixel padded a miss match then a tamper is detected otherwise pixel is not tampered.

Tables below illustrate the portion of near right eye of a gray scale lena test image in-terms of pixel values and there binary equivalent Table.1(a). The Table.1(b) shows the same portion that is padded up with extra bits. Binary equivalent of 177 padded 10001101 padded with extra bit 1.

Table.1. Pixel Values Table

177	**164**	**105**	**140**	**47**	**35**
167	**137**	**107**	**88**	**36**	**41**
156	**115**	**73**	**46**	**88**	**95**
95	**75**	**79**	**91**	**93**	**109**
91	**92**	**99**	**104**	**112**	**125**

10001101

(a) Pixel Values of Portion of Gray Scale Lena Test Image

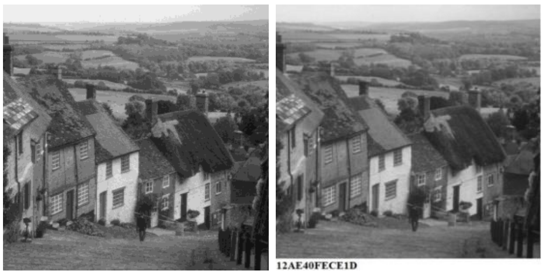
433	**420**	**406**	**396**	**303**	**291**
423	**393**	**363**	**344**	**292**	**297**
412	**371**	**329**	**302**	**344**	**351**
351	**331**	**335**	**347**	**349**	**365**
347	**348**	**355**	**360**	**368**	**381**

100011011

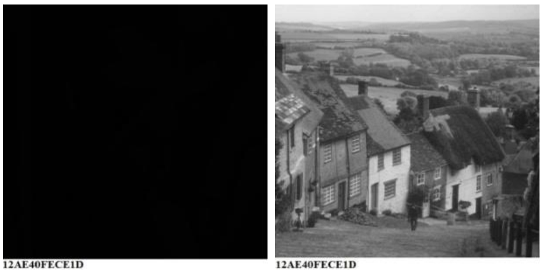
(b) Pixel Values from Table.1(a) After Padding Extra Bit

4. RESULT AND DISCUSSION

In evaluating the proposed image authentication and tamper localization for the cloud using HMAC we took the grayscale test image as the raw image. The original image is shown in Fig.2(a). The Fig.2(b) shows an stage after authentication code generated and attached to original image by execution of Algorithm 1, this code is used later to authenticate the image. The Fig.2(c) shows the result of Algorithm 2 by padding the original image with extra padding sequence the result of this stage will be stored on cloud as the padded image is also providing privacy by hiding the original contents of image and the result of this stage is used for tamper localization. Finally, Fig.2(d) shows the result of un-padding the padded image.



(a) (b)

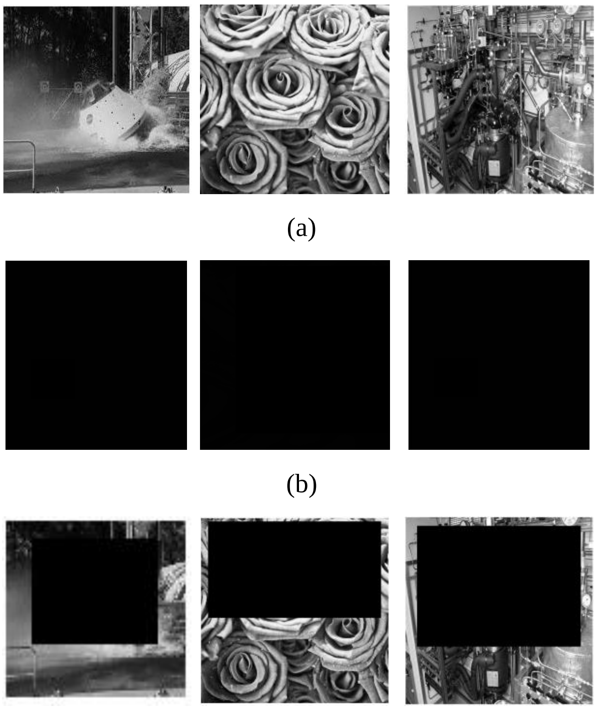


(c) (d)

Fig.1. (a) original image (b) Authentication code attached (c) padded with extra bit plane (d) After un-padding

The Proposed image authentication and tamper localization and rectification for the cloud using HMAC provides authentication along with privacy protection by adding additional bit plane by padded image, these pixels with extra padded bit does not reveal any of the features from original image which is not provided by watermarking approach.

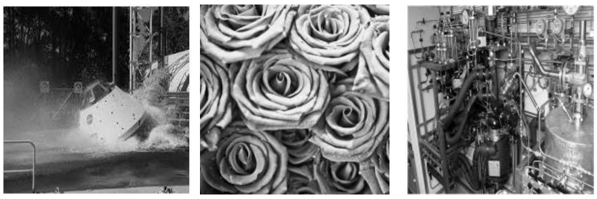
To prove the performance of the proposed Tamper localization and rectification scheme regress experiments were conducted on Dataset of gray images of size 512×512 of 33 images, ORL data set of gray scale face images of images size 112×92 contain 10 categories each contain 40 face images, Flower dataset of 102 Categories each contain 40 images, to show experimental results three 512×512 gray images were used as original images Fig.3(a), tamper Localized images Fig.3(c) and rectified images are shown in Fig.3(d). The padded images shown in Fig.3(b) stored on cloud are privacy preserved as no visual features transparent to minimize the tendency malicious attack.



(a)

(b)

(c)



(d)

Fig.2. Tamper localization and rectification (a) Original images (b) Padded bit plane images with tampering (c) Tamper localized images (d) Tamper rectified images

Robustness Test [24]: To validate the proposed work, algorithms are implemented in MATLAB. The three datasets are executed several number of times and PNSR (Peak Signal to Noise Ratio) is used to determine image distortion degree, where PNSR is measured in dB.

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}}dB \tag{8}$$

where, the constant 255 indicates Max Color intensity,

MSE is Mean Squared Error, which is calculated as,

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[P(i,j)-Q(i,j)\right]^2 \tag{9}$$

where, *n* and *m* are dimensions of image, *P* is the original image, Q is the noisy approximation.

Table.2. PSNR of Original image with Tamper Localized and Tamper Rectified Images

Images	**PSNR of Rectified Image**
Ship with falling part	36.6822
Roses	35.3385
Industrial plant	30.7088

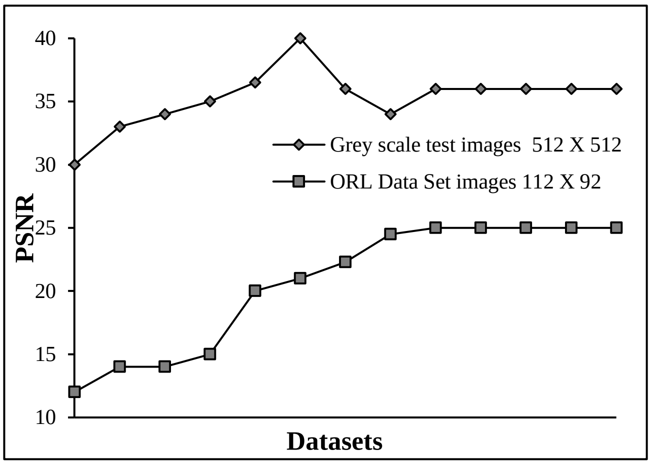


Fig.3. Graph Showing PNSR of test images from Grey scale dataset, ORL dataset, Flower dataset

The Table.2 shows PSNR of the three test images, when an original image is compared with tamper rectified images. The Fig.3 Shows graph of PNSR of rectified images with original images on three different datasets, Experimental analysis shown that as image size increases PNSR increases. The Proposed method provides Tamper localization accuracy of 99.98% irrespective of tamper size, a 0.02% of error may be generated if attacker is familiar with the authentication strategy and using and follows the same padding sequence.

Table.3. Comparison of proposed tamper localization method with Rehashing model [21] and fragile watermark-based image authentication [16]

Methods	**Average Tamper Detection accuracy for Gray Image**	**Rectification Technique**
Rehashing model [21]	99.73%	Watermark feature values in LSB
Fragile watermark-based image authentication [16]	96.01%	Watermarking
Proposed	99.98%	Flat Table

To the best of our knowledge the proposed method provide high tamper detection accuracy, Image rectification is performed without watermarking as if image is tampered the watermark also changes.

5. CONCLUSIONS AND FUTURE WORK

The proposed authentication algorithm has satisfied all the general requirements that essential for any authentication system like sensitivity, robust, Localizable, Recoverable, Security through encryption, Portability, Complexity. The Proposed scheme provide a solution for sabotage attack, if any insider attacks appears on image as no visual feature are visible, so tampering is not based on modification to interest point. If tampering occurs image authentication algorithm identifies the image is tamper and follows tamper localization and rectification. As a research work the proposed scheme can be implemented for color images.

REFERENCES

[1] Matt Bishop, et al., “Insider Threat Identification by Process Analysis”, *IEEE Security and Privacy Workshops*, pp. 251-264, 2014.

[2] Seyed Mohammad Mousavi, “Image Authentication Scheme using Digital Signature and Digital Watermarking”, *International Journal of Computational Engineering and Management*, Vol. 16, No. 3, pp. 59-63, 2013.

[3] M.S. Wang and W.C. Chen, “A Majority-Voting Based Watermarking Scheme for Colour Image Tamper Detection and Recovery”, *Computer Standards and Interfaces*, Vol. 29, No. 5, pp. 561-570, 2007.

[4] J.J. Eggers and B. Girod, “Blind Watermarking Applied to Image Authentication”, *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Vol. 3, pp. 1977-1980, 2001.

[5] E.T. Lin, C.I. Podilchuk and E.J. Delp, “Detection of Image Alterations using Semi-Fragile Watermarks”, *Proceedings of International Society for Optics and Photonics in Electronic Imaging*, pp. 152-163, 2000.

[6] D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication", *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1167-1180, 1999.

[7] S. J. Jereesha Mary, C. Seldev Christopher and S. Sebastin Antony Joe, "Novel Scheme for Compressed Image Authentication using LSB Watermarking and EMRC6 Encryption", *Circuits and Systems*, Vol. 7, pp. 1722-1733, 2016.

[8] P. Meenakshi Devi, "Reversible Image Authentication with Tamper Localization Based on Integer Wavelet Transform", *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, pp. 67-74, 2009.

[9] D.E. Popescu and A.M. Lonea, "An Hybrid Text-Image Based Authentication for Cloud Services", *International Journal of Computer Communication*, Vol. 8, No. 2, pp. 263-274, 2013.

[10] Suraj Kumar Singh, Varun P. Gopi and P. Palanisamy, "Image Security using DES and RNS with Reversible Watermarking", *Proceedings of IEEE International Conference on Electronics and Communication*, pp. 354-368, 2014.

[11] Sajjad Dadkhah , Azizah Abd Manaf and Somayeh Sadeghi, "Efficient Digital Image Authentication and Tamper Localization Technique using 3LSB Watermarking", *International Journal of Computer Science Issues*, Vol. 9, No. 2, pp. 1-8, 2012.

[12] Eric Kee, Micah K. Johnson and Hany Farid, "Digital Image Authentication from JPEG Headers", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, pp. 1066-1075, 2011.

[13] Ching-Yung Lin and Shih-Fu Chang, "A Robust Image Authentication method Distinguishing JPEG Compression from Malicious Manipulation", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 11, No. 2, pp. 153-168, 2001

[14] William R. Claycomb, Carly L. Huth, Lori Flynn, David M. McIntire and Todd B. Lewellen, "Chronological Examination of Insider Threat Sabotage: Preliminary Observations", *Software Engineering Institute*, pp. 1-15, 2012.

[15] Miltiadis Kandias, Nikos Virvilis and Dimitris Gritzalis, "The Insider Threat in Cloud Computing", *Proceeding of 6th International Workshop*, pp. 93-103, 2011

[16] William R. Claycomb and Alex Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges", *Proceedings of IEEE 36th Annual Computer Software and Applications Conference*, pp. 154-159, 2012

[17] Adrian Duncan, Sadie Creese and Michael Goldsmith, "An Overview of Insider Attacks in Cloud Computing", *Concurrency and Computational Practice and Experience*, Vol. 27, No. 12, pp. 2964-2981, 2014.

[18] Mihir Bellare, Ran Canetti and Hugo Krawczyk, "Keying Hash Functions for Message Authentication", *Proceedings of Annual International Cryptology Conference*, pp. 1-15, 1996.

[19] T. Venkata Sainath Gupta, C. Naveen, V.R. Satpute and A.S. Gandhi, "Image Security using Chaos and EZW Compression", *Proceedings of IEEE Students Conference on Engineering and Systems*, pp. 115-119, 2014.

[20] Atef Masmoudi and William Puech, "Lossless Chaos-based Crypto-Compression Scheme for Image Protection", *IET Image Processing*, Vol. 8, No. 12, pp. 671-686, 2014.

[21] Wan-Li Lyu, Chin-Chen Chang and Feng Wang, "Image Authentication and Self-Recovery Scheme based on the Rehashing Model", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, No. 3, pp. 460-474, 2016.

[22] Hong Zhong, Haiquan Liu, Chin-Chen Chang, "A Novel Fragile Watermark-based Image Authentication Scheme for AMBTC-compressed Images", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, No. 2, pp. 362-375, 2016.

[23] Mihir Bellare, Ran Canetti and Hugo Krawczyk, "Keying Hash Functions for Message Authentication", *Proceedings of Advances in Cryptology*, pp. 1-19, 1996.

[24] Bo Zhao, Guihe Qin and Pingping Liu, "A Robust Image Tampering Detection Method based on Maximum Entropy Criteria", *Entropy*, Vol. 17, No. 12, pp. 7948-7966, 2015.