Shodhshauryam, International Scientific Refereed Research Journal
© 2018 SISRRJ | Volume 1 | Issue 4 | ISSN : 2581- 6306

Robust Image Authentication Using Two-Phase Tag Generation Algorithm

Yuvaraj V
Electronic and Communication Engineering, College of Engineering Guindy, Anna University, Chennai, Tamilnadu, India

ABSTRACT

Image authentication techniques have recently gained great consideration due to its importance for a large number of multimedia applications. Digital images are increasingly transmitted over non-secure channels such as an internet. Thus, military, medical and quality control images must be protected against attempts to manipulate them; such manipulations could tamper the decisions based on these images. Hard authentication and soft authentication has some advantages and disadvantages. To overcome these drawbacks, this paper proposed hybrid design to protect the authenticity of multimedia images. The Approximate Message Authentication Code (AMAC) combines error-correcting codes with cryptographic techniques. In two phase tag generation algorithm have two tags where first tag is protect the image content by using dc elements of Discrete Cosine Transform (DCT) image and the second tag shows sensitivity of image by using ac elements of Discrete Cosine Transform (DCT) image. The proposed scheme attains better the robustness and fragility.

Keywords : Approximate Message Authentication Code (AMAC), Discrete Cosine Transform (DCT), Image authentication.

I. INTRODUCTION

Multimedia authentication has recently gained significant attention due to the readily available multimedia editing and reconstruction tools and the need for transmission of multimedia objects, such as audio, video and text, over non-secure networks. Authentication of these multimedia objects is very different from standard data authentication. Multimedia data is almost always preprocessed or modified before usage or transmission over (insecure) networks. The preprocessing and modifications include such as compression, quantization, scaling, cropping etc. These operations affect the multimedia data; however, the content remains unaffected. Standard authentication mechanisms are effective in authenticating the actual multimedia data but not in authenticating the multimedia content. A new method for robust image authentication is discussed and developed in this paper. In general, the purpose of image authentication is to verify the authenticity of the images as long as the content is preserved.

To verify image authenticity using standard image authentication techniques, an authentication tag is calculated by the sender and appended to the compressed image or embedded in it. When the receiver decompresses the image, this may potentially result in a modified image which is usually identical to, or very close to, the original one. The image is declared authentic or inauthentic by comparing the reliably received or the extracted appended tag from the decompressed image with the recalculated or the re-extracted tag. Both sender and receiver use a shared secret key.

Organization of this paper: Section 3 presents the proposed scheme. Section 4 gives the simulated results and discussions. Section 5 deals with the conclusion and future work.

II. PROPOSED METHODOLOGY

The proposed approach consists two major algorithms are two phase tag generation algorithm and verification algorithm.

A. Two Phase Tag Generation Algorithm

Two phase tag generation algorithm consists of preprocessing of image, intermediate hash generation containing feature extraction and final hash. The flowchart for two phase tag generation algorithm is given in Fig.1.to keep the city clean by informing about the garbage levels of the bins by providing graphical image of the bins via IOT Php web development platform.

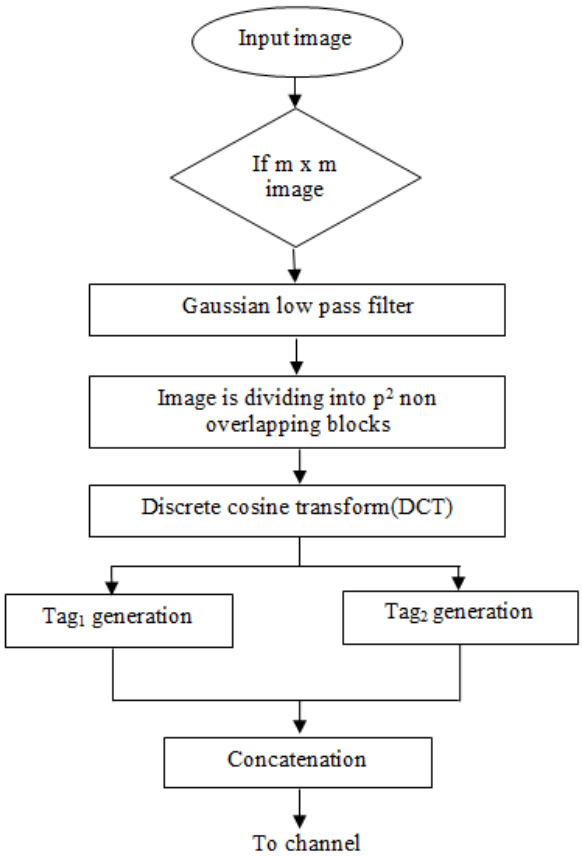


Fig.1. Two-phase tag generation algorithm

1) **Preprocessing**

The preprocessing of an image includes the low pass Gaussian filter, Discrete Cosine Transform (DCT) image processing operation. If the image I is fixed square size image then it is applied to the low pass Gaussian filter. Otherwise the image I mapped to fixed square size image. To increase robustness against minor con- tent-preserving modifications, an optional low-pass filtering such as a low-pass Gaussian filter can be applied. The pre-processed image is called J. Then the image J is divided into p^2 non-overlapping equal size blocks l x l. Here l = 8 which is a good match with the JPEG compression, the DCT mapping and the image size 128 x 128 or 256 x 256 in use.

The DCT is the most popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain.

2) **Intermediate Hash Generation**

The generic method for calculating the intermediate hash consists of first applying a transformation T on the image blocks $J_1,\ldots,J_{p^2}$ to get the feature vector. $v_i = T(J_i)$ is computed for each image block and the elements containing the more compact information about the image such as low frequency components are extracted and denoted by $u_1,\ldots,u_{p^2}$ to be supported by hard authentication mechanism $AMAC_1$. The elements are quantized to form a q-bit message. Let the tag generated in this step be denoted as tag_1. The flowchart for Tag_1 generation is given in Fig .2.The authentication tag is created based on a

systematic error-correcting code (Enc, Dec) , a standard MAC algorithm $MAC(k_1,.)$ and a symmetric encryption-decryption algorithm (E_{k2},D_{k2}). $Enc(.,\delta)(Dec(.,\delta))$ is an encoding (decoding) algorithm with an error correction capability of δ symbols and $E_{k2}(D_{k2})$ indicates an encryption (decryption) algorithm.

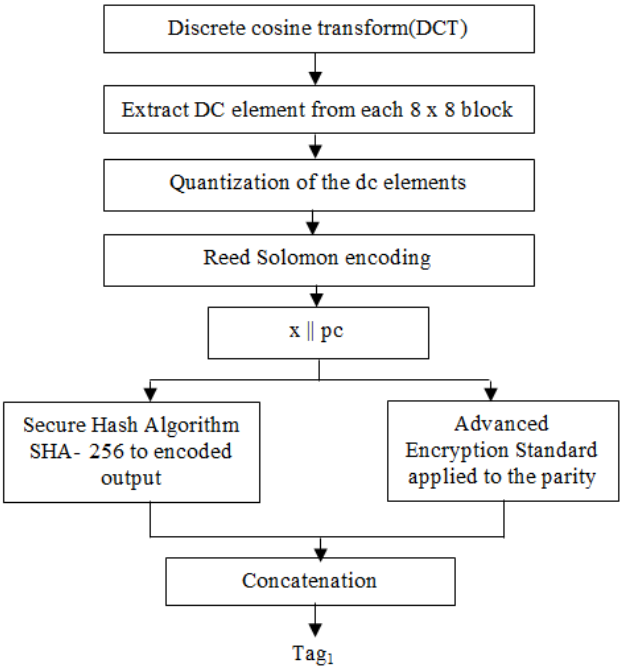


Fig.2. Tag_1 generation

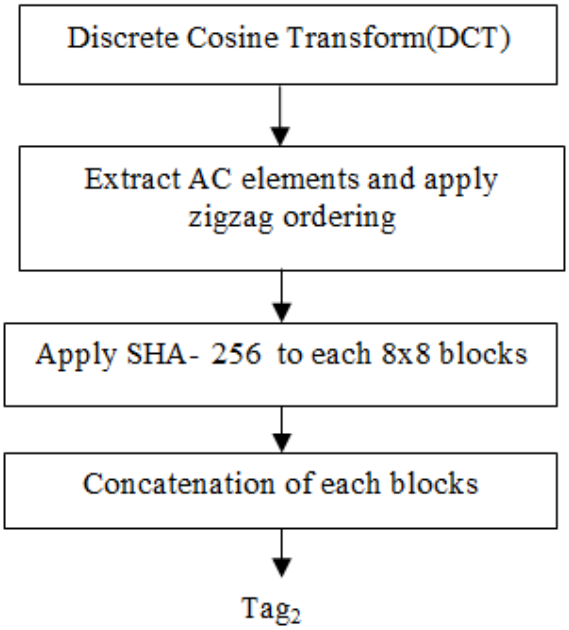


Fig.3. Tag_2 generation

A selection of other elements from DCT image containing less compact information about image (AC components) are considered for the soft authentication step. The elements are used by $AMAC_2$ tag generation algorithm to generate the second tag_2. The second phase of the hash generation tag takes the first ten AC coefficients of the DCT matrix of each block according to zigzag order and quantization table used in the JPEG compression algorithm. Then applying MAC algorithm. The flowchart for Tag_2 generation is given in Fig.3.

1) Final Hash Generation

Concatenating tag_1 output and tag_2 output forms the final hash vector tag of the image or the authentication tag submitted over a reliable channel to the receiver.

B. Verification Algorithm

Let I' and tag denote the received image message and the received tag respectively. tag is decomposed into its components tag_1 and tag_2 corresponding to the received tags generated by $AMAC_1$ and $AMAC_2$.The verification process of the proposed scheme takes place in two phases. I' is pre-processed and divided into image blocks $J'_1,\ldots,J'_{p2}$ (here M = N = p) and after applying T to extract $u'_1,\ldots,u'_{p2}$ and quantization, the MAC is computed using the secret key. If the calculated MAC matches the received one extracted from tag_1, the first phase of the verification corresponding to $AMAC_1$ succeeds. Otherwise an attempt is made to correct $u'_1,\ldots,u'_{p2}$ using the error-correcting code. If the first verification phase succeeds, the second verification phase corresponding to $AMAC_2$ starts. The verification in the second phase is successful if at least $Tr.t_2$ positions in have equal hash blocks.

III. RESULTS AND DISCUSSIONS

An image I is fixed square size image then it is applied to the low pass Gaussian filter. Otherwise the image I mapped to fixed square size image. The output of low pass Gaussian filter is divided into p_2 non-overlapping equal size blocks l x l where l=8 and p=32. Then applying Discrete Cosine Transform to each block. It transforms a signal from spatial domain to frequency domain. Low frequency components are extracted and to be supported by hard authentication mechanism $AMAC_1$. The elements are quantized to form a q-bit message. Let the tag generated in this step be denoted as tag_1. A selection of other elements from DCT image containing less compact information

about image (AC components) are considered for the soft authentication step. The elements are used by $AMAC_2$ tag generation algorithm to generate the second tag_2. Concatenating tag_1 output and tag_2 output forms the final hash vector tag of the image or the authentication tag submitted over a reliable channel to the receiver. The simulation results is shown in Fig.4

Now apply two phase tag generation algorithm for these 9 images that is original images and content preserved versions of images. Then comparing original hash with content preserved versions of images. As the results derives if the comparing hash of original images and content preserved versions of images are equal means the image is authentic, otherwise the image is inauthentic. The robustness and fragility is calculated for the two phase tag generation algorithm.

A. Robustness

The robustness can be measured by using True acceptance rate (TAR). To calculate a true acceptance rate for a total of n_1 images (including original and content-preserved versions), let the number of content-preserved versions of the original images declared as authentic be n_2.

$$\text{True acceptance rate} = n_2 / n_1$$

From simulation, $n_1 = 6$ and $n_2 = 6$.Therefore, the true acceptance rate = 1 which is good for robustness of image.

B. Fragility

The robustness can be measured by using False acceptance rate (FAR). To calculate a false acceptance rate for a total of images (including the original and the modified/attacked versions), the number of n_1' images judged as authentic images is calculated and denoted by n_2'.

(a)

(b)

(c)

Fig.4.(a) cameraman original image, (b) Gaussian Low Pass Filtered image, (c) DCT image.

False acceptance rate = n_2' / n_1'

From simulation, $n_1' = 6$ and $n_2' = 3$. Therefore False acceptance rate = 0.5 which is good for fragility of an image.

(a)

(b)

(c)

Fig.5. Original images : (a) cameraman, (b) saturn, (c) rice.

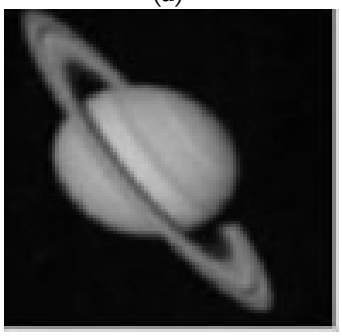
(a)

(b)

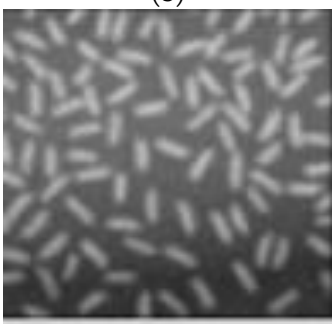
(c)

Fig.6. median filtered images of ordered 4: (a) cameraman, (b) Saturn, (c) rice

(a)



(b)



(c)

Fig.7. Average filtered images of ordered 8: (a) cameraman, (b) Saturn, (c) rice.

IV. CONCLUSION

A generic robust two-phase scheme for image authentication has been presented. The verification algorithm verifies the authenticity of the received image in two phases based on the combination of soft and hard authentication techniques. The proposed scheme was shown to be tolerant to common

content-preserving modifications on images which may be introduced during transmission or which may be the result of image processing operations. The robustness can be measured by using True acceptance rate (TAR) and Fragility can be measured by using False acceptance rate (FAR). Future work will be focused on improvement of the robust two-phase image authentication scheme towards to the tamper/forgery classification and accurate forgery area localization of image.

V. REFERENCES

[1]. Seyed Amir Hossein Tabatabaei, Obaid Ur-Rehman, Natasa Zivic, and Christoph Ruland, "Secure and Robust Two-Phase Image Authentication" IEEE Trans.Inf. VOL. 17, no. 7, july 2015.

[2]. Y Zhao, S. Wang, X. Zhang, and H. Yao, "Robust hashing for image authentication using zernike moments and local features," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 55–63, Jan. 2013

[3]. D Tonien, R. Safavi-Naini, P. Nickolas, and Y. Desmedt, "Unconditional secure approximate message authentication," in Proc. Int. Workshop Coding Cryptology, 2009, vol. 5557, pp. 233–247.

[4]. L Xie, G. R. Arce, and R. F. Graveman, "Approximate image message authentication codes," IEEE Trans. Multimedia, vol. 3, no. 2, , Jun. 2001.

[5]. NE-D. Sherif and M. Mansour, "Fragile and semi-fragile image authentication based on image self similarity image processing," in Proc.Int. Conf. Image Process., 2002, vol. 2, pp. 897–900.

[6]. M P. Queluz, "Toward robust, content based techniques for image authentication," in Proc.Workshop Multimedia Signal Process., 1998, pp.297–302.

[7]. C Kailasanathan, R. Safavi-Naini, and P. Ogunbona, "Image authentication surviving acceptable modifications," in Proc. IEEE-EURASIP, Workshop Nonlinear Signal Image Process., 2001.

[8]. I C. Chang, B. W. Hsu, and C. S. Laih, "A DCT quantization based image authentication system for digital forensics," in Proc.Int. Workshop Systematic Approaches Digit. Forensic Eng., 2005,pp. 223–235.

[9]. H T. Chang, C.-C. H., C.-H. Y., and D.-F. S., "Image authentication with tampering localization based on watermark embedding in wavelet domain," Opt. Eng., vol. 48, no. 5, pp. 1–10, 2009.

[10]. G. D. Crescenzo, R. F. Graveman, and G. R. Arce, "Approximate message authentication and biometric entity authentication," in Proc. Financial Cryptography, 2005, vol. 3570, pp. 240–254.

[11]. R. F. Graveman and K. Fu, "Approximate message authentication codes," in Proc. Annu. Symp. Adv. Telecommun. Inf. Distrib. Res.Program, 1999.