Communication papers of the Federated Conference on Computer Science and Information Systems, pp. 223–226
DOI: 10.15439/2017F202
ISSN 2300-5963 ACSIS, Vol. 13

A Robust Watermarking Technique for Image Content Authentication

Obaid Ur-Rehman and Natasa Zivic
Chair for Data Communications Systems
University of Siegen
Hoelderlinstrasse 3, 57076 Siegen, Germany
email: {obaid.ur-rehman, natasa.zivic}@uni-siegen.de

***Abstract*— A robust watermarking technique for image content authentication is proposed. The proposed technique is robust to minor modifications resulting from legitimate image processing operations. At the same time, the modifications affecting image content are classified as forgery attacks by the proposed scheme. Simulation results are given for intentional modifications (forgery attacks) as well as unintentional modifications (channel noise). Different levels of noisy environments are assumed including the coded orthogonal frequency division multiplexing which is used in 5G networks, to prove the effectiveness of the proposed scheme. A security analysis of the proposed watermarking scheme is given in the end.**

Keywords- Robust Watermarking; Content based Authentication; COFDM; Error Tolerance; Feature Extraction.

I. Introduction

With the widespread availability of multimedia editing tools, image content can be easily edited for forgery. As a consequence, there is a strong need for image integrity verification and content authentication algorithms. A digital watermark is a signature of the image and typically inserted inside the image to prove its authenticity or ownership at a later stage. The watermark might be visible or invisible. Unlike digital signatures, digital watermarking [1] does not require extra transmission bandwidth. Watermarking methods are designed to be prone to minor modifications in the image data. On the other hand, digital signatures are very sensitive to modifications in the image data. Due to a well-known phenomenon, called the Avalanche Effect [2], data authentication fails even in the presence of a single bit error.

A new class of authentication mechanisms have emerged recently, called noise tolerant or soft authentication mechanisms [3]. These mechanisms are different from the standard authentication mechanisms as they are designed to be tolerant to minor changes in the data. Simply put, the authentication succeeds despite the data protected by these mechanisms being a little different (decided based on a threshold) than the data on which the authentication tag was computed.

The watermarking technique proposed in this paper is based on generating the authentication tag using the approximate message authentication code (AMAC) [4] and then using it as a watermark. AMAC is tolerant to minor changes in data as opposed to standard message authentication code (MAC) [5, 6] which does not tolerate data modification. The proposed method is analyzed for security. Simulation results are given for different noisy environments and forgery attacks.

This paper is organized as follows. Related work is presented in Section II. The proposed watermarking technique is presented in Section III, including the improvements on the existing methods. Simulation results are given in Section IV. A security analysis of the proposed scheme is presented in Section V. The paper is concluded in Section VI.

II. Related Work

Noise tolerant data authentication methods proposed in literature include approximate message authentication code (AMAC) [4], noise tolerant message authentication code (NTMAC) [7] and joint channel coding and cryptography [8], just to name a few. AMAC is considered in this work. It is based on the usage of majority logic for generation of the authentication tag. The tag is generated by grouping the data into rows and columns of a chosen dimension and XORing it with pseudo random bit stream. The final tag is obtained using the majority logic.

Another noise tolerant authentication technique is NTMAC, where the data is split into multiple blocks by calculating standard MAC on each block and then retaining only a portion of the MAC (called sub-MAC) for each block, which is then used to detect changes in the block. For tolerance to minor modifications, the concept of partitions is introduced. A variation on NTMAC was proposed by the authors as weighted noise tolerant message authentication code (WNTMAC) [9]. WNTMAC introduces the concept of weights to differentiate the important parts of data from the relatively lesser important parts. The authors also proposed error correcting (EC)-WNTMAC in the same work [9] as an extension of WNTMAC. In EC-WNTMAC, an error location and correction capability was introduced.

The above approaches are not directly suitable for image content authentication, rather only for (image) data authentication. They can be extended to image content authentication by using image features rather than the data. The use of error correction codes further extends the tolerance capability of these techniques.

III. WATERMARKING TECHNIQUE

A. Watermark based on Modified AMAC

Discrete Wavelet Transform (DWT) is computed on the source image, splitting the image into four sub bands, i.e., Low-Low (LL), Low-High (LH), High-Low (HL) and High-High (HH). An AMAC tag is computed on the LL sub band. The computation of AMAC tag is different from the standard AMAC tag [4] which was used in [10]. The modified and strengthened AMAC algorithm uses an extra pseudorandom bit for AMAC tag computation. This avoids the security attack proposed in [11]. The original AMAC uses one pseudorandom bit (x_i) which is XORed with the message bit (m_i). The modified AMAC uses two pseudorandom bits, w_i and x_i and calculates the AMAC tag bit z_i using (1).

$$z_i = m_i \cdot w_i \oplus x_i \quad \textbf{(1)}$$

The AMAC tag is used as a watermark of the image. If there are minor changes in the image, the LL sub band will not change significantly and therefore the corresponding AMAC tag will be the same as for the original image. For changes beyond a chosen threshold, such as in the case of a forgery attack, such as object insertion or object removal, the LL sub band will change significantly resulting in a changed AMAC. The threshold can be chosen as desired using the approach presented in [4]. The watermark generation process for the "Lena" image is shown in Fig. 1.

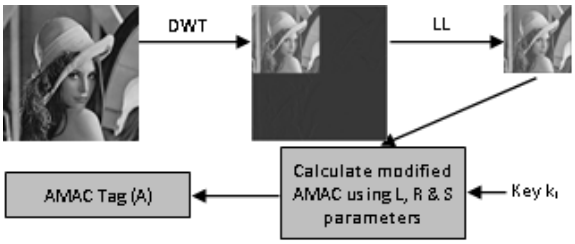

Figure 1. Watermark generation

B. Watermark Embedding

The watermark is self-embedded in the source image in this work. The source image is split into 8 × 8 pixel non overlapping blocks. The length of the AMAC tag is chosen to be 256 bits. The AMAC tag is split into 32 sub-AMACs of 8 bits each. One sub-AMAC is taken at a time and inserted into the Least Significant Bits (LSBs) of every 8th pixel value inside the next image block. Since a block is chosen to be 8 × 8 pixels, the block size is 64 pixels. To embed 8 bits, a total of 8 pixel values are modified. Instead of using the first 8 pixel positions, as in [10], every 8th position is chosen. This enhancement spreads the watermark bits uniformly in the source image block and therefore the quality of the source image is not degraded considerably. The next image block for embedding a sub-AMAC is chosen randomly using a secret permutation, with the help of a secret key, k_2, as seed. This secret permutation makes it very hard for someone (an attacker), without the knowledge of the secret key k_2, to extract and replace the watermark. The watermarked image is the output of the watermark embedding process. It is assumed that the secret keys k_1 and k_2 are pre-shared using standard key exchange mechanisms.

C. Watermark Extraction

In order to prove the authenticity of the image, the watermark is extracted using the procedure as follows. The watermarked image is split into 8 × 8 pixel non overlapping blocks. The LSBs of every 8th pixel's value of the next block (chosen randomly using the same seed k_2 as used at the transmitter) is taken. These bits are appended together to obtain the modified-AMAC tag. This extracted watermark is used for image authentication.

D. Image Authentication

The image verification takes places by comparing the extracted watermark with the watermark recomputed on the image presented for authenticated. Since the watermark is embedded in the spatial domain, it distorts a minor part of the cover image. Authentication based on the standard mechanism will fail in this case. However, since AMAC is tolerant to modifications below a (chosen) threshold, the authentication succeeds in the presence of minor modifications.

IV. SIMULATION RESULTS

The simulations are performed using the following parameters. The dimension of source images used in the simulations is 256 × 256 pixels. The source image is converted into a grayscale image before any other processing. Single level DWT transform is performed on the resultant grayscale image giving four sub-bands, out of which the LL band is used for AMAC tag calculation. The length of modified-AMAC is chosen to be 256 bits and the length of sub-AMACs is chosen to be 8 bits. The watermark is generated using the strengthened AMAC tag as proposed in [11].

Simulation results for the following cases are presented.

A. COFDM Transmission

Orthogonal Frequency Division Multiplex (OFDM) is a crucial technique for modern and future mobile communications (4G, 5G and beyond). Together with Multiple-Input Multiple-Output (MIMO) systems, OFDM is a basis for high speed services to achieve a high Quality of Service (QoS), which is the main advantage of present over previous mobile generations. OFDM is interesting from application point of view as it is used in numerous applications like Digital Audio Broadcasting (DAB, DAB+), Digital Video Broadcasting – Terrestrial (DVB-T [2]), Worldwide Interoperability for Microwave Access (WiMAX), mobile communications 4G and 4.5G - Long Term Evolution (LTE) / LTE-A etc. Coded OFDM (COFDM) is used in case of extreme selective fading channels, e.g., in case that every subcarrier suffers from a different amount of noise measured with different signal-to-noise ratio (SNR).

Results obtained in the presence of COFDM transmission are shown in Fig. 2. COFDM transmission is considered in the presence of regular LDPC codes of rate 1/2 as the forward error correction codes. As all, or most, of the errors are corrected by the LDPC decoder, the image is declared authentic by the proposed algorithm.

Figure 2. Lena image authentication in the presence of COFDM with rate 1/2 LDPC codes

B. Forgery Attack

The authentication for a forged Lena image is shown in Fig. 3 (note the extra hair on the forehead). The LL band of the forged image has a Hamming distance of 17235 to the LL band of the original Lena image of similar dimension. This results in a failed authentication for the forged image.

Figure 3. Lena image authentication in the presence of forgery attack (with extra hair on the forehead)

V. Security Analysis

In this section, the security analysis of the proposed scheme is given. The analysis of AMAC is given in [11], where it is proven that if Hamming distance is used for distance measurement then the scheme might not be secure for large messages, such as high resolution images. The security analysis of the used improved and strengthened AMAC is given in [11]-[12].

The security analysis of the proposed authentication technique is made by considering two major attacks as follows.

A. Key Recovery Attack

Two different keys are used in the proposed authentication technique. The first key (k_1) is used in watermark generation and the other (k_2) is used in watermark insertion. The attacker job is made difficult as he must recover two secret keys, e.g., through brute force attack. In AMAC, the reshaped matrix of size R × L × S bits is used, which means the attack complexity is about $2^{R\times L\times S}$ function (tag generation and verification) operations, which is a very high complexity. For even the smaller image dimension used in the simulations, i.e., 256 x 256 pixels, this attack is computationally infeasible with the current technology.

B. Substitution Attack

A substitution attack can be executed in two steps, i.e., a forgery attack on the strengthened AMAC followed by an attack on the watermark embedding process. The possibility for an attacker to pass the first step can be calculated as follows. Let T be the threshold value below which the difference between the AMAC tags is acceptable and let t indicates the threshold for difference between DWT's LL sub-band tolerance. The probability (P_t) of changes in the "majority" selection round of the AMAC is calculated in [16], as follows,

$$P_t = \frac{1}{2^L \sum_{i=0}^{t} \binom{L}{i}} \sum_{i=0}^{t} \sum_{j=\left\lceil \frac{t+1-2i}{2} \right\rceil}^{\left\lfloor \frac{t-1}{2} \right\rfloor} \sum_{k=0}^{\left\lfloor \frac{2i-2j-t-1}{4} \right\rfloor} \binom{t}{j} \binom{j}{k} \binom{t-j}{i-k} \quad \textbf{(2)}$$

Based on P_t, the probability of deceiving the attacker (P_D) by an image whose AMAC tag is close enough to the reference tag is calculated as,

$$P_D = \sum_{i=0}^{T} \binom{L}{i} P_t^i (1-P_t)^{L-i} \quad \textbf{(3)}$$

It can be observed from (3) that P_D can be decreased by increasing the length of AMAC tag.

VI. Conclusion

A robust watermarking technique for content based image authentication is proposed in the paper. The proposed technique consists of extracting image features using discrete wavelet transform, generating the watermark based on the image features and by protecting it using the noise tolerant

AMAC algorithm. Simulation results are given to show the effectiveness of the proposed algorithm. A security analysis is provided in the end to analyze the security strength of the proposed scheme. In future, a complete mathematical framework, similar to the standard authentication mechanisms, is planned to be proposed for the robust authentication algorithms.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann, 2007.

[2] H. Fiestel, "Cryptography and Computer Privacy", Scientific American, May 1973, vol. 228, no. 5, pp. 15-23.

[3] O. Ur-Rehman, "Applications of iterative soft decision decoding". Aachen: Shaker Verlag; 2013. ISBN:978-3-8440-1641-3.

[4] R. Graveman and K. Fu, "Approximate message authentication codes," in Proceedings of 3rd Fed. lab Symposium on Advanced Telecommuni-cations/Information Distribution, vol. 1, College Park, MD, Feb. 1999.

[5] ISO/IEC 9797-1:2011, "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher".

[6] ISO/IEC 9797-2:2011, "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function".

[7] C. Boncelet, "The NTMAC for authentication of noisy messages", IEEE Transactions on Information Forensics and Security, vol. 1, no. 1, pp. 35-42, Mar. 2006.

[8] Joint Channel Coding and Cryptography, Shaker Verlag, Aachen, 2008, ISBN 978-3-8322-7180-0.

[9] O. Ur-Rehman, N. Zivic, S.A.H.A.E. Tabatabaei, C. Ruland, "Error Correcting and Weighted Noise Tolerant Message Authentication Codes," 5th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1-8, December 12-14, 2011.

[10] O. Ur-Rehman, N. Živic, "Discrete Wavelet Transform based Watermarking for Image Content Authentication", 6th International Conference on Patterns Recognition Applications and Methods, Feb 24-26, 2017, Porto, Portugal.

[11] D. Onien, R. Safavi-Naini, and P. Nickolas, "Breaking and repairing an approximate message authentication scheme," Discrete Mathematics, Algorithms and Applications, World Scientific Publishing Company, 2011.

[12] G. Di Crescenzo, R. F. Graveman, G. Arce and R. Ge, *A Formal Security Analysis of Approximate Message Authentication Codes*, Proc. of the 2003 CTA Annual Symposium, a US Dept. of Defense publication.